Onderzoeksrapport

Security Information Management bij Univé

Versie ter inzage

Rapport

Door : Matthijs Koot

Datum : 2005-05-24

Versie : 1.0

Status : Definitief

Inhoudsopgave

Managementsamenvatting

De strategische keuzes van het bestuur van Univé om meer Internettechnologie te gebruiken bij de primaire bedrijfsprocessen en het beheer van ICT-infrastructuren te decentraliseren naar de leden van de koepelorganisatie verschuift het belang van beveiliging van de buitengrens naar beveiliging van de interne infrastructuur.

In een vooronderzoek is vastgesteld dat er al verschillende preventieve beveiligingsmaatregelen aanwezig zijn binnen de infrastructuur van Univé, maar dat er ook reële scenario's denkbaar zijn waarbij die maatregelen niet zouden volstaan [Unive1]. In een volwassen beveiligingsarchitectuur komen naast preventieve maatregelen ook detectieve maatregelen voor, waarmee bij ontbreken of onverhoopt falen van die preventieve maatregelen pogingen tot inbraak tijdig kunnen worden onderkend. In de context van het *toezicht houden* op de infrastructuur is onderzoek gedaan naar twee beveiligingsmaatregelen: intrusion detection/prevention en consolidatie van loganalyse.

De resultaten van het onderzoek omvatten een theoretische beschrijving van beide maatregelen en een terugkoppeling van die maatregelen naar de situatie bij Univé. Tijdens drie weken bureauonderzoek zijn diverse wetenschappelijke artikelen en boeken onderzocht. Tijdens één week veldonderzoek zijn de beveiligingsdomeinen bij Univé geïdentificeerd, waarmee een beeld is verkregen van de plaats waar de maatregelen mogelijk van toepassing zijn. Ten slotte is een Proof-of-Concept omgeving opgesteld, bestaande uit diverse technische verschijningsvormen van de betrokken maatregelen. Binnen die opstelling zijn diverse hack scenario's uitgevoerd om een indruk te krijgen van de detectieve werking.

Intrusion detection/prevention (IDP) kan worden ingepast op netwerk, host en applicatieniveau en betreft ('van oudsher') een puntoplossing voor detectie van pogingen tot inbraak. Consolidatie van beveiligingsgerelateerde meldingen wordt ook *security information management* (SIM) genoemd en betreft het consolideren en correleren van meldingen van heterogene componenten. Terwijl IDP dus een beperkte focus heeft, beoogt SIM een holistisch overzicht van de beveiliging van een infrastructuur. SIM wordt in Amerika al enige tijd grootscheeps aangewend ter ondersteuning voor compliancy met Section 404 van Sarbanes-Oxley. Hoewel Univé geen beursgenoteerde organisatie is kan SIM op dezelfde manier bijdragen aan de beveiliging van de informatievoorziening van Univé en zou het - anticiperend op toekomstige wet- en regelgeving - nu al een plaats kunnen krijgen binnen de beveiligingsarchitectuur van Univé.

Ter afsluiting van het onderzoek is in een drietal cases teruggekoppeld naar de situatie bij Univé en wordt een indicatie gegeven van technische en beheermatige randvoorwaarden.

De beslissing tot het implementeren van IDP en/of SIM ligt bij het management van Univé; uit een risicoanalyse zal blijken of de kosten van die maatregelen in verhouding zijn met de risico's die (wel of niet) aanwezig zijn.

1. Inleiding

1.1 Onderwerp

Het onderwerp van dit onderzoek is intrusion detection/prevention en geconsolideerde logging bij Univé. In de loop van het rapport zal blijken hoe die onderwerpen relateren aan de term *Security Information Management* die wordt gebruikt in de ondertitel van dit rapport.

Achtereenvolgens zullen aan de orde komen:
- intrusion detection/prevention;
- geconsolideerde logging;
- relatie van beide maatregelen met Univé.

1.2 Probleemstelling

(NB: vrijwel dezelfde probleemstelling als het vooronderzoek)
De opkomst van webtechnologie, draadloze netwerken, VPN-koppelingen en aanverwante technologie leidt bij veel organisaties tot vervaging van de grens tussen de vertrouwde netwerkperimeter en onvertrouwde netwerken. Er is daarom groeiende belangstelling voor 'deperimeterisatie' van netwerkbeveiliging, waarbij de focus verschuift naar beveiliging van de eindpunten [CompWkly1]. Bij de evolutie van beveiligingsarchitectuur is het essentieel om continu af te stemmen met de algemene ontwerpcriteria die gelden voor beveiliging (zie Bijlage 1: Ontwerpcriteria).

Imagoschade door het uitlekken van vertrouwelijke gegevens, winstderving door barbaarse aanvallen op computernetwerken en onopgemerkte fraude door malafide eindgebruikers: de bedreigingen zijn niet nieuw, maar de opmars van onvertrouwde elementen binnen bedrijfsnetwerken creëert de noodzaak om ze opnieuw te beschouwen.

Zo ook bij Univé. Als verzekeraar omgeven door eisen van de wetgever, eisen van toezichthoudende instanties en verwachtingen van verzekerden dient Univé zich bijzonder goed te kwijten van goed ingerichte preventieve en proactieve beveiligingsmaatregelen. Gartner voorspelde in 2004: *"System Downtime Caused by Software Vulnerabilities will Triple by 2008 for Firms that Don't Take Proactive Security Steps"* [Gartner2]. Eén van de onderdelen van proactieve beveiliging is het continu screenen en controleren van de eigen infrastructuur en beveiligingsarchitectuur. Uit een bedreiginganalyse [Unive1] blijkt dat de infrastructuur van Univé redelijk is beschermd tegen bedreigingen van buitenaf, maar dat het in verband met bedreigingen van binnenuit (direct of indirect) wenselijk is om inzicht te hebben in wat er dagelijks op en met de infrastructuur gebeurt. In dit onderzoek staan de volgende vragen centraal: wat zijn intrusion detection en geconsolideerde logging, wat is hun meerwaarde en wat zijn de randvoorwaarden voor implementatie bij Univé?

1.2.1 Doelstelling

In het vooronderzoek is een bedreiginganalyse uitgevoerd op de infrastructuur van Univé. Uit dat rapport volgde dat er bij Univé een gebrek aan inzicht is in de infrastructuur en dat er weinig maatregelen zijn genomen om bedreigingen van binnenuit tegen te gaan. Als aanvullende maatregelen werden onder meer intrusion detection/prevention en consolidatie van logging genoemd. Dit onderzoek beoogt beide maatregelen dieper te beschouwen en een advies te geven over de randvoorwaarden bij toekomstige productkeuze of implementatie binnen de infrastructuur van Univé.

1.3 Werkwijze

Het onderzoek is opgedeeld in drie delen: bureauonderzoek (drie weken), veldonderzoek (een week) en experimenteel onderzoek (vier weken). Bij het bureauonderzoek zijn de theoretische concepten achter intrusion detection/prevention en geconsolideerde logging onderzocht en is de rol die beide maatregelen binnen een beveiligingsarchitectuur hebben beschreven.

Bij het veldonderzoek is een interview afgenomen waaruit duidelijk werd welke beveiligingsdomeinen bij Univé kunnen worden onderscheiden en op welke plaatsen in de infrastructuur monitoring maatregelen wenselijk zijn (of juist niet). Samen met opgedane ervaring in het eerste deel van de experimentele fase zijn de volgende vragen beantwoord:

- welke netwerkkoppelingen, systemen of applicaties zijn relevant;
- welke eisen dienen aan de logging en IDP-architectuur te worden gesteld;

Ten slotte wordt in de conclusie een advies geformuleerd over de implementatie van intrusion detection/prevention en geconsolideerde logging binnen Univé.

2. Intrusion Detection en Prevention

Met de opkomst van Internet verzamelen en verwerken steeds meer organisaties hun gegevens in netwerken van informatiesystemen. Dankzij het open karakter van Internet is inbraak in zulke netwerken een steeds serieuzer probleem geworden. *Intrusion detection* is gericht op het detecteren van activiteiten die niet overeenstemmen met het beveiligingsbeleid van een organisatie en wordt – net als toegangscontrole, firewalls, *honeynets*, et cetera [Spitzner1] – als een normaal onderdeel beschouwd van een gezonde beveiligingsarchitectuur om die systemen te beschermen.

Afhankelijk van de taak die zo'n systeem binnen een infrastructuur kan uitoefenen wordt onderscheid gemaakt tussen *passieve* systemen en *reactieve* systemen [Wikipedia1]. Een passief systeem kan potentiële[1] beveiligingsproblemen detecteren en meldingen genereren naar (bijvoorbeeld) een management console. Die meldingen moeten daarna door een persoon worden gelezen, onderzocht en afgehandeld. In die vorm wordt gesproken van een *Intrusion Detection System* (kortweg *IDS*) en wordt vaak een analogie getrokken met een inbraakalarm. Een reactief systeem is in staat om na detectie zélf handelingen te verrichten om incidenten te voorkomen of verdere schade te beperken. In die vorm wordt gesproken van *Intrusion Prevention System* (kortweg *IPS*). Om aan beide vormen te refereren wordt vaak de afkorting *IDP* gebruikt, zo ook in dit rapport[2]. Waar wordt gesproken over *IPS* wordt dus expliciet alleen intrusion *prevention* bedoeld, waar wordt gesproken over *IDS* wordt expliciet intrusion *detection* bedoeld.

2.1 Inleiding van IDP

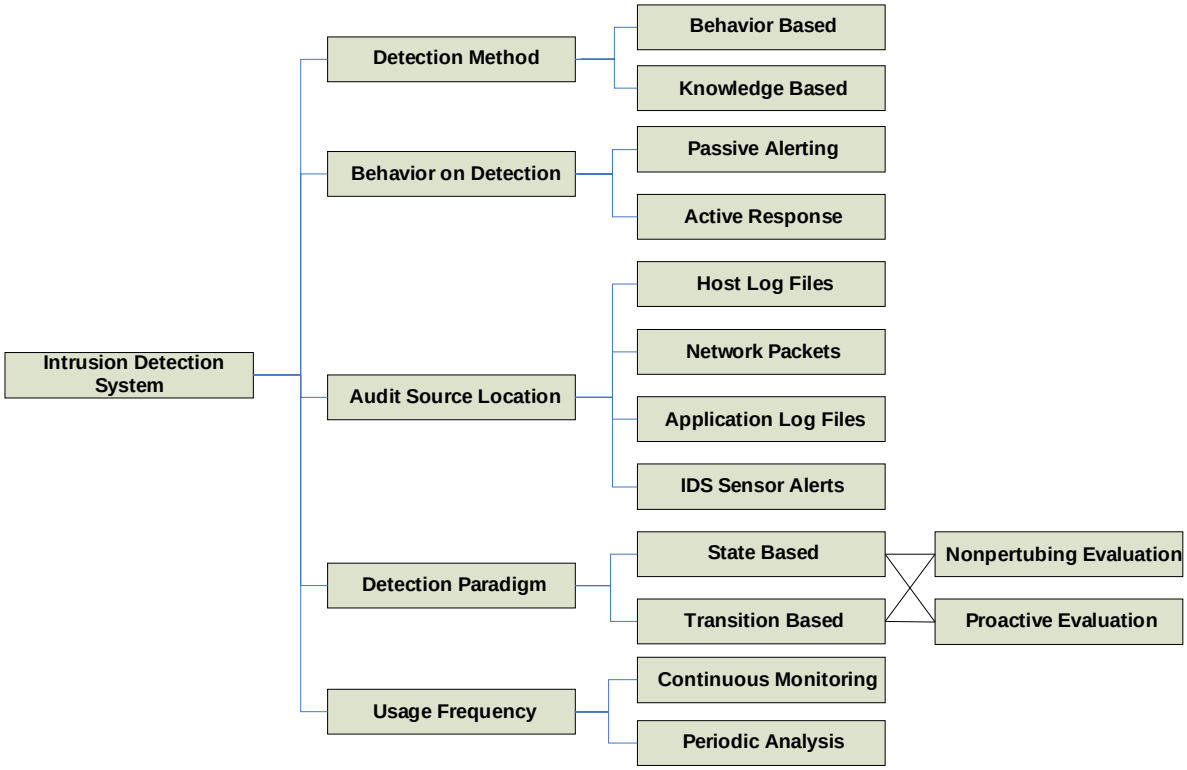
IDP vormt een extra laag van beveiliging in een infrastructuur. Waar firewalls het leeuwendeel aan rommel kunnen tegenhouden, kan IDP detecteren welke ongewenste zaken alsnog door een firewall heen komen. IDP kan bijvoorbeeld webservers bewaken op exploits die door de firewall worden doorgelaten (terwijl een normale firewall de inhoud van het verkeer niet controleert en alleen werkt op basis van *alles of niets*). Afhankelijk van de gekozen IDP-architectuur kan de infrastructuur bovendien ook worden bewaakt op aanvallen van binnenuit (zie Bijlage 3: Voorbeeld beveiligingsarchitectuur (deel 2)). Een nevenfunctie van IDP is tijdige onderkenning van misconfiguraties van firewalls; als de IDP sensor gebruikt maakt van *anomaly-based detectie* (zie H2.3.2) kan afwijkend netwerkverkeer direct worden opgemerkt. Zonder IDP zullen de meeste pogingen tot inbraak nooit worden opgemerkt en zullen geslaagde pogingen vaak alleen worden opgemerkt als er zichtbare schade is aangericht [Innella2]. Met IDP kan informatie over dit soort ongewenste zaken in (near) real-time boven tafel komen, waarmee incidenten kunnen

[1] Er wordt opzettelijk gesproken van 'potentieel', omdat bepaalde zaken soms onterecht worden gemeld als beveiligingsprobleem of de gemelde zaak geen gevolgen kan hebben voor de infrastructuur (zoals bij een MS IIS exploit die op Apache wordt uitgeprobeerd).

[2] De hoeveelheid acroniemen en begrippen zal indrukwekkend blijken; in dit rapport wordt echter getracht op dezelfde manieren aan de materie te refereren als gebruikelijk is in de literatuur en wetenschappelijke stukken op basis waarvan dit rapport is geschreven.

worden voorkomen – en zo niet, dan is forensisch onderzoek nog altijd gebaat bij de IDP-rapportages.

Henri Débar heeft in 1998 een taxonomie beschreven van intrusion detection (prevention) systemen. In 2001 is door een tiental onderzoekers onder de vlag van IBM's lab in Zürich een gereviseerde taxonomie uitgebracht [IBM3]:



In 2000 heeft Stefan Axelsson de taxonomie van detectiemethoden verder gedetailleerd [Axelsson1] - die uitbreiding valt echter buiten de scope van dit onderzoek. In de volgende paragrafen zullen tegen de achtergrond van de bovenstaande taxonomie achtereenvolgens worden besproken:
- de architectuur van IDP-systemen;
- detectiemethoden;
- problemen en beperkingen.

Voor de geschiedenis van IDP – een onderwerp dat eigenlijk al 25 jaar oud is – wordt verwezen naar [Anderson1], [Denning1], [Endorf1] en [Innella1].

Een onderwerp waar veel onderzoek naar wordt gedaan en dat gerelateerd is aan IDP is *correlatie* van meldingen. Dat onderzoek overschrijdt echter het onderwerp IDP, daarom is gekozen om correlatie pas te behandelen in het hoofdstuk over geconsolideerde logging (H3.6). Dat onderzoek draagt bijvoorbeeld bij aan het reduceren van het aantal *false positives* (zie H2.4.1).

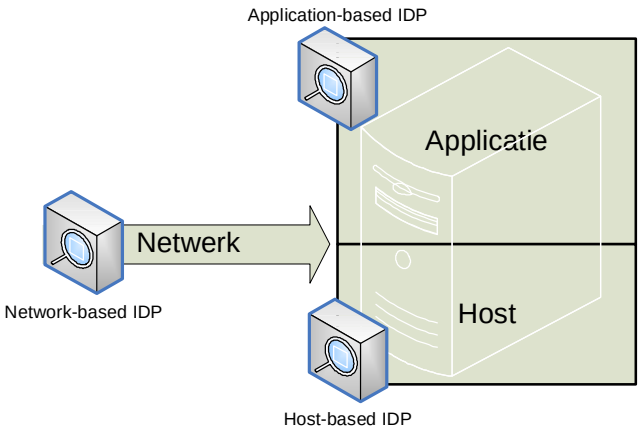
2.2 Architectuur

Er zijn in de wetenschappelijke wereld al in 1975 verschillende ontwerpcriteria geformuleerd voor beveiligingsarchitecturen (zie Bijlage 1: Ontwerpcriteria). In dit onderzoek ligt het zwaartepunt bij gelaagdheid en gedistribueerdheid.

2.2.1 Gelaagdheid

In [Unive1] werd een lagenmodel gehanteerd om bedreigingen en maatregelen in te plaatsen; in de wereld van IDP worden dezelfde functionele lagen onderscheiden [Computer1], [Endorf1], [Rieck1], [Steffen1]. IDP kan worden toegepast op:

- een applicatie (*Application-based IDP*, kortweg *AIDP*);
- een computer (*Host-based IDP*, kortweg *HIDP*);
- een netwerk (*Network-based IDP*, kortweg *NIDP*) .



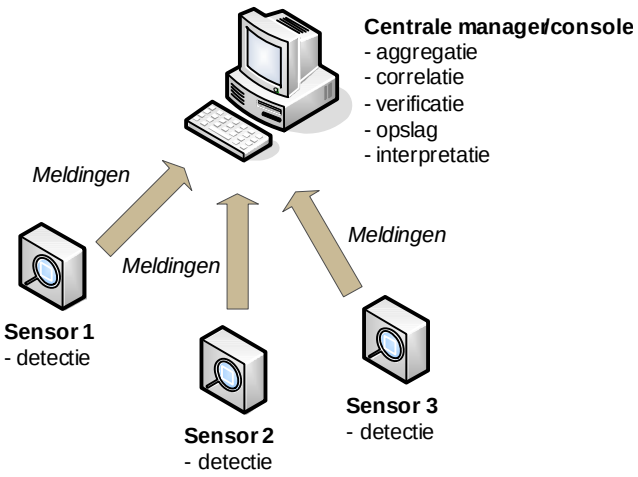
Passieve network-based IDP was de laatste jaren het meest populair, maar Gartner voorspelde in december 2004 dat passieve IDP inmiddels z'n beste tijd heeft gehad en dat er meer behoefte zal komen aan reactieve host-based IPS [Gartner1]. De verschillende IDP-gebieden en begrippen worden straks in meer detail besproken.

2.2.2 Gedistribueerdheid

Een 'volwassen' IDP systeem – daarmee wordt een systeem bedoeld dat geschikt is voor een grote infrastructuur – heeft een multi-tier architectuur waarin samenwerkende IDP-componenten op verschillende locaties samen één IDP-systeem vormen. Zo'n architectuur bestaat meestal ten minste uit *sensors*, *managers* en een *console* [Endorf1]. In [Nan1] worden enkele eigenschappen beschreven van de vorm van gedistribueerde IDS, zoals momenteel in gebruik bij een onderzoeksproject van SURFnet [SURFnet1]:

"- Characteristics of a truly Distributed IDS:
- sensors all over the network
- sensors all use the same rule set
- alert storage on a central location
- expertise on a central location"

De meest eenvoudige multi-tier architectuur is de gecentraliseerde architectuur:



Alle sensoren sturen hun meldingen naar dezelfde centrale console (die tevens manager is). Die ene console voert vervolgens alle verwerking van de meldingen uit. Bij een grote hoeveelheid sensors kan een grote hoeveelheid meldingen worden gegenereerd en zal de console overbelast raken (in de praktijk ligt het maximum na goede tuning rond 25 sensoren, aldus [Cisco2]). Voorbeelden van implementaties van deze architectuur zijn DIDS van University of California in Davis (1991) en STAT van University of California in Santa Barbara (1992) [Cuppens1], [STAT1].

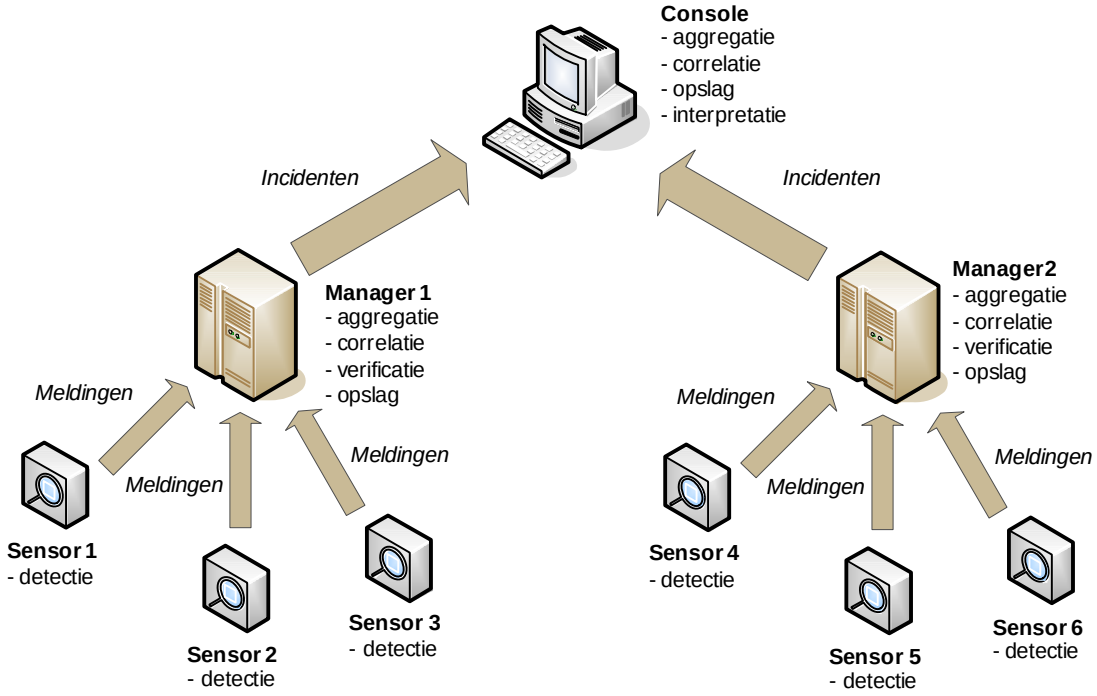
Enkele kernvragen bij het ontwerpen van een IDP-architectuur zijn:

- welk soort sensors wordt gebruikt en hoeveel sensors zijn er nodig?
  - netwerk
    - welke koppelingen moeten worden gescreend?
  - host
    - welke hosts moeten worden gescreend?
    - welke besturingssystemen zijn op die hosts in gebruik?
  - applicatie
    - welke applicaties moeten worden gescreend?
- welke reactieve functies zijn nodig?
  - voor netwerk, host, applicatie
    - wat is het beleid?
    - welke reactieve mogelijkheden zijn er?
- waar worden de meldingen verwerkt en hoe wordt gerapporteerd?
  - alleen centrale verwerking
  - centrale verwerking met decentrale voorverwerking (filtering en aggregatie)
- wat communiceren de componenten?
  - informatiestroom
  - controlestroom
- hoe communiceren de componenten?
  - fysiek gescheiden netwerk
  - beveiligde covert channel

Het antwoord op deze vragen hangt behalve het beleid van de organisatie ook af van de grootte van de infrastructuur waarvoor de IDP-architectuur geschikt moet zijn en het aantal (logische) segmenten dat moet worden gemonitord [Cisco2]. De schaalbaarheid wordt in elk geval een belangrijker criterium naar mate het aantal sensors groeit. Er zijn verschillende mogelijkheden om IDP schaalbaar te maken [Innella2], [Rieck1]:

1. een hiërarchisch model met één root node (de console), meerdere normale nodes (gecentraliseerde managers) en meerdere leave nodes (de sensors) [Debar2];
2. een puur gedistribueerd model waar elk component zowel sensor als manager is of kan zijn – feitelijk een Peer-to-Peer model voor intrusion detection [Locasto1].

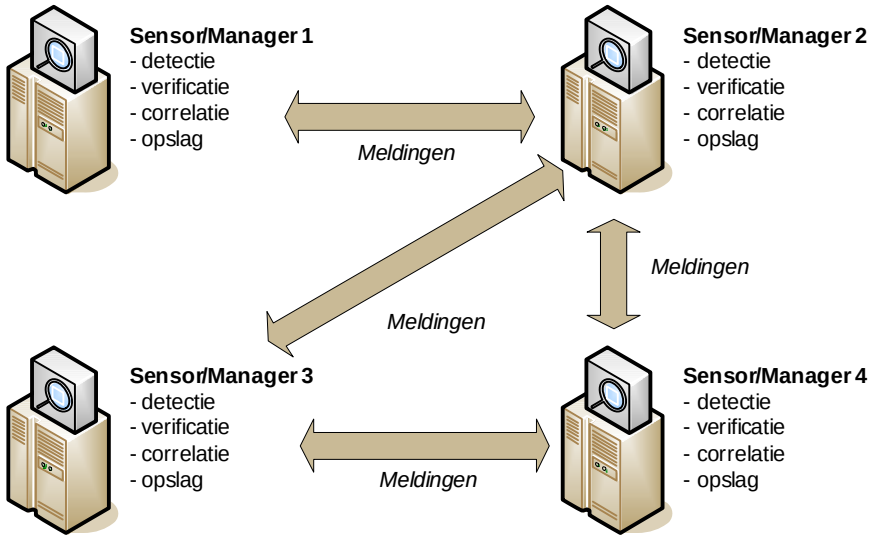
Een hiërarchische IDP-architectuur kan er als volgt uitzien:



Hiërarchische architecturen bevatten per definitie *single points of failure*; uitval van één manager component (bijvoorbeeld als gevolg van een Denial-of-Service aanval) leidt tot uitval van (een deel van) de IDP-functie [Mell1]. Voorbeelden van implementaties van deze architectuur zijn EMERALD van SRI International (1997) en AAFID van Purdue University (1998) [Cuppens1].

In een puur gedistribueerde Peer-to-Peer architectuur is geen sprake van een single point of failure, omdat elk component zowel sensor als manager is en volledig onafhankelijk van andere componenten functioneert:

(z.o.z.)

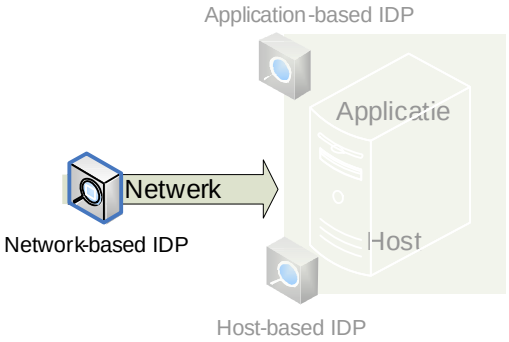


Bij de Peer-to-Peer architectuur spelen echter weer andere problemen, waaronder extra complexiteit en onvolledige correlatie (geen enkele sensor kent de volledige context, terwijl bij het hiërarchische model de volledige context ten minste bekend is bij de root node). Er zijn nog geen bruikbare implementaties van deze architectuur, maar er wordt volop onderzoek naar gedaan [Locasto1].

Varianten op de genoemde architecturen zijn ook mogelijk, zoals toepassing van autonome agents [Barrus1], [Deeter1], [Ingram1], [Perumal1]. Maar ook van die architecturen lijken vooralsnog geen bruikbare implementaties beschikbaar.

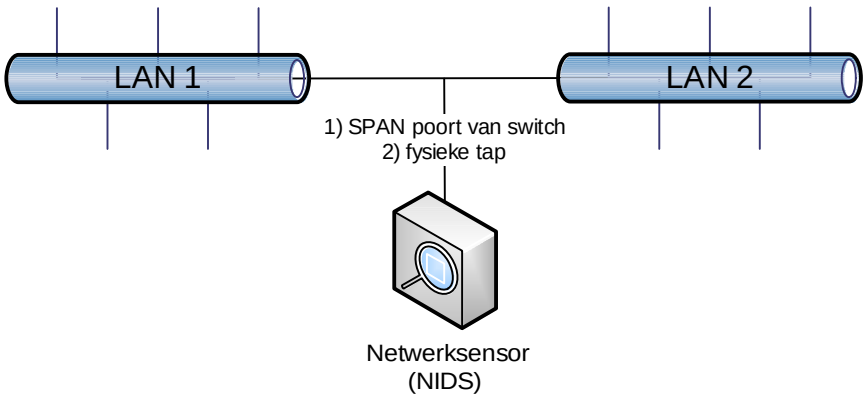
Eerder werd al onderscheid gemaakt tussen een *informatiestroom* en een *controlestroom*. De informatiestroom bevat de meldingen van de sensors en is in een hiërarchische architectuur typisch alleen upstream. De controlestroom bevat commando's om de sensors en lagere managers te besturen (wijzigen van policies, reactieve handelingen) en is typisch alleen downstream. Het is niet ondenkbaar dat er voor de stromen verschillende producten worden gebruikt, zoals IBM Risk Manager voor de informatiestromen en Cisco CiscoWorks voor de controlestromen voor configureren van Cisco IDP componenten. Van beide stromen zijn beveiliging en vertrouwensniveau belangrijke eigenschappen; de integriteit, authenticiteit en vertrouwelijkheid van de communicatie tussen managers en sensors moeten in orde zijn; een manager mag bijvoorbeeld geen (gespoofde) meldingen accepteren van niet-bestaande sensors.

2.2.3 Network-based IDP

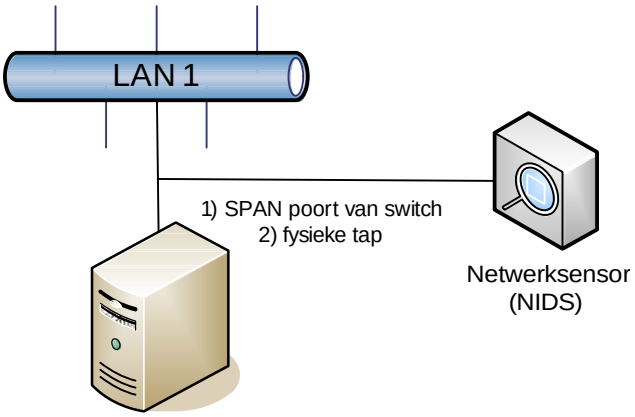


NIDS

Een *Network-based Intrusion Detection System* (kortweg *NIDS*) kan met slechts een paar sensors op weloverwogen plaatsen een grote infrastructuur in de gaten houden. Een NIDS wordt als zelfstandig element aan een bestaand netwerk gehangen en is onafhankelijk van de bestaande platformen binnen een infrastructuur. Een NIDS heeft nauwelijks of geen impact op de performance van het netwerk dat wordt gemonitord, zeker wanneer de sensor *out-of-band* wordt geplaatst (zie het plaatje onder deze alinea). De sensor – feitelijk een promiscous packet sniffer – wordt doorgaans aangesloten op een *SPAN poort* (Switch Port ANalyzer) van een switch, op een willekeurige poort van een hub of met een fysieke tap aan een bestaande verbinding gehangen [Snort1]. Op de laatste manier is het absoluut zeker dat de sensor *al* het verkeer op de gemonitorde koppeling ontvangt en er zelf geen verkeer op kan genereren - een fysieke tap dwingt een alleen-ontvangen koppeling af. Bij het gebruik van een SPAN poort zal de switch pakketten moeten kopiëren, waarbij geheugenbuffers zullen moeten worden gebruikt – als die buffers vollopen resulteert dat ofwel in een verminderde performance van de hele switch, ofwel in het negeren van overvloedige pakketten waardoor de sensor de overvloedige pakketten niet zal zien en mogelijk aanvallen zal missen (*false negatives*, zie H2.4.1).



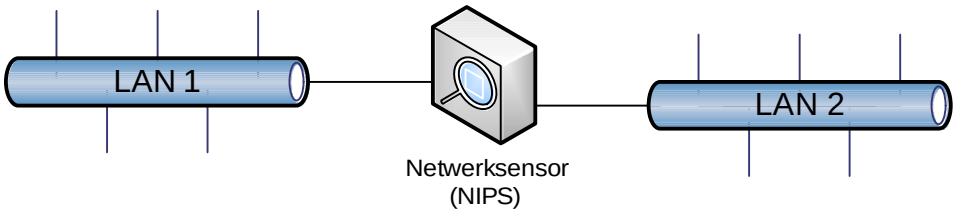
In het voorgaande plaatje screent de sensor het netwerkverkeer tussen LAN 1 en LAN 2; vanzelfsprekend is dat niet de enige denkbare situatie. Indien de organisatie slechts het netwerkverkeer van en naar één bepaalde server wil screenen kan de volgende opzet worden gebruikt:



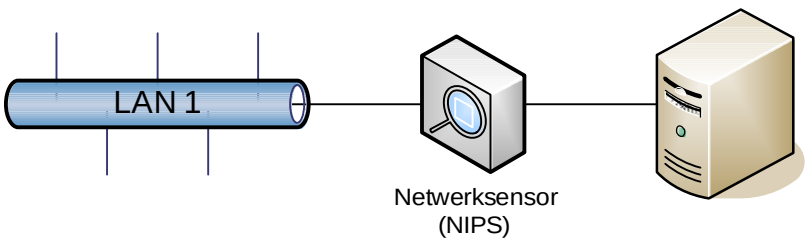
(Et cetera.)

NIPS

Een *Network-based Intrusion Prevention System* (kortweg *NIPS*) kan in geval van een veronderstelde aanval het betreffende netwerkverkeer blokkeren om een incident te voorkomen. Een NIPS is evenals een NIDS platformonafhankelijk, maar vereist *in-line* plaatsing (het netwerkverkeer moet door de NIPS heen om preventie mogelijk te maken) en kan daarom in tegenstelling tot NIDS een grote impact hebben op de performance en beschikbaarheid van de koppeling die wordt gemonitord.



Hier geldt wederom dat deze opstelling zeker niet de enige denkbare is. Indien de organisatie slechts het netwerkverkeer van en naar één bepaalde server wil screenen kan de volgende opzet worden gebruikt:



NIDS en NIPS (NIDP)

Met NIDP is het dus mogelijk om netwerkverkeer te bewaken, maar er zijn enkele beperkingen. Versleuteld netwerkverkeer kan zonder aanvullende handelingen niet worden geïnspecteerd door een normale netwerksensor – versleuteld verkeer kan dus alleen worden geïnspecteerd tot en met de OSI-laag waarop de versleuteling plaatsvindt (bij SSL

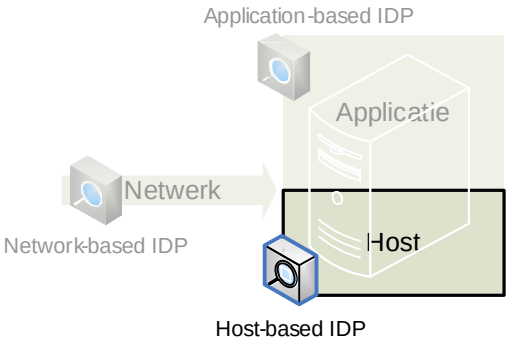
is dat bijvoorbeeld de transportlaag, bij IPSec de netwerklaag). Bovendien moet de sensor voldoende capaciteit hebben om al het netwerkverkeer over de koppeling te kunnen analyseren; typisch 100Mbit, 1Gb of hoger. Een belangrijk aandachtspunt is hoe een sensor zich gedraagt bij overbelasting; blijft de sensor volgens *best effort* het verkeer screenen of valt de sensor helemaal weg? (CPU belasting, geheugengebruik, TCP buffers)

Voorbeelden van producten die voorzien in NIDP functies:
- ISS Proventia (www.iss.net)
- Symantec Gateway Security (www.symantec.com)
- Enterasys Dragon Network Sensor (www.enterasys.com)
- McAfee IntruShield (www.mcafee.com)
- Snort (IDS, www.snort.org)
- Hogwash (IPS en packet scrubber, hogwash.sourceforge.net)

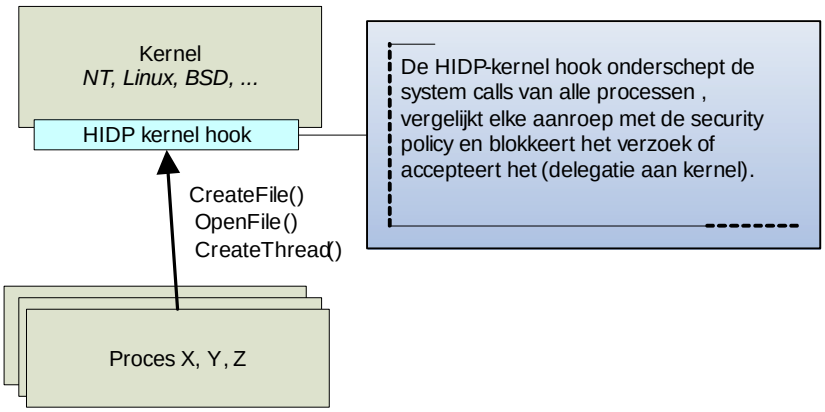
Idealiter communiceren de netwerksensors via een fysiek gescheiden netwerk (‘out of band’) met andere IDP-componenten; op die manier blijft de IDP-informatievoorziening beschikbaar als de gescreende infrastructuur slachtoffer is van een Denial-of-Service aanval en wordt de kans op verstoringen die door de IDP-componenten zelf worden veroorzaakt verminderd. In Bijlage 2: Voorbeeld beveiligingsarchitectuur (deel 1) en Bijlage 3: Voorbeeld beveiligingsarchitectuur (deel 2) zijn illustraties opgenomen van architecturen waarin IDP is ingebed met een fysiek gescheiden netwerk.

Detectie gaat altijd vooraf aan eventuele preventie of correctie/repressie, dat geldt voor alle soorten IDP; de benaderingen c.q. mechanismen van detectie worden besproken in H2.3. Het volstaat hier te zeggen dat een NIDP sensor netwerkverkeer screent en dat zulk verkeer met ‘deep packet inspection’ moet kunnen worden ontleed tot aan de applicatielaag om aanvallen op applicatieniveau te kunnen herkennen. Preventie is alleen mogelijk door een sensor in-line te plaatsen en als bridge te laten functioneren (L2 switch) - de sensor heeft daarbij zelf meestal geen IP-adres om te voorkomen dat de sensor zelf doelwit wordt van IP-gebaseerde aanvallen. Bij in-line plaatsing kan de sensor ongewenste IP-pakketten simpelweg droppen (of de Time-To-Live van de pakketten op 0 zetten, met idem resultaat). Een andere mogelijkheid is vervanging van de kwetsbare payload, zoals het vervangen van een shellcode met allemaal 0x00 bytes. In beide gevallen is het gevaar van false positives duidelijk aanwezig. Correctie/repressie is eigenlijk alleen van toepassing op NIDS en kan voor TCP-verkeer worden gerealiseerd door gespoofde TCP RST (reset) pakketten te sturen naar zowel het doel als de bron van een veronderstelde aanval. Ongewenst UDP-verkeer kan worden afgeketst door ICMP destination unreachable pakketten te sturen naar de bron, hoewel de effectiviteit van die methode twijfelachtig is door de ‘spoofbare’ aard van het verbindingsloze UDP en de kans dat de aanvaller ICMP verkeer wegfiltert bij de bron.

2.2.4 Host-based IDP



Host-based Intrusion Detection/Prevention (kortweg *HIDP*) is in staat om de activiteiten te screenen op de host waarop een host sensor is geïnstalleerd. De host sensor is als platformspecifieke software aanwezig, maakt typisch gebruik van '*kernel hooks*' en heeft altijd een bepaalde impact op de performance van de host die wordt bewaakt omdat de sensor zelf geheugen en CPU cycles gebruikt. HIDP stelt een organisatie in staat om processen, bestanden, gebruikers en netwerkverbindingen op een host te monitoren en levert daarmee een veel gedetailleerdere monitoring van individuele systemen dan NIDPs kunnen. Er wordt ook onderzoek gedaan naar intrusion detection op basis van patronen in system calls [Garfinkel1], [Hofmeyr1], [Kang1], [Rieck1], [Zimmerman1]. Het concept van onderschepping van system calls door een 'kernel hook' kan als volgt worden weergegeven:



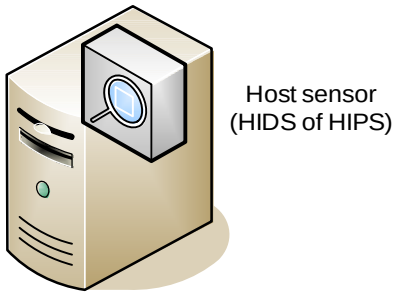
Een aansprekend voorbeeld is een policy die definieert dat webserver processen slechts een beperkte verzameling bestanden mogelijk benaderen (de HTML pagina's en plaatjes van een website); een onverhoopte buffer overflow zou dan niet langer kunnen leiden tot het uitlezen of wijzigen van systeembestanden. Een aanvaller is dan bijvoorbeeld ook niet in staat om via shellcode een nieuw console/shell/prompt proces te starten.

Infrastructureel gezien is er geen verschil tussen de architectuur van HIDS en HIPS; in beide gevallen is sprake van software op een host – ofwel ingebed en meegeleverd in het besturingssysteem van de host, ofwel achteraf toegevoegd als los component. Een HIPS zou als preventieve maatregel bijvoorbeeld een systeem kunnen afsluiten, een OS account

kunnen locken, een buffer overflow kunnen onderscheppen of (zoals in bovenstaande situatie) een system call kunnen blokkeren.

Een groot verschil tussen HIDP en NIDP is dat de laatste met slechts één sensor het netwerkverkeer tussen tientallen of honderden systemen kan monitoren, terwijl HIDP een sensor vereist op élk systeem dat moet worden gemonitord. Een tweede minpunt is dat HIDP-sensors moeten vertrouwen op de informatievoorziening van de kernel op een host en bijgevolg onbetrouwbaar zijn als die host eenmaal is gecompromitteerd.

Het 'architectuurplaatje' van HIDP is simpel:

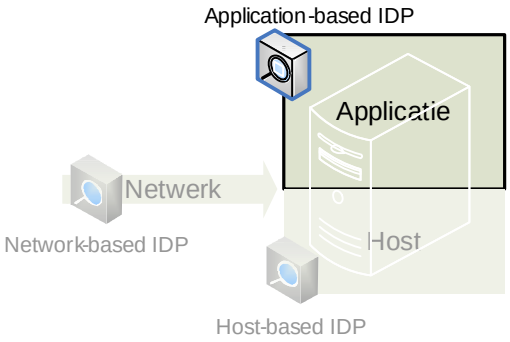


Voorbeelden van producten die voorzien in HIDP functies:
- Tripwire (www.tripwire.org, sec detectief)
- Advanced Intrusion Detection Environment (www.cs.tut.fi/~rammer/aide.html, idem)
- Linux Intrusion Detection System (www.lids.org)
- GFI LANguard System Integrity Monitor (www.gfi.com/lansim)
- Symantec Host Intrusion Detection System (www.symantec.com)
- McAfee Entercept (www.mcafee.com)
- PrevX (www.prevx.com)
- HP-UX Host Intrusion Detection System (www.hp.com)

Door verschillende actuele ontwikkelingen worden hosts langzaamaan al voorzien van bepaalde HIDP functionaliteit, zoals door personal firewalls, anti-virus software, anti-spyware software en bijvoorbeeld de integriteitscontroles die Windows zelf uitvoert op systeembestanden (corrupte .dll's, niet-gesigneerde drivers, et cetera). Al die systemen hebben ongeveer hetzelfde doel: een host beschermen tegen bedreigingen van binnenuit (lokale exploits, spyware, virussen van draagbare media) en buitenaf (remote exploits, DoS, spam, virussen van het netwerk).

Host-based IPS is in harmonie met de toenemende behoefte aan c.q. de noodzaak van beveiliging van eindpunten en wordt door Gartner gezien als een groeimarkt (ten minste tot 2008). Met name de implementaties waarbij weinig of geen onderhoud nodig is hebben de aandacht - de werking van een HIDP sensor mag niet volledig afhankelijk zijn van de volledigheid en correctheid van een database met signaturen, zoals nog steeds gebruikelijk bij network-based sensors. Die aanpak is in zekere zin achterhaald.

2.2.5 Application-based IDP



Application-based Intrusion Detection/Prevention (kortweg *AIDP*) is applicatiespecifiek en maakt het mogelijk om activiteiten binnen één bepaalde applicatie zeer gedetailleerd te monitoren [Sielken1], [Steffen1]. Een *reactief* AIDP systeem is in feite synoniem aan een application-level firewall [Wikipedia1], zoals een XML firewall [NWFusion2], [Reactivity1].

Bij veel applicaties is detectie alleen mogelijk op basis van logbestanden en is dus geen preventie mogelijk; de logregels worden immers pas weggeschreven *nadat* een (malicieuze) handeling heeft plaatsgevonden. Een AIDP sensor zou zich kunnen laden binnen de procesruimte van een applicatie en zich daar nestelen om validaties uit te voeren op gegevensinvoer en aanroep van functies, qua concept vergelijkbaar met kernel hooks bij HIDP. In .NET zou zoiets bijvoorbeeld kunnen worden gerealiseerd met HTTP Modules en HTTP Handlers, waarbij inkomende verzoeken eerst aan een IDP module wordt gedelegeerd alvorens verder te worden behandeld.

Voorbeelden van producten die voorzien in AIDP functies:
- eEye's SecureIIS voor Microsoft IIS (www.eeye.com)
- mod_security voor Apache (www.modsecurity.org)
- AppRadar voor Microsoft SQL Server (www.appsecinc.com)

De architectuur van AIDP is sterk afhankelijk van de applicatie, er wordt daarom geen illustratie gegeven. AIDP kan ingebed zijn *binnen* een applicatie (door ontwikkelaars die veilig ontwerp en veilige code praktiseren, of als mee te compileren of optioneel laadbare module zoals in het geval van mod_security), maar kan ook achteraf worden toegevoegd als een losse schil om de applicatie (zoals AppRadar). Infrastructureel gezien is er geen verschil tussen application-based IDS en application-based IPS, behalve wellicht bij gedistribueerde technologie als CORBA of DCOM [Stillerman1]. Een AIPS zou als preventieve maatregel bijvoorbeeld een applicatie account kunnen locken, eigen processen afsluiten/herstarten of verzoeken vanaf een bepaald IP-adres kunnen negeren.

AIDP is vrij kostbaar in ontwerp, implementatie en beheer en zal daarom alleen voorhanden zijn als er een grote markt voor is (zoals voor populaire applicaties met een hoog risicoprofiel) of als er vanuit bijzondere omstandigheden noodzaak toe is (eisen van de wetgever, eisen van toezichthouders, militaire of bancaire toepassingen, et cetera). Het

lijkt echter waarschijnlijk dat AIDP samen met webservices en verwante technologie zal groeien in populariteit.

Nota bene: applicaties als CRM en ERP bevatten vaak standaardrapportages waarin accounting informatie staat over het gebruik van de applicatie. Door de controle van dergelijke rapportages kunnen bepaalde ongewenste zaken als autorisatiebreuk en misbruik van privileges aan het licht komen. Die procedure zou ook kunnen worden gezien als een vorm application-based IDS [Steffen1]; in dit rapport wordt echter uitgegaan van een meer technische betekenis.

2.2.6 Combinaties

Het functionele onderscheid in drie lagen is in de praktijk niet altijd even helder. Zo zijn er hybriden die verschillende functionele gebieden combineren; *Enterasys Dragon Host Sensor* (www.enterasys.com) combineert bijvoorbeeld HIDP en AIDP; de sensor voert integriteitscontroles uit op het besturingssysteem, bewaakt de kernel op privilege escalations, checkt het Windows Event log, maar biedt daarnaast ook op applicatieniveau bescherming aan IIS en Apache.

Daarnaast zijn er ook combinaties met andersoortige componenten. Soms voegen leveranciers IDP functionaliteit toe aan bestaande niet-IDP producten; enkele firewalls hebben bijvoorbeeld eenvoudige pattern-based detection ingebouwd voor detectie van Nimda en Code Red [Cisco1], [Yoo2]. Verder komt het voor dat verschillende componenten samenwerken; Cisco heeft enkele jaren geleden verzonnen dat hun IDS bij naderend onheil een firewall moest kunnen instrueren om (tijdelijk) ACLs aan te passen – een mogelijkheid die ze *shunning* hebben genoemd [Cisco2], [SFocus1].

Onderscheid behoort echter wel duidelijk te zijn tussen IDS en IPS taken. Sommige NIDS-leveranciers voegen ‘TCP reset spoofing’ of ‘ICMP error spoofing’ functionaliteit toe om hun product als NIPS te kunnen marketen, terwijl de aard van IPS een verschil in netwerktopologie impliceert: een NIPS behoort immers in-line te worden geplaatst om écht preventief te kunnen optreden. Een NIDS kan detecteren dat er een exploit wordt uitgevoerd, maar tegen de tijd dat er gespoofde ‘TCP reset’ of ‘ICMP error’ pakketten worden verstuurd of een firewall is geïnstrueerd om ACLs aan te passen heeft de exploit zijn doel wellicht al lang bereikt – er is bijvoorbeeld een exploit bekend voor Microsoft SQL Server waarbij slechts één UDP-pakket wordt gebruikt [NSS1], [Counterpane1]. Zulke systemen behoren eigenlijk niet te worden beschouwd als *preventieve* maatregel, maar liever als *repressieve* maatregel.

2.2.7 Integratie van IDP-systemen

Hoe heterogener de infrastructuur, hoe minder waarschijnlijk één leverancier kan voorzien in een totaaloplossing voor IDP – zeker bij HIDP of AIDP. De ene leverancier levert sensors voor Windows en Linux, maar niet voor AIX. De andere levert sensors voor Apache, maar niet voor IIS. Bovendien kan de kwaliteit van sensors voor een bepaald gebied verschillen tussen leveranciers, waardoor diversiteit in productkeuze nog waarschijnlijker wordt. In zo’n infrastructuur zullen IDP-systemen van verschillende leveranciers dus met elkaar moeten kunnen samenwerken, of ten minste in één IDP

raamwerk zijn te integreren [ACM1], [Innella2]. Er zijn op dat gebied verschillende standaarden ontwikkeld of in ontwikkeling, doch met vooralsnog beperkte praktische waarde. Twee daarvan specificeren een formaat voor de beschrijving van IDP-meldingen: het *Intrusion Detection Message Exchange Format* van IETF (kortweg *IDMEF*) en het *Common Intrusion Detection Framework* (kortweg *CIDF*) dat zijn oorsprong vindt bij DARPA [IETF1], [ISI1]. Het CIDF project is in 1999 stilgelegd, maar het op XML-gebaseerde IDMEF is nog volop in ontwikkeling en wordt – hoewel het nog geen officiële standaard is – ondersteund door bijvoorbeeld Prelude-IDS [Prelude1] en kleinere academische IDP-projecten [Maglaris1], [STAT1], maar ook door het commerciële IBM Risk Manager [IBM1]. Aanvullend op IDMEF is er anno 2002 in de vorm van het *Intrusion Detection Exchange Protocol* van IETF (kortweg *IDXP*) een poging gedaan tot standaardisatie van een applicatieprotocol voor uitwisseling van dergelijke berichten, waarbij wederzijdse authenticatie, integriteit en vertrouwelijkheid zouden zijn ingebed. De status van die ontwikkeling is helaas onbekend [IETF2]. Een derde initiatief is de ontwikkeling van het Security Device Event Exchange (kortweg *SDEE*), een samenwerkingsverband tussen onder andere Cisco, ISS, Sourcefire, Symantec en TruSecure in TruSecure's ICSA Labs [ICSA1], [ICSA2]. SDEE specificeert zowel een XML-dialect voor beschrijving van IDS alerts als een applicatieprotocol voor de uitwisseling daarvan. SDEE is daarmee vergelijkbaar met de combinatie van IDMEF en IDXP. De aanleiding voor het ontwikkelen van SDEE is niet helemaal duidelijk (wellicht de trage ontwikkeling van IDMEF, het uitblijven van een definitieve IDMEF standaard, of een politiek spel), maar het bestaan van SDEE verklaart het uitblijven van ondersteuning van IDMEF in producten van bijvoorbeeld Cisco en ISS. Een groot verschil tussen IDMEF/IDXP en SDEE en is dat de eerste van nature een open standaard is, terwijl de laatste onderhevig is aan het intellectueel eigendomsrecht van Cisco, ISS, et cetera. Het is in elk geval niet duidelijk welk van de twee in de toekomst het grootste draagvlak en de grootste kans van slagen zal hebben.

Het Franse MITRE doet een poging tot standaardisatie van naamgeving van kwetsbaarheden in de vorm van het welbekende *Common Vulnerabilities and Exposures* woordenboek (kortweg *CVE*), waarin elke kwetsbaarheid een naam krijgt volgens het formaat '*AAA-yyyy-####*' [Mitre1]. CVE is inmiddels wijdverspreid en wordt door veel producten ondersteund. Zolang alle IDP-leveranciers de CVE-namen voor kwetsbaarheden gebruiken in hun meldingen kunnen verschillende IDP-producten enigszins worden geïntegreerd. De integratie blijft daarbij echter wel beperkt tot meldingen die kunnen worden geassocieerd met een CVE-naam; kwetsbaarheden waarvoor (nog) geen CVE-naam beschikbaar is vallen daar dus buiten. MITRE heeft zich echter tot doel gesteld om *alle* (publiekelijk) bekende kwetsbaarheden te benoemen.

Samenvattend lijken de commerciële leveranciers vooralsnog weinig mogelijkheden te bieden voor integratie met IDP-producten van andere leveranciers. Ian Duffy van de US Air Force heeft zulke integratie geprobeerd te bereiken met IDEA, maar ook dat is niet meer dan een experiment gebleven – de enige sensor die IDEA ondersteunt is Snort en de ontwikkeling lijkt na december 2003 te zijn gestopt [Duffy1].

2.3 Detectiemethoden

Er worden twee manieren van detectie onderscheiden: *anomaly-based* en *pattern-based* [Endorf1], [Rieck1], [Wieringa1], [Wikipedia1]. Bij *anomaly-based detection* wordt eerst gedurende een bepaalde periode het 'normale' gebruik of gedrag van een applicatie, host of netwerk gemeten, waarna in operationele modus afwijkingen op die patronen worden opgemerkt als potentieel beveiligingsprobleem. Bij *pattern-based detection* wordt het gegevensverkeer gescreend op aanwezigheid van elementen uit een verzameling signaturen waarvan bekend is dat ze wijzen op een potentieel beveiligingsprobleem.

2.3.1 Pattern-based

Pattern-based detection – waaraan ook wordt gerefereerd met *rule-based detection*, *signature detection* en *misuse detection* – is de meest eenvoudige vorm van intrusion detection. De detectie vindt plaats op basis van een database met signaturen die niet mogen voorkomen op het netwerk, de host of de applicatie. Als de sensor zo'n signatuur aantreft wordt een melding gegenereerd naar een persoon of een andere IDP-component. De kwaliteit van de detectie hangt af van de kwaliteit van de database met signaturen; de signaturen dienen continu up-to-date te worden gehouden en moeten accuraat te zijn.
Als de onderstaande signatuur wordt herkend in een HTTP-verzoek, wijst dat mogelijk op de aanwezigheid van de PHPInclude.Worm [Snort2]:

```
?&cmd=cd%20/tmp\;wget%20
```

Als de onderstaande signatuur wordt herkend in een netwerkpakket, wijst dat mogelijk op de aanwezigheid van de HackerDefender Root Kit [Snort2]:

```
01 9a 8c 66 af c0 4a 11 9e 3f 40 88 12 2c 3a 4a 84 65 38 b0
b4 08 0b af db ce 02 94 34 5f 22
```

Een nadeel aan pattern-based detection is dat alléén bekende kwetsbaarheden worden opgemerkt. Kwetsbaarheden waarvoor geen signatuur beschikbaar is of die niet via een signatuur zijn te herkennen blijven onopgemerkt.

2.3.2 Anomaly-based

Anomaly-based detection – waaraan ook wordt gerefereerd als *profile-based detection* – maakt gebruik van statistische en karakteristieke gedragskenmerken die worden gemeten of vastgelegd alvorens de detector in productie te zetten [Endorf1]. Een belangrijk verschil met pattern-based detectie is dat bij deze manier wordt vastgelegd wat *wel* mag.

Statistische gedragskenmerken zijn *kwantificaties* van het normale gebruik of gedrag, zoals:
- "dit systeem genereert normaliter maximaal 25% van zijn capaciteit aan UDP-verkeer";
- "deze applicatie gebruikt normaliter maximaal 30% van het werkgeheugen";
- "op dit netwerksegment ligt de framegrootte normaliter gemiddeld tussen 1024 en 4096 bytes".

Karakteristieke gedragskenmerken zijn *kwalificaties* van het normale gebruik of gedrag, zoals:
- “deze gebruiker verstuurt normaliter geen bestanden over het netwerk met FTP”;
- “dit netwerksegment bevat normaliter geen IPv6 verkeer”;
- “dit systeem zet normaliter geen uitgaande IRC-verbindingen op”.

Een afgeleide is *protocol anomaly detection*, waarbij afwijkingen of misbruik van zwakheden in communicatieprotocollen worden gedetecteerd [Lemonnier1], [Yoo1]. Voorbeeld van zo’n afwijking is een onmogelijke combinatie van vlaggen in een TCP pakket (de SYN en FIN vlaggen zijn tijdens een normale TCP-sessie nooit tegelijk gezet).

Een voordeel aan anomaly-based detection is dat het in tegenstelling tot pattern-based detection ook bepaalde onbekende kwetsbaarheden kan opmerken. Een nadeel is dat deze vorm van detectie typisch veel false positives genereert (zie H2.4.1).

2.4 Problemen en beperkingen

Naast de problematiek van integratie van IDP-systemen, zoals besproken in H2.2.7, is er nog een aantal andere problemen bij IDP; die worden in de volgende paragrafen besproken.

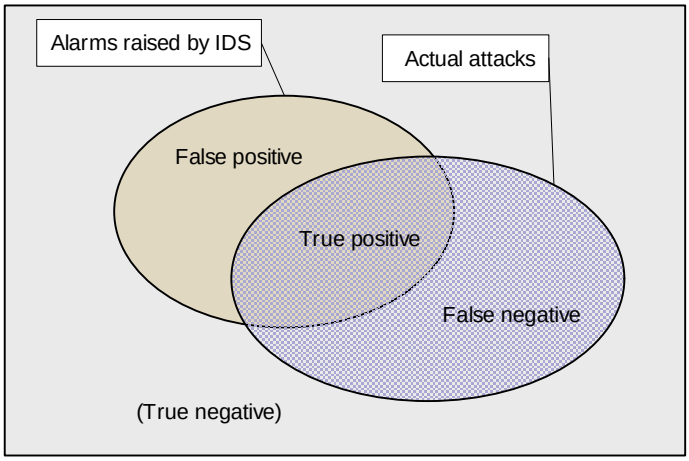
2.4.1 False positives en false negatives

IDP is complex en wordt omgeven door zowel technische als beheermatige problemen, vaak gerelateerd aan *false negatives* en *false positives*.

Een false positive betreft een onjuiste of ongewenste beoordeling van sensorinput als beveiligingsprobleem door een IDP – ofwel: vals alarm. Veel ‘normale’ sensorinput heeft de potentie om gerelateerd te zijn aan een aanval, maar is dat niet altijd. Evengoed wordt het door veel IDPs als beveiligingsprobleem opgemerkt. Het doel van IDP-ontwikkelaars is om het aantal false positives zoveel mogelijk terug te dringen; hoe meer false positives, hoe minder vertrouwen een beheerder of organisatie zal hebben in het IDP-systeem. Een false positive percentage van 90% of meer is niet ongebruikelijk bij intrusion detection systemen die geen mechanisme implementeren om de melding te verifiëren [King1], [MAFTIA2], mede afhankelijk van de afstemming van de IDS/IPS op de omgeving waarin de sensor is geplaatst. Verificatie vindt typisch ofwel *passief* plaats door terug te koppelen met actuele inventories van hardware, software en bekende kwetsbaarheden (kan de waargenomen exploit überhaupt wel impact hebben op het aangevallen systeem? – bijv. een Apache chunked exploit die wordt uitgevoerd op een Microsoft IIS server), ofwel *actief* door (near) real-time terug te koppelen met het aangevallen systeem (de sensor vraagt dan bijv. de actieve processen op bij het systeem). De aanwezigheid van dergelijke mechanismen is een prima selectiecriterium zijn bij productkeuze.

Een false negative betreft het onjuist of ongewenst *uitblijven* van beoordeling van sensorinput als beveiligingsprobleem door een IDP. De meeste false negatives hebben tot gevolg dat bedreigingen die wél op een infrastructuur aanwezig zijn, níet worden opgemerkt. Het doel van IDP-ontwikkelaars is om ook het aantal false negatives zoveel

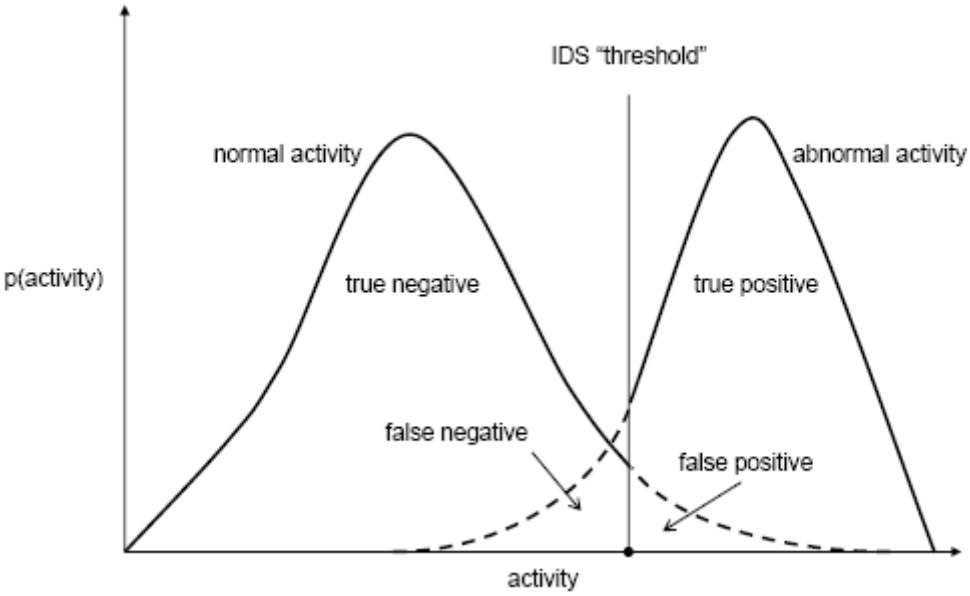
mogelijk terug te dringen; hoe meer false negatives, hoe minder vertrouwen een beheerder of organisatie zal hebben in het IDP-systeem. De tegenhangers van false positives en false negatives zijn *true positives* en *true negatives*; de juiste en gewenste beoordelingen. In een schematische weergave [MAFTIA1]:



Zojuist werden de kwalificaties *onjuist* en *ongewenst* met opzet apart gebruikt. Een *onjuiste* beoordeling betreft een fout of gebrek in de detectie en kan (behoudens uitzonderingen) worden opgelost door het algoritme of de signaturen te verbeteren – een voorbeeld van een onjuiste beoordeling is het niet herkennen van een zero-day exploit (false negative). Met een *ongewenste* beoordeling wordt een beoordeling bedoeld die in principe correct is, maar gezien de specifieke infrastructuur waarin de sensor is geplaatst anders had moeten worden beoordeeld – een voorbeeld van een ongewenste beoordeling is een melding van een exploit waarvoor de infrastructuur niet kwetsbaar is (false positive). Een sensor die ‘aware’ is van zijn infrastructuur zal veel minder false positives geven [SFocus2], [Valeur1].

Volgens [OSSIM1] zijn bij de beoordeling van sensorinput – dus, bij de detectie – twee eigenschappen van belang: gevoeligheid en volledigheid. De gevoeligheid staat in lineair verband met false positives; hoe gevoeliger de detector, hoe hoger het aantal false positives. De volledigheid betreft de mate waarin een sensor in staat is om beveiligingsproblemen te herkennen en staat in omgekeerd verband met false negatives; hoe vollediger de detectie, hoe lager het aantal false negatives. De gevoeligheid kan middels tuning worden geoptimaliseerd als de sensor eenmaal is geplaatst. In de onderstaande grafiek is de gevoeligheid weergegeven als “IDS threshold” en is te zien hoe die eigenschap relateert aan de overlap tussen “normal activity” en “abnormal activity” bepaalt [MAFTIA1]:

(z.o.z.)



Door de threshold naar links te schuiven zal een groter deel van die overlap resulteren in false positives, maar worden false negatives verminderd – en vice versa.

De medewerkers die het beheer gaan uitvoeren op het IDP-systeem zullen moeten worden getraind in de configuratie en tuning; de medewerkers die het IDP-systeem gaan gebruiken voor toezicht zullen moeten worden getraind om de overgebleven false positives te herkennen en te negeren en adequaat te reageren op 'echte' meldingen.

2.4.2 Incident response

Als een IDP-systeem een terechte melding geeft van een inbraak dan zal iemand moeten reageren. Het moet helder zijn wie de verantwoordelijkheid draagt voor (tijdige) reactie en welke procedure moet worden doorlopen. Zulke incident response richtlijnen moeten worden vastgelegd voordat een IDP-systeem wordt geïmplementeerd [Innella2].

Zie Bijlage 9: Incident Response Flowchart voor een voorbeeld van een procedure voor incident response.

2.4.3 Praktische problemen

Elke sensor moet meldingen kunnen sturen naar een manager en dus kunnen communiceren. Afhankelijk van de gemiddelde hoeveelheid false positives en het aantal benodigde sensors kan de benodigde bandbreedte snel oplopen. IDP mag de normale productieprocessen niet in de weg zitten, dus zullen er maatregelen moeten worden genomen om overbelasting van het productienetwerk te voorkomen (bijvoorbeeld door gebruik van een fysiek gescheiden netwerk voor IDP-meldingen). Geografische verspreiding van de sensors betekent tijdrovende beheer-op-locatie, topologische verspreiding van sensors betekent extra complexiteit bij het opzetten van communicatiekanalen tussen sensors en managers. Het tunen en onderhouden van de configuratie van IDP is bepaald geen sinecure en vereist veel specifieke kennis van de infrastructuur.

2.4.4 De meerwaarde van IDS vs IPS

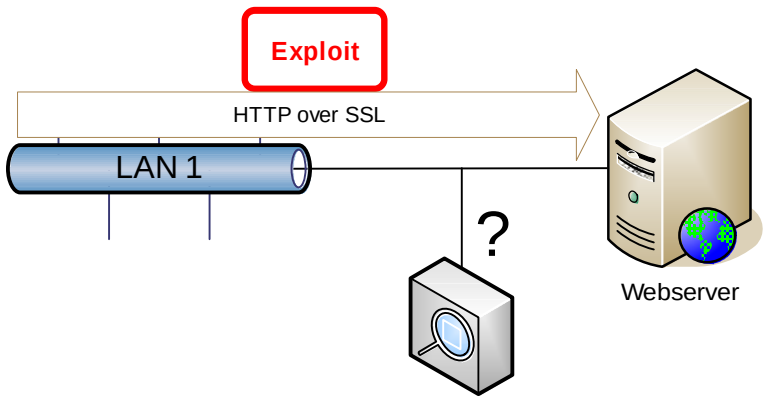
IDSs vormen ‘slechts’ een complementaire, facultatieve laag in de beveiliging die geen werkelijke bescherming biedt, maar waarvoor wel bedrijfsprocessen moeten worden aangepast of ingericht (toezicht, incident response). Een beveiligingsspecialist zal het nut van IDS inzien, maar veel budgethouders zien liever een maatregel die de infrastructuur (lees: bedrijfsvoering) ook werkelijk *beschermt*. In zo’n situatie is er misschien alleen draagvlak voor IPS, maar de impact van IPS is zo groot dat zelfs de beveiliger dat misschien niet aandurft en er dus geen enkele IDP-maatregel wordt gekozen.

2.4.5 Afwijking vereist norm

Beleid en normenkaders gaan per definitie vooraf aan succesvolle implementatie van IDP-maatregelen. Om een IPS te implementeren die werkt op basis van afwijkingen in gebruikspatronen dient eerst het normale gebruikspatroon bekend te zijn. Dat betekent dat van alle gebruikers en systemen in kaart moet worden gebracht welke netwerkverbindingen worden gebruikt, waarvoor die worden gebruikt en hoe vaak die worden gebruikt. Op basis van dat overzicht moet een norm worden vastgesteld, die vervolgens moet worden ingevoerd bij het IPS. Het vaststellen van die norm zal bij veel organisaties een behoorlijke klus zijn en wellicht dodelijk voor de effectiviteit van de preventie. Bij een te scherpe norm zullen veel false positives worden gegenereerd; het is erg complex om ‘normaal gedrag’ vast te stellen.

2.4.6 Versleutelde gegevens

Een ander probleem – dat in een eerdere paragraaf al even aan de orde is geweest – is de onmogelijkheid van een sensor om versleutelde gegevens te screenen. Als een exploit op een webapplicatie over een versleutelde verbinding wordt verstuurd zal een netwerk sensor die exploit bijvoorbeeld niet herkennen:



Deze netwerk IDS sensor
ziet versleuteld verkeer
en zal de exploit niet detecteren

Om de exploit in het bovenstaande voorbeeld tóch te kunnen detecteren zijn er drie mogelijkheden:

1. de netwerk sensor voorzien van de privésleutel van de webserver, zodat de sensor het verkeer zelf kan ontsleutelen en alsnog kan screenen (resulterend in complexere beheerprocedures en een bepaalde performance impact op de sensor);

2. de SSL-verbinding laten termineren door een SSL-concentrator en de netwerk sensor het verkeer tussen de concentrator en de webserver laten screenen (resulterend in verminderde vertrouwelijkheid en ongewenste aanpassingen in de productieomgeving);
3. de webserver voorzien van een applicatiesensor die inhaakt op de processen waar de ontsleuteling plaatsvindt (resulterend in een bepaalde performance impact op de webserver).

Welke keuze de organisatie ook maakt, feit blijft dat NIDP wordt bemoeilijkt door een omgeving waarin versleutelde verbindingen worden gebruikt en dat de IDP in zulke omgevingen dichter naar de eindpunten zal moeten verschuiven.

2.4.7 Ongewenste preventie

Ter benadrukking van de gevolgen van false positives: bij een IPS kunnen false positives leiden tot Denial of Service aan legitieme eindgebruikers. Bij een NIPS zal legitiem netwerkverkeer worden geblokkeerd, bij een HIPS of AIPS zal toegang tot een (informatie)systeem worden ontzegd aan een legitieme gebruiker. Bij een IDS ondervinden eindgebruikers geen gevolgen van false positives, bij een IPS *wel* (althans, zolang de preventiefunctionaliteit van de IPS is ingeschakeld). Het is essentieel dit te beseffen alvorens IDP te implementeren. Het mechanisme dat een IPS gebruikt voor de detectie en blokkade behoort bekend te zijn, zodat een organisatie zelf kan bepalen of de IPS voor hun infrastructuur geschikt is; een black box IDP-systeem vormt in theorie dus zelf een bedreiging voor de infrastructuur.

2.5 Conclusie

IDP is een complementaire laag in een beveiligingsarchitectuur, omgeven door technische en beheermatige problemen. IDS werkt ‘slechts’ als detectieve maatregel, waardoor de toegevoegde waarde niet altijd helder is voor buitenstaanders. IPS werkt als preventieve maatregel, maar kan bij onzorgvuldige configuratie tot Denial-of-Service leiden aan legitieme gebruikers. Soms schaffen organisaties IPS aan, maar wordt de preventiefunctionaliteit niet ingeschakeld omdat de beheerder uitsluiting van een dergelijk ricochet niet denkt te kunnen waarborgen – waardoor in werkelijkheid dus alsnog sprake is van ‘slechts’ een detectieve maatregel. Geografische verspreiding van IDP-sensors impliceert tijdrovende beheer-op-locatie, topologische verspreiding impliceert extra aandacht voor het opzetten van communicatiekanalen tussen de sensors en de managers.

Een voorwaarde voor effectieve anomaly-based detectie is een helder gespecificeerde norm waarin staat welke informatiesystemen er zijn, welke netwerkverbindingen worden opgezet en wie vanaf welke locatie verbinding mag maken. De effectiviteit van pattern-based detectie is afhankelijk van de kwaliteit en actualiteit van de signaturen.

Pattern-based detection kan als volgt worden getypeerd:

Weinig false positives / Detecteert alleen bekende aanvallen / Wat mag níet?

Anomaly-based detection kan als volgt worden getypeerd:

Veel false positives / Detecteert afwijkingen op norm / Wat mag wél?

Er zijn verificatiemechanismen waarmee IDP-meldingen kunnen worden geverifieerd, zodat het aantal false positives kan worden verminderd. Bij *passieve verificatie* koppelt een IDP-systeem terug met hardware, software en vulnerability inventories om te controleren of een aangevallen systeem überhaupt wel kwetsbaar is voor de uitgevoerde aanval. Bij *actieve verificatie* wordt het aangevallen systeem (near) real-time uitgevraagd om de veronderstelde inbraak te verifiëren; daarbij worden bijvoorbeeld de actieve processen opgevraagd. Indien de melding is gefalsifieerd zal er hooguit een melding worden gegenereerd met een lage prioriteit.

In omgevingen waar versleuteling wordt gebruikt zullen netwerksensors moeten worden gecombineerd met host- of applicatiesensors. Hoewel er standaarden in ontwikkeling zijn is integratie tussen IDP-producten van verschillende leveranciers vooralsnog moeilijk, zo niet onmogelijk.

Hoewel IPS in theorie een heldere, voorgedefinieerde norm vereist, zijn er anno 2005 zowel HIPS als NIPS producten op de markt waarvan de leverancier claimen dat ze volledig ‘zelflerend’ zijn, weinig tot geen onderhoud vereisen, waarvoor geen signatures hoeven te worden bijgehouden en die ook nog eens accuraat zouden zijn. Zulke systemen werken op basis van statistische en/of karakteristieke gedragskenmerken, zoals besproken in H2.3.2. De drempels (wat is normaal en wat niet) worden aangeleerd vanaf het moment dat het product in gebruik wordt genomen. Voorwaarde is wel dat het product niet in gebruik wordt genomen in een gecompromitteerde productieomgeving, want in dat geval zal de sensor het verkeerde gedrag als ‘normaal’ aanleren en alsnog geen bescherming bieden. Bij NIPSs moet meestal vooraf worden opgegeven welke systemen dienen te worden beschermd, op basis van combinaties van IP-adressen en poortnummers; vaak wordt daarbij aangegeven welke functie een bepaald systeem heeft, zodat de NIPS zich enigszins ‘bewust’ is van zijn omgeving. HIPS en NIPS kunnen de infrastructuur helpen te beschermen tegen *onbekende* bedreigingen en vullen daarmee weer een extra laag van de beveiligingsarchitectuur. Er is geen wetenschappelijk onderzoek gedaan naar die producten, maar er zijn wel enkele reviews beschikbaar:

NFR Security’s Sentivist IPS (november 2004):
http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss506_art1051,00.html

Prevx home IPS (19 september 2004):
http://netsecurity.about.com/od/readproductreviews/fr/aapr091904.htm

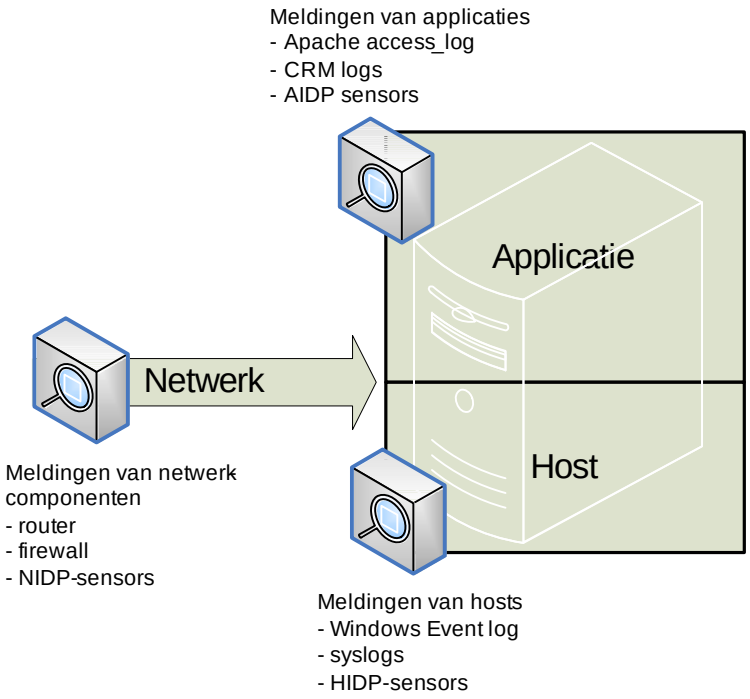
Review: Intrusion-Prevention Systems (14 januari 2005):
http://www.systemsmanagementpipeline.com/showArticle.jhtml?articleID=159400004

Intrusion detection systems reviewed (24 augustus 2004):
http://www.zdnet.com.au/insight/security/0,39023764,39157029,00.htm

3. Consolidatie van logging

Onder *consolidatie van logging* wordt verstaan: “gecentraliseerde verwerking van loggegevens uit een heterogene infrastructuur”. Een moderne ICT-infrastructuur omvat uiteenlopende componenten die allemaal meldingen (kunnen) genereren, waarvan een deel vanuit beveiligingsoogpunt interessant kan zijn. Applicaties als Apache, anti-virus en anti-malware systemen, hosts als Unix en Windows, netwerkcomponenten als routers, firewalls, VPN appliances, et cetera – en ook IDP systemen. Door meldingen (die normaliter bijvoorbeeld in een logbestand worden opgeslagen) van verschillende componenten te centraliseren en te correleren kan meer en betere beveiligingsinformatie worden verkregen.

Het lagenmodel kan ook hier weer worden toegepast:



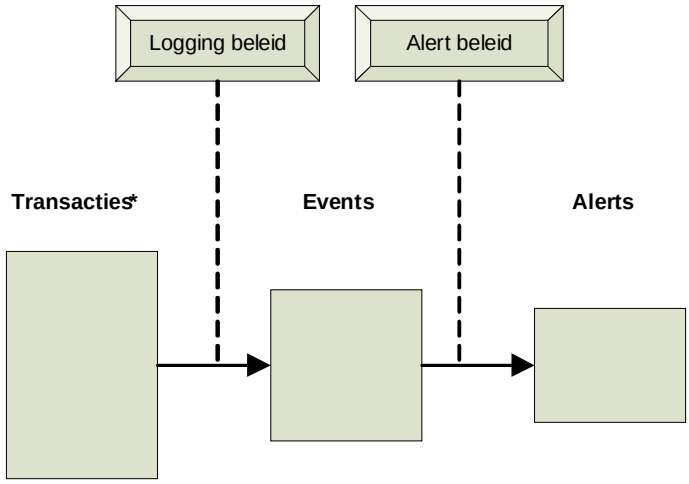
In het vorige hoofdstuk is intrusion detection vooral afzonderlijk besproken per laag; in de loop van dit hoofdstuk zal blijken dat correlatie van gegevens van alle lagen het proces van intrusion detection zou kunnen verbeteren.

3.1 Introductie van logging

Een *transactie*, zoals hier bedoeld, is de kleinste logische verwerkingseenheid waarvan een systeem of component het voorkomen kan registreren of laten registreren, typisch in een logboek. Een geregistreerde transactie heet een *event*. In het *logging beleid* staat gespecificeerd welke transacties wel en eventueel welke transacties niet moeten worden geregistreerd. Het logging beleid wordt primair opgesteld vanuit de tactische bedrijfsprocessen, waarbij rekening wordt gehouden met externe factoren – normenkaders

van toezichthouders, wet- en regelgeving, security baselines, et cetera. Bepaalde events of combinaties van events zijn significant en geven aanleiding tot handelen; daarvan wordt tijdens het *loganalyse* proces een *alert* gegenereerd. Welke (combinaties van) events een *alert* veroorzaken staat gespecificeerd in het *alerting beleid*. Het alerting beleid wordt primair opgesteld vanuit de operationele processen, waarbij de keuzes vooral worden bepaald door relevantie en impact op die operationele processen.

Bovengenoemde is samengevat in het onderstaande schema:

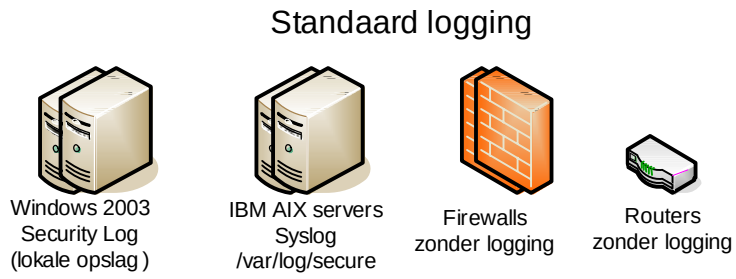


Logging en loganalyse kunnen allerlei bedrijfsprocessen ondersteunen – voor capaciteitsbeheer kan de analyse gericht zijn op de gebruikte systeembronnen (er zou een alert kunnen worden gegenereerd wanneer de harde schijf van een server 95% vol is); voor beschikbaarheidsbeheer kan de analyse gericht zijn op o.a. de bereikbaarheid van componenten (er zou een alert kunnen worden gegenereerd als een router is uitgevallen); voor kostenbeheer kan de analyse gericht zijn op het gebruik per afdeling, et cetera. In dit onderzoek staan logging en loganalyse centraal als functie voor beveiligingsbeheer.

Transacties kunnen van verschillende aard zijn. Voor dit onderzoek wordt onderscheid gemaakt tussen beveiligingsgerelateerde en niet-beveiligingsgerelateerde transacties, waarbij eerstgenoemde de primaire focus heeft. Logging van beveiligingsgerelateerde transacties kan van belang zijn bij forensisch onderzoek naar aanleiding van een inbraak op de infrastructuur, maar kan de organisatie ook een beeld geven van de bedreigingen die op de infrastructuur spelen.

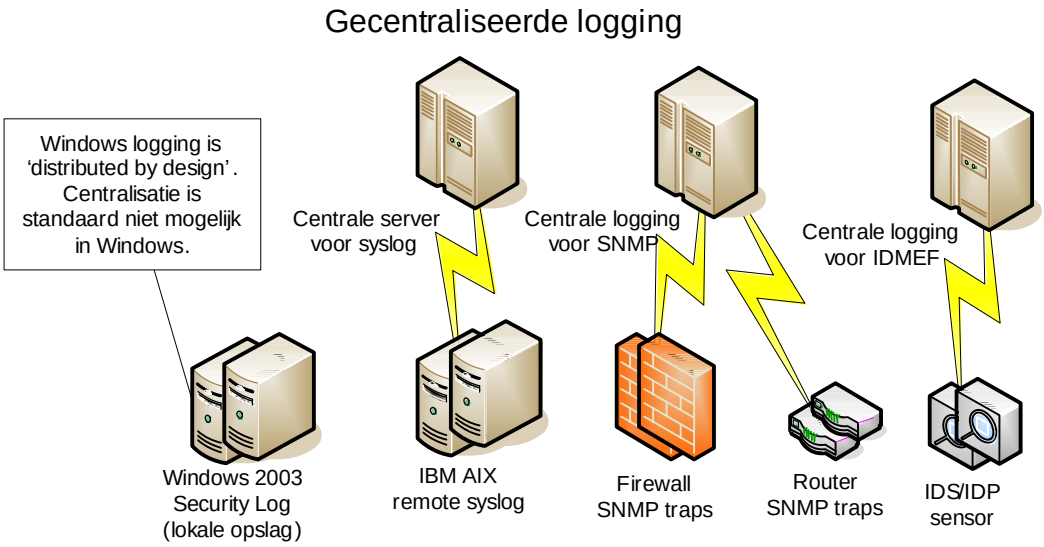
Dit hoofdstuk gaat over de wijze waarop events kunnen worden verzameld voor verdere verwerking. Ter inleiding volgt eerst een korte vergelijking tussen standaard logging, gecentraliseerde logging en geconsolideerde logging. Hierbij zal zoveel mogelijk worden geabstraheerd van het toepassingsgebied beveiliging; wel zullen de voorbeelden op dat gebied worden gericht.

3.1.1 Standaard logging



Bij standaard logging, zoals typisch ingericht bij versgeïnstalleerde besturingssystemen en Commercial Off The Shelf (COTS) producten is het logging beleid in het beste geval minimaal en worden alleen lokaal events vastgelegd. Elk component moet apart worden benaderd om de events te kunnen raadplegen en de grote hoeveelheid events maakt het lastig om zelfs in één enkel component inzicht te krijgen. En áls er al een geautomatiseerde analyse op de meldingen zou worden uitgevoerd dan zal het inzicht altijd beperkt zijn tot dat individuele component. In een grote infrastructuur is het onmogelijk om met deze manier van logging zicht te krijgen op de status van de infrastructuur als geheel.

3.1.2 Gecentraliseerde logging



Bij gecentraliseerde logging worden de events van *homogene componenten* op één locatie opgeslagen. Onder 'homogene componenten' worden groepen van componenten verstaan die events in hetzelfde formaat aanbieden. Er zijn dus verschillende formaten en protocollen waarin events kunnen worden aangeboden:

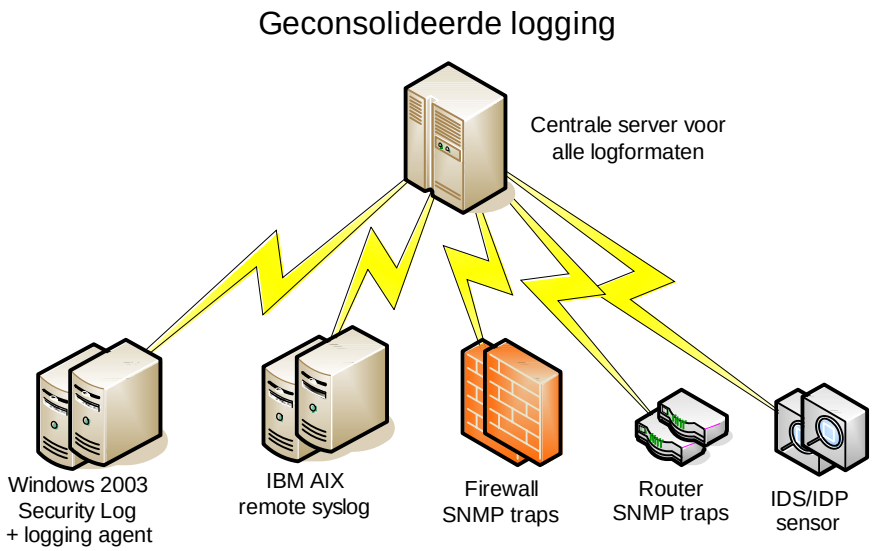
- Syslog (Unix-achtigen)
- SNMP (netwerkcomponenten)

- Microsoft Windows Event Log over WMI [3]
- CheckPoint OPSEC LEA (CheckPoint componenten)
- Cisco POP / RDEP (Cisco componenten)
- IDMEF/IDXP (IDP-componenten)
- (…)

De meerwaarde ten opzichte van standaard logging ligt in de mogelijkheid tot *correlatie* van events van verschillende componenten. Bij correlatie worden events van verschillende componenten aan elkaar gerelateerd, om na interpretatie te kunnen leiden tot een (geautomatiseerde) stelling of conclusie over de status van het component of de infrastructuur. In H3.6 wordt dieper ingegaan op de achtergronden van correlatie.

Hoewel gecentraliseerde logging al een beter zicht kan verschaffen op de status van de infrastructuur als geheel, ontbreekt het hierbij nog steeds aan de mogelijkheid om events van *verschillende componentgroepen* met elkaar te kunnen koppelen. De persoon die de centrale consoles in de gaten houdt zal dus zelf rekening moeten houden met de context van de informatie in elke console – een bepaalde groep homogene componenten, dus – en moet zelf eventuele relaties kunnen herkennen.

3.1.3 Geconsolideerde logging



Bij geconsolideerde logging worden events van zoveel mogelijk *heterogene componenten* op één centrale locatie opgeslagen. Hierbij wordt een vertaalslag gemaakt op het formaat waarin events door elk component worden aangeleverd (*normalisatie*, zie H3.5) of door op elk individueel systeem software te plaatsen die de events in het juiste formaat aanlevert

[3] De logging faciliteit van Microsoft Windows NT/2k is 'distributed by design'. Het logboek wordt lokaal vastgelegd in binair formaat. Het is zonder aanvullende maatregelen alleen mogelijk om de events via Windows Management Instrumentation (WMI) te raadplegen (pull), maar niet om de meldingen automatisch naar een centrale logging faciliteit te sturen (push). Om dat tóch mogelijk te maken is aanvullende software nodig, zoals eIQ System Analyzer (www.eiqnetworks.com) of het onder GPL vrijelijk beschikbare NTSysLog (ntsyslog.sourceforge.net).

(*wrappers* of *agents*). Vanwege de potentie van geconsolideerde logging – namelijk, een *360-degree view* over de gehele, heterogene infrastructuur – heeft deze vorm de voorkeur vanuit zowel regulier systeem- en netwerkbeheer als vanuit beveiligingsbeheer.

3.1.4 Schaalbaarheid

De omvang en hoeveelheid van de events verschilt per component en is vooral afhankelijk van configuratie-instellingen (de implementatie van het logging beleid) en gebruikslast. De subjecten die vanuit beveiligingsoogpunt interessant zijn – productieservers, firewalls – hebben vaak een hoge gebruikslast en genereren veel events; puur centrale logging van meerdere soortgelijke subjecten zou dus veel overhead veroorzaken op het netwerk [InfoWorld1]. In de architectuur van een modern logging systeem zullen dan ook maatregelen zijn geïmplementeerd om het bandbreedtegebruik te beperken of te reduceren (gefedereerde aggregatie, correlatie of interpretatie, compressie, et cetera). Het aantal events per seconde is zelfs een metriek die wordt gebruikt bij productselectie; de consolidatie-oplossing moet immers in staat zijn om álle events die op een infrastructuur worden gegenereerd af te handelen [Angelino1]. Evenals bij IDP is het bij logging gebruikelijk om hiërarchische architecturen te gebruiken, waarbij tussenliggende nodes aggregatie en filtering uitvoeren en slechts een beperkt aantal events (voor verdere analyse) doorsturen naar hogere nodes.

3.2 Beveiligingsgerelateerde events

Per component zullen de events die vanuit beveiligingsoogpunt interessant is verschillen, maar in de meeste gevallen gaat het om events die te maken hebben met:

1. toegangscontrole
    a. authenticatie
    b. autorisatie
2. monitoring
    a. beschikbaarheid
    b. afwijkingen op normaal gebruik

Voorbeelden:
- events betreffende inlogpogingen **à** dictionary/brute force attacks
- events betreffende Denial of Service attacks
- events betreffende ongeautoriseerde scans (poortscan, ping sweep)
- events betreffende ongeautoriseerde toegang tot geprivilegieerde accounts
- events betreffende netwerkverkeer dat niet bij geautoriseerde applicaties/services hoort
- events betreffende virus en malware meldingen
- events betreffende het opstarten of afsluiten van een beveiligingssysteem
- events betreffende de beschikbaarheid van netwerkservices (Kerberos, …)

3.3 Niet-beveiligingsgerelateerde events

Voor dit soort events geldt eveneens dat ze verschillen per component, maar er valt te denken aan events betreffende:

- bandbreedtegebruik
- gemiddelde CPU-belasting
- vrije schijfruimte
- geautomatiseerde OS-taken (cronjob gestart, defragmentatie voltooid, …)

3.4 De relatie tussen geconsolideerde logging en IDS

In algemeen gebruik lijkt de term ‘intrusion detection’ voornamelijk te worden geassocieerd met het screenen van netwerkverkeer; IDS wordt in die zin bijna synoniem gesteld aan NIDS, terwijl de oorsprong van IDS eigenlijk juist ligt in auditing van systeemlogs – daarbij wordt verwezen naar het rapport *Computer Security Threat Monitoring and Surveillance* dat James Anderson in 1980 opstelde in opdracht van de US Air Force [Anderson1] en het onderzoek dat Dorothy Denning tussen 1983 en 1987 in opdracht van de US Navy heeft uitgevoerd en dat resulteerde in het eerste *Intrusion Detection Expert System* [Denning1]. Intrusion detection, zoals hier bedoeld, is een beveiligingsfunctie die op verschillende lagen in een infrastructuur kan worden ingezet; applicatie, host en netwerk.

Geconsolideerde logging verwijst naar consolidatie van *alle* soorten events in een infrastructuur, dus ook naar niet-beveiligingsgerelateerde events. Het gaat hier echter niet om het consolideren van volledige OS-logs, applicatielogs en andere logs. Enkele jaren geleden is uit groeiend besef dat consolidatie van beveiligingsgerelateerde events een hele aparte discipline is een nieuwe term verzonnen: *security information management* (kortweg *SIM*) [Keldsen1], [Chuvakin1]. Een mogelijke definitie van SIM software [NWFusion1]:

"Software designed to automate the collection of event log data from security devices and helping users make sense of it through a common management console.

SIM products use data aggregation and event correlation features similar to those of network-management software and applies them to event logs generated from security devices such as firewalls, proxy servers, intrusion-detection systems and antivirus software. What's more, SIM products can normalize data - that is, they can translate Cisco and Check Point Software alerts, for example, into a common format so the data can be correlated.

Like network-management software, SIM tools generally consist of server software, agents installed either on servers or security devices, and a central management console."

Citaat uit een uitnodiging voor een webcast over SIM (medio 2005):
“What: Security Information Management solutions (SIMs) have moved beyond

> *merely aggregating log files for a small set of devices and are taking a more inclusive approach to managing the risk lifecycle. These systems perform both threat detection and vulnerability scanning, correlate threats to identified vulnerabilities, prioritize mitigation workflows based on risk severity and applicable regulations, and provide a "big red button" capacity that allows real-time threat and incident response."*

Vanaf hier zal niet langer worden gesproken over geconsolideerde logging, maar specifiek over SIM (geconsolideerde logging in beveiligingscontext). Gene Gomez van Prelude-IDS definieerde ze als volgt [Gomez1]:

"IDS: A system that checks for intrusion events using a single approach (HIDS, NIDS, log parsers, etc).
SIM: A system that collects data from a variety of IDS systems and centralizes (and maybe correlates) it into a single console"

Omdat IDS niet de enige input is voor SIM wordt die vergelijking hier iets aangepast:

1. SIM is gericht op een totaalbeeld van de beveiligingsstatus van een infrastructuur door het consolideren en correleren van events van uiteenlopende security devices, terwijl intrusion detection is gericht op het herkennen van één bedreiging/incident;
2. Intrusion detection kan één input zijn voor SIM.

Dr. Anton Chuvakin typeerde SIM al eens als *meta-IDS* [Chuvakin1]:
"SIM (Security Information Management) is the "discipline" that will solve the correlation security event data challenge. (…) a SIM function as a kind of meta-IDS, operating on a higher-level data: log records as opposed to packet (streams)."

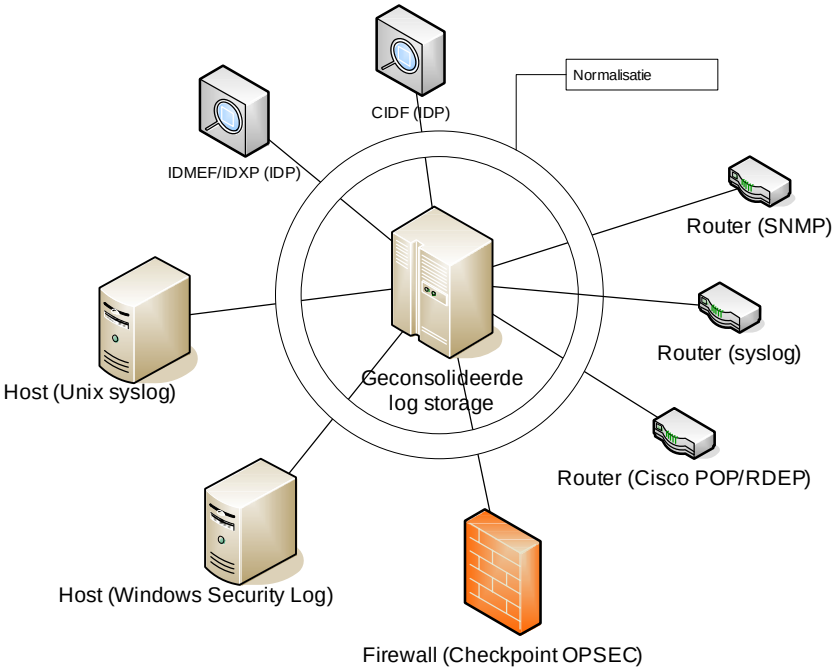
Er zijn al enkele producten beschikbaar die het SIM-probleem adresseren, waaronder ArcSight's ESM, Open Services Security Threat Manager en netForensics' SIM.

De termen zijn verwarrend en overvloedig, maar het doel van SIM is simpel: het samenbrengen en analyseren van beveiligingsgerelateerde events uit heterogene delen van de infrastructuur om een totaalbeeld te krijgen van de beveiligingsstatus van die infrastructuur.

3.5 Consolidatie nader beschouwd

Consolidatie, in deze context nauwkeuriger bekend als *multisensor data fusion*, is gericht op het verzamelen van events uit heterogene systemen [DeBoer1]. Een event is een set van attributen waarmee de afzender een bepaald feit over zichzelf kenbaar wil maken, omdat het beleid van een organisatie – vertaald naar configuratie-instellingen – dat voorschrijft.

Om meldingen van verschillende bronnen in verschillende formaten te kunnen centraliseren zal elk event eerst moeten worden *genormaliseerd*:



Onder *normalisatie* wordt de vertaling verstaan van een inkomende melding naar een (standaard)formaat dat het SIM systeem begrijpt. Daarbij zijn twee aandachtspunten [Valeur1]:

1. syntaxis
2. semantiek

De syntaxis betreft de volgorde van attributen en de gegevenstypen die worden gebruikt om feiten te beschrijven in events; daarbij worden attributen 'gemapt' naar het standaardformaat van het SIM systeem (veld 1 **à** bron IP, veld 2 **à** doel IP, eventuele typeconversies). De semantiek betreft de betekenis van attributen en is veel complexer; de betekenis van zelfs simpele attributen kan verschillen, bijvoorbeeld afhankelijk van de topologische context en de betekenis die een fabrikant aan zo'n attribuut heeft gegeven. Bij het normalisatieproces zal dus ook rekening moeten worden gehouden met de betekenis van attributen; een ontologie voor intrusion detection zal – mits algemeen geaccepteerd en ondersteund – in de toekomst wellicht helpen dit probleem op te lossen [Undercoffer1], [Valeur1].

De normalisatiestap impliceert het gebruik van een aparte wrapper of procedure voor elk eventformaat dat in een infrastructuur voorkomt. De focus van het SIM systeem wordt daardoor beperkt tot die componenten waarvoor expliciet ondersteuning wordt aangeboden, waarmee het beoogde doel – een *totaalbeeld* van de infrastructuur – eigenlijk voorbij wordt gestreefd. Er zijn enkele ontwikkelingen op dat gebied; in H2.2.7 werd bijvoorbeeld al gerefereerd aan de IDXP en IDMEF standaarden. Hoewel prima bruikbaar als standaardformaten voor IDP, zijn die standaarden tegelijkertijd *alleen* geschikt voor IDP en dus niet bruikbaar voor consolidatie van events van andersoortige componenten als firewalls, routers, anti-virus en VPNs. Enkele andere initiatieven waarin dit normalisatieprobleem wordt geadresseerd zijn het proprietaire *Symantec Enterprise*

Security Architecture (kortweg *SESA*) van Symantec [Symantec1] en het *Security Events* schema dat sinds juni 2004 binnen het *Security Protection Model* onderdeel uitmaakt van het *Common Information Model* van de Distributed Management Task Force [DMTF1]. Aan het DMTF nemen onder andere Microsoft, Cisco, Novell, IBM en (!) Symantec deel (Windows Management Instrumentation is bijvoorbeeld compliant met CIM). Beide initiatieven beogen integratie van heterogene (beveiligings)systemen en hebben de potentie om te voorzien in het gewenste totaalbeeld. Symantec ontwikkelt daarbij sec vanuit beveiligingsoptiek, het DMTF ontwikkelt vanuit 'general systems management'.

Symantec heeft al een heel assortiment aan producten die op SESA zijn gebaseerd (niet in de laatste plaats dankzij expertise uit overnames van @Stake, Axent, Recourse Technologies en Manhunt/Mantrap). DMTF is veelbelovend, maar vooralsnog nergens geïmplementeerd. Het is onduidelijk welke kant DMTF op zal gaan met het Security Events schema.

Een ander recent initiatief voor consolidatie van beveiligingsgerelateerde events is UCLog van de University of Illinois in Urbana-Champaign [Li1]. UCLog bespreekt *unified logging* als een soort intrusion detection middleware waaraan verschillende monitors kunnen worden toegevoegd om verschillende soorten event logs te analyseren (kernel logs, netwerk logs, filesystem logs). Er is nog geen publiek beschikbare implementatie van UCLog.

3.6 Correlatie nader beschouwd

Correlatie is het op verschillende manieren associëren van events of alerts om relaties te ontdekken [Endorf1]. Correlatie heeft verschillende doelen [Debar4]:

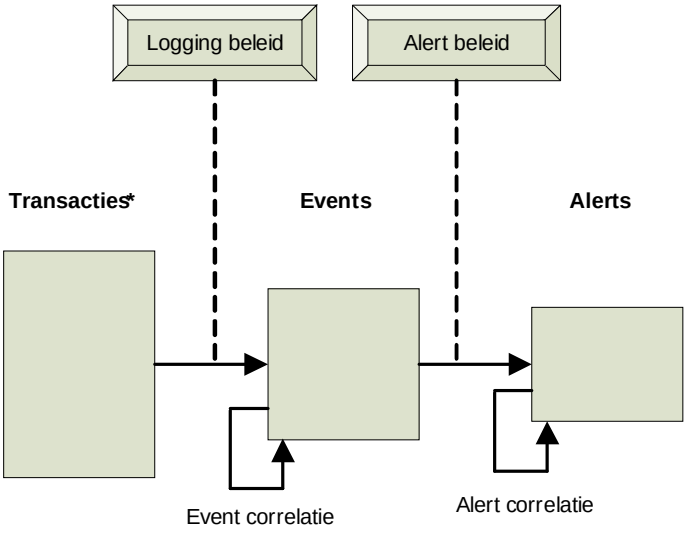
1. reductie van het aantal meldingen;
    a. eliminatie (wegfilteren van de eerste ruis);
    b. fusie (samensmelten van dezelfde meldingen van verschillende sensors);
    c. aggregatie (groeperen van gelijksoortige meldingen);
    d. synthese (logische verbanden leggen tussen meldingen);
2. verbeterde diagnose;
    a. type activiteit (welk soort aanval? geen aanval?);
    b. relevantie (is de infrastructuur überhaupt kwetsbaar?);
    c. verificatie (is de aanval geslaagd?);
3. activity tracking;
    a. informatie die is uitgelekt naar de tegenstanders;
    b. informatie over de tegenstanders.

Er wordt onderscheid gemaakt tussen correlatie van *events* en correlatie van *alerts* [Gorton1]:

"*Intrusion event correlation refers to the interpretation, combination, and analysis of neutral events from all available sources, about target system activity for the purposes of intrusion detection and response.*"

"Intrusion alert correlation refers to the interpretation, combination, and analysis of intrusion alerts, together with information external to the intrusion detection system, with the purpose of intrusion alert refinement and intrusion scenario building."

Samengevoegd met het eerdere logging schema:



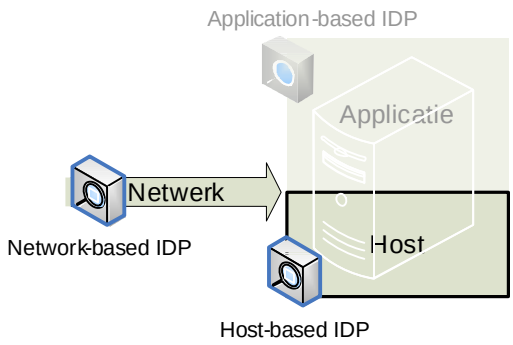
Vanaf hier zal de focus liggen op correlatie van *alerts*, omdat uit die stap (in theorie) de meest waardevolle informatie kan volgen: de reconstructie van een hack scenario dat heeft plaatsgevonden. Typische aandachtsgebieden bij het correleren van alerts [Valeur1]:

- *temporal proximity* (tijd)*;*
  - verhoudingen in timestamps van verschillende alerts kunnen wijzen op causaliteit; deze eigenschap kan helpen bij detectie van *multi-step intrusions* (eerst heeft de aanvaller een covert channel opgezet, toen een interne webserver gehackt via een exploit, daarna een DDoS bot gestart);
- *spatial proximity* (ruimte)*;*
  - correlatie van alerts met hetzelfde doelwit (bijv. doel-IP, doel-poort);
  - correlatie van alerts met dezelfde vermoedelijke veroorzaker (bijv. bron-ID, user-id, proces-id);
  - correlatie op basis van de afkomst van de melding (topologische context en host versus netwerk sensor).

Om de *temporal proximity* te kunnen bepalen dient te tijdsynchronisatie op de verschillende componenten vrij nauwkeurig te zijn; van elk component waarvan de tijd niet synchroon loopt zullen bij correlatie geen verbanden kunnen worden ontdekt in tijd. Correlatie van heterogene logbestanden vergroot de effectiviteit en accuraatheid van intrusion detection en vermindert het aantal false positives. De logica daarachter is als volgt [Yin1]:

- sommige aanvallen verlopen via verschillende componenten en laten sporen achter in logs op die verschillende componenten, dus moeten meerdere logs worden geanalyseerd om een totaalbeeld van zo'n aanval te krijgen;
- verschillende soorten aanvallen zijn beter herkenbaar in verschillende soorten logs – de ene aanval laat meer sporen achter in host logs, de andere aanval in firewall logs;
- het gebruik van verschillende sensors bemoeilijkt het omzeilen van het intrusion detection systeem (zoals door IDS evasion en sensor flooding);
- sommige aanvallen kunnen niet worden gedetecteerd door één log te analyseren;
- correlatie van logbestanden maakt verificatie van een aanval mogelijk en reduceert daarmee het aantal false positives.

Er wordt veel onderzoek verricht naar correlatiemechanismen, waarbij zowel wordt gekeken naar correlatie van homogene als heterogene bronnen. Er is vooral materiaal beschikbaar over correlatie van alerts binnen de netwerklaag (IDS alerts van verschillende netwerk sensors) en correlatie tussen de netwerklaag en de hostlaag (IDS alerts van host en netwerk sensors) [Carey1], [King1], [Kruegel1], [Ning1], [SFocus2], [STAT1], [Valeur1]. Onderzoek waarin correlatie met alerts van applicatie IDS sensors wordt geadresseerd is wat schaarser; alleen in M2D2, een voorgesteld formeel model voor correlatie van IDS meldingen, wordt aan dat gebied gerefereerd [Debar1]. Correlatie van IDS alerts met bijvoorbeeld alerts van anti-malware software of CRM-applicaties lijkt vooralsnog niet mogelijk; het semantische gat is daarvoor te groot en bovendien ontbreekt het aan bruikbare standaarden voor consolidatie van dergelijke alerts. Zowel in de wetenschap als de praktijk is correlatie dus nog voorbehouden tot de host- en netwerklaag:



Huidige theorieën rondom correlatie vallen uiteen in twee categorieën [Yu1]:
1. alert clustering;
2. intention recognition.

Bij alert clustering worden alerts gecorreleerd op basis van overeenkomsten in attributen, zoals bron IP, doel poort, proces-id en user-id [Valdes1], [Cunningham1]. Het doel van alert clustering is *root cause analysis* [Julisch1]. Door gebruik van clustering kan het aantal alerts dat de console bereikt drastisch worden verminderd; de overgebleven alerts zijn bovendien van hogere kwaliteit [Valeur1].

Bij intention recognition (ook bekend als *attack plan recognition*) wordt geprobeerd om op basis van alerts te herleiden (of voorspellen) wat de intentie van de tegenstander is. Als de

beheerder tijdig weet wat de tegenstander van plan lijkt te zijn (multi-step attack) kan hij tijdig adequate maatregelen nemen om escalatie te voorkomen. Enkele voorbeelden zijn correlatie op basis van voorgedefinieerde aanvalsscenario's [Debar2], [Debar3], correlatie op basis van pre- en postcondities [Ning3], [Ning4] en state transition analysis [Kemmerer1], [Payer1], [STAT1].

In de komende paragrafen zullen enkele vormen van correlatie worden toegelicht. De verschillende vormen van correlatie zijn vaak complementair [Valeur1]. De mechanismen die in dit rapport worden besproken zijn allen vormen van *knowledge-based correlation*; bij dergelijke mechanismen is kennis vereist van kwetsbaarheden en aanvalsscenario's. Bij *behaviour-based correlation* is zulke kennis niet vereist, maar worden statistische methoden als Bayes en Granger-Causality gebruikt om causaliteit van meldingen te bepalen [Barbara1], [Qin1]. Er zijn echter nog geen bruikbare implementaties van deze vormen van correlatie, daarom blijven ze in dit rapport verder buiten beschouwing.

3.6.1 Alert clustering

Bij alert clustering worden alerts gegroepeerd op basis van overeenkomsten in hun attributen, waardoor *attack threads* ontstaan. Eén thread bevat alle alerts die aan één aanval gerelateerd lijken te zijn. Elke inkomende alert wordt vergeleken met *alle* bestaande threads maar wordt alleen toegevoegd aan de thread die het 'best' overeenkomt. Belangrijke vragen zijn wélke attributen moeten worden vergeleken, hoe de overeenkomst wordt bepaald en hoe zwaar elk attribuut meeweegt bij die vergelijking. Voorbeelden van te vergelijken attributen zijn de locatie en naam van de betrokken sensor, bron en doel IP-adressen, bron en doel poorten, de bron en doel user id's, het soort aanval en de tijd. Elke attribuut heeft een eigen metriek op basis waarvan de mate van overeenkomst wordt bepaald. Bij IP-adressen kan worden vergeleken met subnets, bij poortscans kan worden gekeken naar overlap van poorten of TCP vlaggen, bij tijd kan worden gekeken naar nabijheid, et cetera. Deze methode wordt *probablistic alert correlation* genoemd en is geïmplementeerd in het EMERALD systeem [Valdes1].

Voor verschillende aanvallen wordt voor verschillende attributen een verschillende mate van overeenkomst verwacht. Die verwachte waarde kan vervolgens meetellen bij de clustering. Het lijkt bijvoorbeeld redelijk om van een SYN flood te verwachten dat er géén overeenkomst is in bron-IP (IP spoofing is immers essentieel bij zo'n aanval – anders zou de aanval met een simpele ACL zijn af te weren); van een portsweep wordt verwacht dat de overeenkomst in bron-IP en doel-poort groot is, maar dat de overeenkomst in doel-IP klein is.

De clusters worden ten slotte samengesmolten (*alert fusion*), waarna een meta-alert wordt gegenereerd die de hele cluster vertegenwoordigt [Cuppens2], [Valeur1], [Yu1].

De kwaliteit en effectiviteit van alert clustering is afhankelijk van parametrisatie van het algoritme; de *similarity matrices* en *similarity expectations* moeten door een expert worden ingesteld, waardoor de mens en zijn kennis hierbij kritieke succesfactoren zijn [Ning4].

3.6.2 Voorgedefinieerde scenario's

Aan deze vorm van correlatie liggen vooraf gedefinieerde aanvalsscenario's ten grondslag [Debar3]. Zulke scenario's kunnen ofwel handmatig door beveiligingsexperts worden gespecificeerd, ofwel automatisch worden aangeleerd door data mining van 'training data sets' (afgetapt hacking verkeer) [Ning4].

Enkele voorbeeldscenario's staan in de onderstaande tabel. Het gaat bij deze voorbeelden om *sjablonen* voor aanvallen; de werkelijke waarde van de attributen verschilt per aanval.

Scenario	Indicatie van kenmerkende attributen
Eén tegenstander valt één aanval uit op één doelwit	Zelfde bron-IP, doel-IP en soort aanval
Eén tegenstander die aanvallen uitvoert vanaf en op één doelwit	Zelfde bron-IP en doel-IP
Een gedistribueerde aanval op één doelwit.	Zelfde doel-IP en soort aanval.
Eén tegenstander die dezelfde aanval op meerdere doelwitten uitvoert	Zelfde bron-IP en soort aanval

De inkomende alerts worden geanalyseerd vanuit deze voorgedefinieerde scenario's, waarbij alerts die samen een bepaald scenario lijken te vormen worden gecorreleerd. Nadeel aan deze manier is dat onbekende aanvalsscenario's niet zullen worden opgemerkt. Recentelijk is in dat kader onderzoek gedaan naar *plan recognition and prediction* op basis van causale netwerken [Qin1]. Van die theorie zijn echter nog geen bruikbare implementaties beschikbaar.

De aanvalsscenario's worden gespecificeerd in declaratieve talen (predikaten) zoals *chronicles formalism* [Debar3], *Attack Scenario Language* [Kruegel1] of LAMBA [Cuppens3]. Evenals bij alert clustering kan alleen worden gecorreleerd op basis van voorkennis – in dit geval kunnen alleen aanvallen worden herkend waarvan een voorgedefinieerd scenario bekend is; onbekende scenario's worden niet herkend.

3.6.3 Pre- en postcondities

Correlatie op basis van pre- en postcondities (ook wel *prerequisites* en *consequences* genoemd) – is gericht op voorwaardelijke relaties tussen alerts. Een preconditie specificeert een noodzakelijke voorwaarde voor een geslaagde aanval. Een postconditie specificeert het mogelijke resultaat van een geslaagde aanval (en wordt daarom ook wel *gevolg* of *consequentie* genoemd). Het correlatiealgoritme zoekt naar paren van alerts waarbij de postconditie van de ene alert overeenkomt met de preconditie van een andere alert; daardoor ontstaat een *(may-)prepare-for* relatie (mits de chronologische volgordelijkheid dat toestaat).

Pre- en postcondities worden – net als aanvalsscenario's – als predikaten gespecificeerd. De combinatie van een alerttype, preconditie en postconditie wordt *hyper-alert* genoemd [Ning3] , [Ning4].

Een hyper-alert wordt als volgt gespecificeerd:

(fact, prerequisite, consequence)

Het veld *fact* specificeert het soort informatie dat het alerttype betreft; het veld *prerequisite* specificeert de voorwaarden waaraan moet worden voldaan, wil de aanval succesvol zijn; het veld *consequence* specificeert de gevolgen van een succesvolle aanval.

Stel, een tegenstander is voor DDoS doeleinden op zoek naar Sun Solaris systemen die een kwetsbare versie van de Sadmind service draaien. Bij exploitatie van die service verkrijgt de tegenstander root-rechten en kan een DDoS daemon worden geïnstalleerd. De hyper-alert voor exploitatie van de SAdmin service wordt als volgt gespecificeerd:

Hyper-alert Type *SadmindBufferOverflow* =
({*VictimIP, VictimPort}*,
ExistHost(VictimIP)^VulnerableSadmind(VictimIP),
GainRootAccess(VictimIP))

De *facts* zijn het doel-IP en de doel-poort. De *prerequisites* zijn dat het doelsysteem bestaat en een kwetsbare versie van Sadmind draait. De *consequence* is dat de tegenstander root-rechten verkrijgt op het doelsysteem.

De aanval bestaat uit verschillende stappen die allemaal alerts veroorzaken. Correlatie van die alerts resulteert in een gerichte acyclische graaf, waarvan de nodes de meldingen zijn en de leaves de *(may-)prepare-for* relaties voorstellen. Op het moment dat de melding van de buffer overflow exploit op Sadmind binnenkomt ziet die graaf er als volg uit [Ning3]:

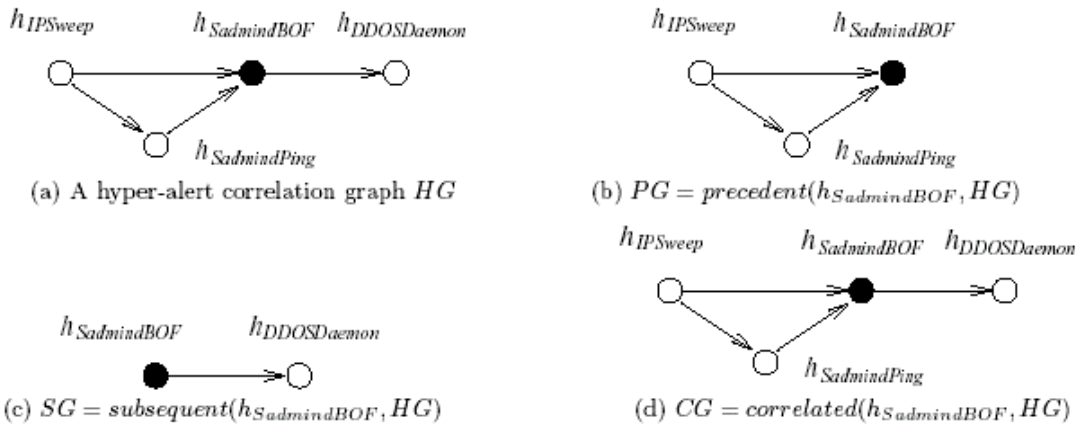


Figure 1: Hyper-alerts correlation graphs

Uit (a) zou blijken dat de aanval als volgt is uitgevoerd:

1. tegenstander pingt een IP reeks (hIPSweep);
2. tegenstander controleert de systemen die antwoorden op aanwezigheid van SAdmin service (hSadmindPing, optioneel);

3. tegenstander exploiteert de SAdmin service (hSadminBOF, instantie van het hyper-alert type *SadmindBufferOverflow*);
4. tegenstander *prepares-for* installatie van een DDoS daemon (hDDOSDaemon).

Stap 4 betreft een voorspelling (!); de postconditie van hSadmindBOF vervult in dit voorbeeld de preconditie van hDDOSDaemon (root-rechten op een systeem). Naar mate de complexiteit van de aanval toeneemt en er meer hyper-alert typen zijn groeit ook de resulterende graaf [Ning3]:

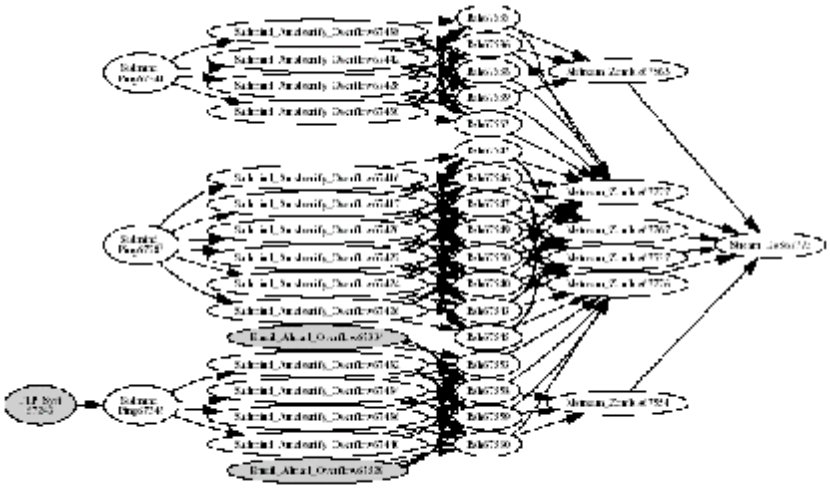


Figure 3: The (only) hyper-alert correlation graph discovered in the inside network traffic of LLDOS 1.0.

Deze benadering van correlatie is gelijktijdig onderzocht door verschillende onafhankelijke groepen, waaronder Templeton en Levitt (JIGSAW, 2000-2001), Cuppens (MIRADOR, 2002) en Ning, Cui en Reeves (TIAA, 2002-2005) [Templeton1], [Cuppens3], [Ning5].

Evenals bij alert clustering en aanvalsscenario's kan alleen worden gecorreleerd op basis van kennis – in dit geval kunnen alleen voorgedefinieerde aanvallen worden herkend; onbekende aanvallen worden niet herkend.

3.6.4 Tests en vergelijkingen

In 2003 is in het door DARPA ondersteunde *Information Assurance and Survivability Laboratory* in Virginia een experiment uitgevoerd waarin – met een testopstelling die bestond uit vijf netwerksegmenten, enkele tientallen systemen en in totaal 69 sensoren – voor verschillende HIDP- en NIDP-producten IDMEF-wrappers waren geschreven, met als doel om van verschillende correlatiemechanismen de capaciteit tot herkenning van malicieuze activiteiten te kwantificeren [IEEE2]. De resultaten van die tests zijn echter geanonimiseerd om competitie tussen de onderzoekers te voorkomen. Daardoor zijn er alsnog geen conclusies bekend over de effectiviteit van de verschillende mechanismen.

Er zijn wel kleinere experimenten bekend, hoewel die meestal niet volledig onafhankelijk zijn. In 2001 hebben Cunningham en Dain in een experiment alert clustering vergeleken met correlatie op basis van voorgedefinieerde aanvalsscenario's [Cunningham2]. Uit dat experiment bleek dat alert clustering met een zekerheid van 88,81% juiste correlaties

opleverde en de (middels data mining verkregen) scenario's met een zekerheid van maar liefst 99,90%. Een menselijke expert bepaalde daarbij welke correlaties 'juist' waren.

Verder zijn er helaas geen tests bekend waarbij in dezelfde testopstelling verschillende mechanismen zijn geëvalueerd. Wel is bekend dat er onderzoek wordt gedaan naar combinatie van verschillende mechanismen om een beter resultaat te bereiken [Ning2], [Valeur1].

3.7 Conclusie

Security Information Management is de discipline die orde moet gaan scheppen in de chaos van de vele beveiligingsgerelateerde events die in een grote, heterogene infrastructuur worden gegenereerd. Door events van verschillende bronnen – host, netwerk, applicatie – te consolideren naar een centrale repository kan daarna middels verschillende vormen van correlatie kennis worden verkregen over intrusions en andere policy violations. Bij het consolideren worden zowel de syntaxis als semantiek van meldingen genormaliseerd. Er zijn geen standaarden voor die normalisatie, waardoor wetenschappelijk onderzoek naar correlatie tussen host, netwerk en applicatie wordt bemoeilijkt. De huidige inzichten van correlatie bieden alleen praktische mogelijkheden voor correlatie op basis van kennis; alleen bekende aanvallen, bekende patronen, bekende scenario's worden herkend. Er wordt weliswaar onderzoek gedaan naar verschillende vormen van statistische correlatie waarmee onbekende aanvallen zouden kunnen worden herkend, maar dat onderzoek heeft nog niet geleid tot bruikbare implementaties. Om correlatie goed te kunnen laten geschieden is tijdsynchronisatie tussen de verschillende componenten essentieel.

Concluderend kan worden gesteld dat de huidige stand van correlatietechniek goede mogelijkheden biedt voor herkenning van bekende aanvalspatronen, maar nog niet voor onbekende aanvalspatronen (althans, voor zover die niet via inductie uit bekende patronen kunnen worden herleid). Aan een beveiligingsarchitectuur zullen dus aanvullende lagen moeten worden toegevoegd om zo goed mogelijk tegen zulke aanvallen te beschermen (firewalls, netwerksegmentering, …).

4. Security Information Management bij Univé

De decentrale organisaties van Univé zijn zelf verantwoordelijk voor de inrichting en het beheer van hun infrastructuur, inclusief de beveiliging daarvan. Ze kunnen zelf eventuele beveiligingscomponenten kiezen en aanschaffen. De centrale concernafdeling Security Management kan functionele en technische eisen stellen aan de aan te schaffen producten, waardoor Univé-breed toch een bepaalde samenhang kan worden bereikt (dit is in overeenstemming met het strategische plan Focus Verscherpt [Unive2]).

Bij de (nog in te richten) processen en infrastructuur voor monitoring en toezicht spelen belangen op zowel centraal als decentraal niveau:
- de decentrale beheerders willen toezicht houden op hun eigen infrastructuur;
- de centrale afdeling Security Management wil een totaalbeeld van wat er gaande is op de infrastructuur.

Er zal rekening moeten worden gehouden met beide belanghebbenden, wil er draagvlak zijn om monitoring en toezicht effectief in te zetten. De keuze tot het implementeren van tools die monitoring en toezicht faciliteren, zoals SIM en IDP, zal afhangen van een risicobepaling waarbij de werkelijke waarde van de productiesystemen wordt meegenomen in een kosten-baten analyse. Andere factoren die daarbij meewegen zijn de implicaties voor onderhoud, beheer en training. Zo'n risicobepaling zou moeten worden uitgevoerd door het management van team IOB.

In de komende hoofdstukken zal achtereenvolgens worden besproken:
- welke argumenten er bij Univé kunnen zijn om SIM en IDP in te zetten;
- uit welke stappen een implementatietraject grofweg bestaat.

Daarna zal een drietal cases worden besproken waarin de toepassing van SIM en IDP duidelijk wordt in concrete situaties bij Univé.

4.1 Motivaties voor SIM en IDP

Hoewel Univé een Nederlandse organisatie is, zou Section 404 van de Amerikaanse Sarbanes-Oxley Act een motivatie kunnen zijn voor inzet van SIM. Section 404, getiteld "Management Assessment of Internal Controls", verplicht organisaties om controls en procedures te implementeren en te onderhouden om risicobeoordelingen te kunnen doen van alle factoren die potentieel impact hebben op de tijdigheid en juistheid van financiële informatie. De beveiliging van de ICT-infrastructuur is één van die factoren. Het is niet ondenkbaar dat vergelijkbare regelgeving in de komende jaren zal worden ingevoerd in Nederland. Zo niet wettelijk, dan wel door organen als DNB/PVK. SIM speelt op dit moment bij veel Amerikaanse bedrijven al een belangrijke rol bij het aantonen van compliancy met Section 404 van Sarbanes-Oxley. Univé zou SIM en IDP dus proactief kunnen inzetten om te anticiperen op toekomstige regelgeving.

Een betere motivatie is echter: “omdat Univé het zelf wil”. Idealiter volgt vanuit strategisch beleid dat Univé *in control* wenst te zijn van de interne processen. De ICT-infrastructuur is een voorbeeld van één van de aspecten van die interne processen en waarover de organisatie *in control* kan raken, mits daarvoor de juiste maatregelen worden genomen. Monitoring en toezicht zijn voorbeelden van zulke maatregelen. De implementatie van SIM is een concretisering van die maatregelen en werkt ondersteunend bij het bedrijfsbreed *in control* raken van de ICT-infrastructuur.

Verder veroorzaakt de opkomst van webtechnologie, draadloze netwerken, VPN-koppelingen en aanverwante technologie een verschuiving van beveiligingseisen aan de perimeter naar beveiligingseisen aan de eindsystemen [Unive1]. Uit Focus Verscherpt blijkt dat zulke technologie ook bij Univé een (groeiende) rol zal gaan spelen:

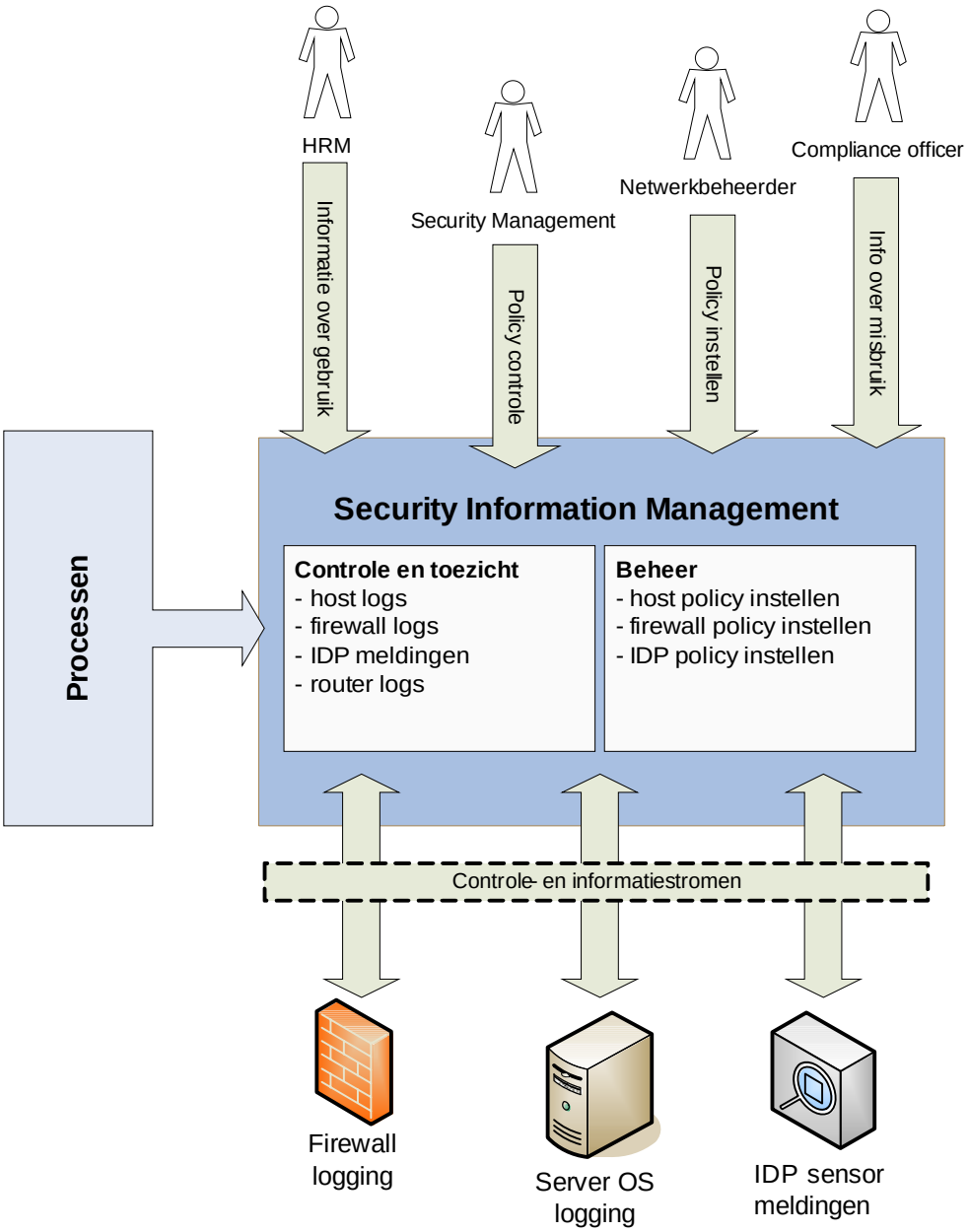
“*Internet zal een steeds grotere rol spelen in de verdergaande procesintegratie tussen verzekeraar, Onderlingen en klanten/leden.*”

“*Het gebruik van webtechnologie zal dan ook worden overwogen bij alle systeem-vernieuwingen binnen Univé.*”

Informatiesystemen van Univé zullen in toenemende mate via webtechnologie over Internet worden ontsloten. Het is voor de bedrijfsvoering van Univé van belang dat die systemen adequaat zijn beveiligd. Voor systemen die direct of indirect vanaf Internet toegankelijk zijn impliceert dat, dat er behalve de ‘standaard’ beveiligingsmaatregelen die Univé momenteel al toepast op de netwerklaag om die systemen te beschermen – zoals network-based firewalls – ook maatregelen worden aangeraden op de hosts zelf; het inschakelen van logging functies en inrichten van een SIM-omgeving om die logs te monitoren is daarbij een eerste stap, het implementeren van HIPS een logische vervolgstap.

4.2 SIM en IDP

Ter recapitulatie: IDP wordt beschouwd als een ‘enge’ functie die via één of enkele netwerk-, host- of applicatiesensors veel meldingen en veel (ir)relevante details oplevert, SIM wordt beschouwd als een ‘ruime’ functie die een holistisch beeld over de infrastructuur beoogt. IDP sensors zijn één mogelijke input voor een SIM systeem en worden idealiter gecorreleerd met security events van andere systemen, zoals firewalls of OS accounting logs. Er zijn bij Univé verschillende belanghebbenden bij een SIM systeem, elk met een eigen informatiebehoefte:



De netwerkbeheerders van Univé zouden in staat moeten zijn via het SIM systeem policies te distribueren naar de onderliggende systemen; Security Management wil een high-level overzicht hebben van (pogingen tot) inbraak; de compliance officers willen de policies kunnen controleren zoals die door de netwerkbeheerders (zouden moeten) worden

gedistribueerd; HRM wil informatie hebben over hoe vaak gebruikers hun wachtwoord vergeten, et cetera.

In Bijlage 4: Beveiligingsarchitectuur bij Univé (deel 1) en Bijlage 6: Beveiligingsarchitectuur bij Univé (deel 2 + domeinen) is in vereenvoudigde vorm zichtbaar hoe bij Univé het gebied tussen het interne netwerk en Internet is ingericht. In het laatste diagram zijn de verschillende beveiligingsdomeinen weergegeven die uit het interview met André Koot naar voren zijn gekomen (zie Bijlage 7: Interview met). De beveiligingsdomeinen vormen de fundamenten voor inrichting van SIM en IDP. Per domein zal moeten worden geïnventariseerd welke systemen er aanwezig zijn met welke besturingssystemen en applicaties. Univé moet bepalen welk logging en alerting beleid moet worden gehanteerd en op welke plekken IDS of IPS wenselijk is. Dat beleid dient te worden vastgesteld in overleg met verschillende proceseigenaren en beheerders – enerzijds om draagvlak te creëren en anderzijds om discrepanties te voorkomen tussen verschillende belangen en gebieden van het beleid. Het logging beleid moet vervolgens worden geïmplementeerd op de betrokken systemen, idealiter op afstand via het SIM systeem. Afhankelijk van het gekozen SIM systeem zullen daarvoor op sommige systemen agents moeten worden geïnstalleerd. Het alerting beleid wordt geïmplementeerd op het SIM systeem zelf. Het ligt voor de hand om voor de Speciale Zaken en Rekencentra domeinen een stringenter logging en alerting beleid te voeren dan voor de Research-Ontwikkeling-Test omgevingen; uit laatstgenoemde domeinen zal waarschijnlijk veel ruis afkomstig zijn.

4.3 Cases bij Univé

Ter illustratie worden hier enkele cases besproken waaruit duidelijk wordt hoe de besproken maatregelen zinvol zouden kunnen zijn bij Univé. Er wordt uitgegaan van de domeinen zoals benoemd in Bijlage 6: Beveiligingsarchitectuur bij Univé (deel 2 + domeinen). Het moge duidelijk zijn dat er andere maatregelen mogelijk zijn die wellicht economischer of effectiever zijn, deze cases dienen slechts als voorbeelden.

4.3.1 Case 1 - IDP: Internetdiensten (Zwolle en Amsterdam)

Het aantal DDoS aanvallen dat vanaf Internet op allerlei doelen wordt uitgevoerd neemt nog steeds toe [Citec1]. Op alle systemen waarmee Univé over Internet diensten aanbiedt is de bedreiging van DDoS van toepassing. De Internetdiensten van Univé kunnen worden gesplitst in publieke diensten (www.unive.nl) en interne diensten (SSL-VPNs, e-mail voor de eigen medewerkers). De gevolgen van DDoS verschillen tussen die gebieden; bij de publieke diensten ligt imagoschade op de loer, bij de interne diensten zal eerder de productiviteit van de medewerkers worden geschaad. Hoewel de meest triviale vormen van DDoS (SYN flooding e.d.) misschien kunnen worden tegengehouden door perimeter firewalls zullen complexere vormen van DDoS en remote exploits zonder aanvullende

maatregelen een bedreiging blijven vormen. Van zowel de publieke als interne diensten vallen de gebruikte ICT-componenten onder het beheer van Univé; de webserver van www.unive.nl die bij de Amsterdamse ISP LeaseWeb staat, de SSL-VPN appliance en Microsoft Exchange server die bij het hoofdkantoor in Zwolle staan incluis. Om die systemen te beschermen tegen complexere vormen van DDoS vanaf Internet zou een NIPS product kunnen worden overwogen. In de komende paragrafen zal de interne SSL-VPN dienst worden beschouwd als case voor IPS.

De F5 FirePass appliance die Univé momenteel in het kader 'mobiliteit' aan het inrichten is om over het Internet via SSL-VPN bepaalde functionaliteit te bieden van interne systemen draagt een inherent risico bij zich. Hoewel er op dit moment van de F5 FirePass geen publiek bekende kwetsbaarheden zijn[4], zijn er op bijvoorbeeld cryptografisch gebied ontwikkelingen die de SSL-versleuteling op wellicht korte termijn zullen kunnen ondermijnen (zoals collision attacks op hashing algoritmes als MD5, SHA0 en SHA1). De perimeter firewalls beschermen de infrastructuur niet tegen de gevolgen van dergelijke bedreigingen.

Daarnaast bleek het begin 2004 in Internet Explorer mogelijk te zijn om via Browser Helper Objects (BHO's) gebruikersinvoer op beveiligde pagina's te onderscheppen voordat die met SSL werd versleuteld; een kort experiment met TamperIE wees uit dat die truc nog steeds mogelijk is met Internet Explorer 6+SP1. De medewerkers van Univé zullen het SSL-VPN typisch via Internet Explorer gaan gebruiken; als een systeem van een medewerker geïnfecteerd zou zijn met een dergelijke BHO dan kunnen inloggegevens uitlekken. Univé heeft bovendien niet volledig grip op de systemen die medewerkers gebruiken om het SSL-VPN te raadplegen; elk systeem met een webbrowser kan daarvoor worden gebruikt, dus complementaire maatregelen aan de cliëntzijde kunnen in deze situatie niet worden afgedwongen. Los van de eventuele randvoorwaarden voor een succesvolle aanval is ontegenzeglijk sprake van nieuwe risico's. Het feit dat op afstand slechts beperkte functionaliteit beschikbaar is en dat er met sterke authenticatie en eenmalige wachtwoorden wordt gewerkt doet daar niets aan af. Op die risico's zou kunnen worden geanticipeerd door extra lagen toe te voegen aan de beveiligingsarchitectuur (voor zover dat nog niet is gedaan). De interne systemen waarvan via SSL-VPNs functionaliteit wordt ontsloten zouden kunnen worden voorzien van HIPS; mocht een tegenstander toegang verkrijgen tot een SSL-VPN account, dan kan het in elk geval tijdig worden opgemerkt als de tegenstander exploits probeert uit te voeren of wijzigingen probeert te doen aan systeeminstellingen (en het systeem daartegen worden beschermd). Een NIDS sensor zou aanvullend kunnen helpen om op te merken dat die systemen als 'stepping stone' worden gebruikt om andere systemen over het netwerk aan te vallen.

[4] Behalve een algemeen (doch bij F5 FirePass relevant) probleem met OpenSSL ASN.1 parsing (http://www.securityfocus.com/bid/8732) en algemene SSL-VPN kwesties, zoals:
- enumeratie van gebruikersnamen (31 januari 2005): http://www.nta-monitor.com/news/vpn-flaws/index.htm
- uitlekken van bedrijfsdocumenten a.g.v. nieuwe desktop search technologie zoals Google Desktop Search, die documenten indexeren die tijdens SSL-sessies zijn opgehaald (12 december 2004): http://www.infoworld.com/article/04/11/12/HNsslrisk_1.html

De SSL-VPN van Univé is slechts één voorbeeld waar IDP mogelijk een rol kan spelen als extra beveiligingslaag tegen bedreigingen vanaf Internet. Een ander gebied waarop in de toekomst mogelijk bedreigingen vanaf Internet van toepassing kunnen gaan zijn is het op webservices gebaseerde Commercieel Informatie Systeem (CIS) dat momenteel in ontwikkeling is bij Marketing & Verkoop.

4.3.2 Case 2 - SIM: De beveiligde koppeling (Zwolle)

Bijlage 4: Beveiligingsarchitectuur bij Univé (deel 1) is een vereenvoudigde weergave van de beveiligde koppeling die het UBN van Internet scheidt en waar externe koppelingen worden gefaciliteerd. In een ideale situatie, waarbij IDP sensors goedkoop zijn en makkelijk te beheren en sprake is van een triviale topologie, zouden sensors worden geplaatst op dezelfde wijze als zichtbaar in Bijlage 2: Voorbeeld beveiligingsarchitectuur (deel 1). Helaas is de praktijk vooralsnog anders en dient zorgvuldig te worden overwogen of IDP wenselijk en haalbaar is.

De inrichting van de beveiligde koppeling is vergelijkbaar met de standaard ‘dubbele sandwich’ firewall architectuur. De buitenste firewall(s) blokkeren het gros van de ongewenste zaken van Internet, de binnenste firewalls blokkeren het gros van de ongewenste zaken van het interne netwerk. Wat overblijft is – als het goed is – legitiem netwerkverkeer. Aangenomen dat de Watchguard 500’s zijn geconfigureerd om ***niets*** door te laten, behalve wat expliciet is opgegeven, is elk pakket dat wordt geblokkeerd op de middelste verbindingen (ofwel inkomend vanaf het buitenste DMZ, ofwel uitgaand vanaf het binnenste DMZ) in principe verdacht. Om dat te monitoren zou elk geblokkeerd pakket moeten worden gemeld/gelogd naar een centrale logging server (met uitzondering van ‘te blokkeren standaard verkeer’).

Enkele vragen die Univé in dit geval zou moeten beantwoorden:

1. Welke transacties moeten worden vastgelegd door de Watchguard 500? (bepaalde dropped packets, …)
2. Welke events leiden tot een alert? (thresholds, alert correlatie)
3. Wie is verantwoordelijk voor het logging beleid?
4. Wie implementeert het logging beleid?
5. Wie is verantwoordelijk voor het alerting beleid?
6. Wie implementeert het alerting beleid?
7. Wie is verantwoordelijk voor het toezien op alerts? (monitoring)
8. Wie is verantwoordelijk voor het reageren op alerts? (incident response)

In dit geval zou de Watchguard 500 de events via rsyslog aanleveren aan het SIM systeem, dat de events vervolgens kan correleren met andere events – zoals dat van de HIPS en

NIDS sensors die in de eerste case zijn genoemd. Zodoende zou het kunnen worden opgemerkt als iemand via de SSL-VPN of de e-mail server probeert in te breken op het interne netwerk (richting CODA, zie de volgende case).

4.3.3 Case 3 - IDP: CODA in Productie (Zwolle)

Het domein Productie omvat alle productieservers in Zwolle, waaronder systemen als Siebel (CRM) en CODA (financieel pakket). Op dit moment is het Productie-domein niet afgeschermd van de rest van het interne netwerk, hoewel het aannemelijk is dat er in de toekomst nieuwe bedreigingen zullen worden geïntroduceerd door 'pseudo-internal intruders'[5] [Unive1].

Om de juistheid van de afkomst van berichten die naar CODA worden verstuurd te controleren, zou anomaly-based intrusion detection kunnen worden toegepast.

[5] 'Pseudo-internal intruders' worden beschreven in [Unive1]; een voorbeeld daarvan is een tegenstander die via een Internetdienst van Univé door het DMZ naar het interne netwerk doordringt.

4.4 Randvoorwaarden

De randvoorwaarden voor IDP en SIM kunnen nog niet volledig worden geformuleerd, omdat daartoe eerst bekend moet zijn op welke plaatsen Univé die maatregelen wil toepassen. Die informatie volgt uit een toekomstige risicoanalyse die namens het management van IOB zou moeten worden uitgevoerd. Om een indicatie te geven van mogelijke randvoorwaarden volgt hieronder een eerste aanzet, voortvloeiend uit de resultaten van het vooronderzoek [Univé1] en dit onderzoeksrapport.

4.4.1 Technische randvoorwaarden

Indicatie van toepassingen IDP/SIM bij Univé		
Beveiligingsdomein	**Vb. relevante componenten**	**Vb. mogelijke inzet van IDP/SIM**
Productie, Zwolle	- Microsoft Windows 2003 servers - Microsoft Exchange server - IBM AIX 5.x servers - Cisco 4500 en 6000 routers	- Loganalyse voor Windows 2003 servers - Loganalyse voor IBM AIX 5.x servers - NIPS rondom CODA en het Postkantoor (anomaly-based)
Beveiligde koppeling, Zwolle	- Microsoft ISA servers - Microsoft Exchange server - Watchguard firewalls - F5 FirePass SSL-VPN appliance - Barracuda anti-spam appliance	- Loganalyse voor de ISA servers - Loganalyse voor de Watchguards - Loganalyse voor de F5 FirePass - HIPS op de systemen die via VPN worden gebruikt
e-Business, Amsterdam	- Microsoft IIS server (www.unive.nl) - Microsoft SQL Server 2000 - Cisco PIX firewall	- Loganalyse voor de Cisco PIX - NIPS voor de publieke webserver (bescherming tegen DDoS) - AIPS voor Microsoft IIS (bescherming tegen hacks die niet door NIPS kunnen worden herkend, zoals SQL injectie over SSL) - AIPS voor Microsoft SQL Server (bescherming tegen hacks vanaf de IIS server)

Uit het bovenstaande schema volgen enkele randvoorwaarden:

- de SIM/IDP oplossing moet voorzien in loganalyse voor Windows 2003;
- de SIM/IDP oplossing moet voorzien in loganalyse voor IBM AIX 5.x;
- de SIM/IDP oplossing moet voorzien in loganalyse voor Watchguard (syslog?);
- de SIM/IDP oplossing moet voorzien in loganalyse voor Cisco PIX (syslog?);
- de SIM/IDP oplossing moet voorzien in loganalyse voor F5 FirePass (syslog?);
- de SIM/IDP oplossing moet voorzien in NIPS (+voldoende capaciteit);
- de SIM/IDP oplossing moet voorzien in HIPS voor verschillende platformen;
- de SIM/IDP oplossing moet voorzien in AIPS voor Microsoft IIS;
- de SIM/IDP oplossing moet voorzien in AIPS voor Microsoft SQL Server;

De events van alle genoemde componenten dienen op één centrale locatie te worden opgeslagen en gecorreleerd, zodat een holistisch beeld wordt verkregen over alle beveiligingsdomeinen van Univé.

4.4.2 Beheermatige randvoorwaarden

De decentrale verantwoordelijkheden bij Univé impliceren dat decentrale beheerders in staat moeten zijn om 'hun' deel van de infrastructuur te monitoren, terwijl de concernafdeling Security Management juist behoefte heeft aan een Univé-breed overzicht. De SIM/IDP oplossing moet dus voorzien in twee informatiebehoeften:

- de SIM/IDP oplossing moet voorzien in monitoring op decentraal niveau;
- de SIM/IDP oplossing moet voorzien in monitoring op centraal niveau;
- de SIM/IDP oplossing moet voorzien in beheer op centraal niveau.

4.4.3 Aanvullende randvoorwaarden

Aanvullende technische randvoorwaarden zouden kunnen zijn:

- de SIM/IDP oplossing moet voorzien in (optionele) versleuteling van de gebruikte communicatiekanalen (i.v.m. events vanaf de Speciale Zaken domeinen), bijvoorbeeld:
    - SSL-tunneling
    - SSH-tunneling
    - productspecifieke versleuteling
- de SIM/IDP oplossing moet ondersteuning bieden voor de Cisco Secure IDS 4235, die reeds is aangeschaft door BU Schade in Assen;
- de IDP sensors mogen niet volledig afhankelijk zijn van pattern-based detectie, maar moeten op z'n minst één vorm van anomaly-based detectie implementeren.

Aanvullende beheermatige randvoorwaarden zouden kunnen zijn:

- de SIM/IDP oplossing moet voorzien in de mogelijkheid tot invoer van security policies, bijvoorbeeld:
    - volledige logging moet zijn ingeschakeld voor account logons op alle Windows servers;
    - patch ### moet zijn geïnstalleerd op alle Windows werkstations en servers;
    - op alle Windows werkstations mogen alleen processen A, B en C draaien;
    - op alle Windows servers mogen alleen processen X, Y en Z draaien;
    - op server A, B en C is inkomend verkeer alleen toegestaan op poort #;
    - op alle Windows systemen moet anti-virus software zijn geïnstalleerd en mogen de virussignaturen niet ouder zijn dan 1 maand;
    - van alle situaties waarin wordt afgeweken van bovenstaand beleid moet een melding worden gegenereerd.
- de SIM/IDP oplossing moet voorzien in de mogelijkheid tot (automatische) distributie van security policies naar de aangesloten systemen (logging en alerting beleid, et cetera), bijvoorbeeld:
    - door alle policies af te dwingen via Active Directory;
    - door policies te distribueren naar lokale componenten.
- de SIM/IDP oplossing moet voorzien in de mogelijkheid tot controle op implementatiestatus van de security policies, bijvoorbeeld:
    - Microsoft Baseline Security Analyzer (MBSA)

- andere productspecifieke controles

4.5 SIM Proof-of-Concept

Bij Univé is IBM Tivoli in gebruik als raamwerk voor beheer. De optionele module Tivoli Risk Manager (TRM) kan worden gebruikt voor consolidatie en correlatie van security events en is daarmee een verschijningsvorm van SIM [IBM1]. TRM claimt expliciet ondersteuning voor veel verschillende systemen, waarvan de volgende bij Univé relevant zijn:

- loganalyse voor Windows 2000 (“Adapter for HIDS”)
- loganalyse voor IBM AIX 5 (“Adapter for HIDS”)
- loganalyse voor Cisco routers (“Adapter for Cisco routers”)
- loganalyse voor Cisco IDS (“Adapter for Cisco Secure IDS”)
- loganalyse voor Cisco PIX (“Adapter for Cisco Secure PIX Firewall”)

De events belanden uiteindelijk in de Tivoli Enterprise Console (TEC). TEC heeft standaard al de mogelijkheid tot het creëren van verschillende *views*, waarmee de informatievoorziening kan worden afgestemd op de behoeften van de Univé. Daarmee lijkt TRM te functioneren in overeenstemming met de primaire beheermatige randvoorwaarde.

De originele fundamenten van correlatie in TRM staan beschreven in [Debar2], maar latere versies zijn mogelijk gebaseerd op het door de Europese Unie gefinancierde *Malicious and Accidental Fault Tolerance for Internet Applications*, dat deels in IBM’s Research Lab in Zürich is ontwikkeld [MAFTIA1], [MAFTIA2].

In 2003 won TRM de Crossroads (Open System Advisors) prijs in de categorie *Security Event Management*. Daarbij werden enkele succesfactoren genoemd, die anno 2005 nog steeds van toepassing zullen zijn [Crossroads1]:

SUCCESSFACTORS
Project strategy: It’s up to you to protect your brand from external and internal threats, say IBM Tivoli Risk Manager reference customers. There is nowhere to run and no place for a major enterprise to hide from this responsibility. They recommend, therefore, that skills transfer be your watchword. **Start with a simple project and expand steadily as the team acquires skills**.
Skills: Pay attention to the synergy between security generalists using IBM Tivoli Risk Manager and specialists manning the firewalls and other equipment or applications. **Each has a role to play—both individually and in the group process—to deal with threats and minimize false positives.**
Resources: **Allow adequate time for testing**, including network load testing, and for ascertaining the most pertinent reports.
Fit: IBM Tivoli Risk Manager is a good fit **for large corporations committed to effective self-defense** against security intrusion.

Hoewel er andere, meer gespecialiseerde SIM-producten bestaan, zoals de eerdergenoemde ArcSight ESM (www.arcsight.com), Open Services Security Threat Manager (www.open.com), netForensics’ SIM (www.netforensics.com) en de producten van Intellitactics (www.intellitactics.com), zijn er een paar goede argumenten om voor deze Proof-of-Concept te kiezen voor IBM Tivoli Risk Manager:

- **kosten à** Univé beschikt door een eerdere deal met IBM over licenties van een hele reeks Tivoli producten, waaronder de voor dit onderzoek relevante Risk Manager;
- **beheer à** door te kiezen voor uitbreiding van een product dat al door Univé wordt gebruikt en beheerd wordt de beheerorganisatie niet onnodig belast met de eigenaardigheden van een volledig nieuw product – inclusief frictie met andere ICT-componenten. Draagvlak en kans van slagen worden daardoor vergroot (of ten minste niet verkleind);
- **implementatie à** omdat de basisinfrastructuur van Tivoli al aanwezig is hoeven geen (of nauwelijks) wijzigingen te worden gedaan aan die infrastructuur – er worden bijvoorbeeld geen nieuwe communicatiekanalen geïntroduceerd. De reeds op alle Windows en AIX servers geïnstalleerde Tivoli Endpoint wordt voor Risk Manager gebruikt;
- **ondersteuning à** IBM is bijna alomtegenwoordig en zal waarschijnlijk niet snel failliet gaan - Univé is dus redelijk zeker van (toekomstige) ondersteuning; bovendien is IBM zelf ook gevestigd in Nederland, terwijl van de concurrerende leveranciers in Nederlands vaak alleen een importeur is gevestigd.

Het belangrijkste argument tégen de keuze van Risk Manager is de onduidelijke status van de ontwikkeling van het product. De meest recente versie van Risk Manager (4.2) dateert van 2002; het is niet duidelijk of toekomstige beveiligingscomponenten zullen worden ondersteund door Risk Manager en of IBM van plan is om Risk Manager, indien voortschrijdend inzicht in SIM/IDP daartoe aanleiding geeft, nog verder te ontwikkelen. Echter, uitgaande van het besef dat Risk Manager deel uitmaakt van IBM's On-Demand dienst Security Event Management 'zal het misschien wel meevallen' – de On-Demand diensten zijn immers het huidige vlaggenschip van IBM, dus kan IBM het zich niet permitteren een inferieur of obsoleet product te leveren [IBM2].

Voor de Proof-of-Concept (PoC) is Risk Manager gekozen. Er is een apart PID opgesteld, getiteld "*Experiment IBM Tivoli Risk Manager*", waarin de opzet en fasering van het experiment staan beschreven. De PoC bestaat uit enkele voor Univé representatieve ICT-componenten die allerlei beveiligingsmeldingen kunnen leveren aan Risk Manager. Risk Manager is in de PoC verantwoordelijk voor het consolideren en correleren van die meldingen – een standaard SIM taak. Op basis van enkele gesprekken met Rick Veenstra, Herman Slagman en André Koot van Univé en Marcel Snippe van IBM is besloten om de Proof-of-Concept omgeving te laten inrichten door een externe partij; de belangrijkste reden daarvoor is de benodigde en gewenste expertise op het gebied van Risk Manager. Uit de opgeleverde PoC-omgeving zou na enkele tests blijken hoe Risk Manager functioneert en hoe de meldingen worden gecorreleerd.

Helaas bleek het niet mogelijk om binnen de beschikbare tijd een Proof-of-Concept omgeving te realiseren met Risk Manager. Als alternatief is NetIQ Security Manager getest. Het experiment-PID en de hack scenario's konden daarbij vrijwel onveranderd worden gebruikt.

4.6 Keuze van een SIM/IDP oplossing

In H4.4 zijn enkele randvoorwaarden geformuleerd waaraan SIM en IDP zou moeten voldoen om inzetbaar te zijn bij Univé. Er zijn echter meer aandachtspunten. Het inrichten en afstemmen van zowel SIM als IDP zijn activiteiten waarvoor – na definitieve keuze voor een product – wordt aangeraden om externe expertise in te zetten, omdat er veel specialistische kennis voor nodig is. Het toezicht houden op het SIM systeem is een taak die typisch bij Univé zelf thuishoort – SIM vervult immers de informatiebehoefte die de cluster Security Management heeft geformuleerd bij aanvang van dit onderzoek. Het lijkt bovendien aannemelijk dat Univé zelf in staat is om wijzigingen in de infrastructuur van Univé te verwerken in het SIM-systeem en de informatievoorziening te onderhouden zodra het logging en alerting beleid eenmaal is opgesteld en voor de eerste keer geïmplementeerd (mits de betrokken personen een training hebben gehad voor het SIM-product).

Het beheer van en toezicht op IDS en IPS vereist in de regel echter expertise die bij Univé niet aanwezig is en waarvoor waarschijnlijk geen mankracht zal kunnen worden vrijgemaakt. Elke dag komen er nieuwe exploits bij en regelmatig worden nieuwe soorten aanvallen bedacht. Als gebruik wordt gemaakt van pattern-based detectie, zal de configuratie van het IDP systeem voor elke nieuwe exploit of soort aanval moeten worden aangepast, waarbij opnieuw false positives kunnen ontstaan. Het lijkt daarom zinvol om die taken te outsourcen naar een gespecialiseerd bedrijf, waar specialisten toezicht houden op de gegenereerde meldingen en contact opnemen met Univé bij een geverifieerde inbraak.

Samenvattend zijn er dus twee aanvullende randvoorwaarden:

- indien pattern-based detectie wordt gebruikt, moet de IDP oplossing voorzien in de mogelijkheid tot outsourcing van de beheertaken betreffende de afstemming en het onderhoud aan de signatures, bijvoorbeeld:
    - remote updaten van signatures;
    - remote updaten van policy.
- de IDP oplossing moet voorzien in de mogelijkheid tot outsourcing van de monitoring taken betreffende het toezicht houden op en beoordelen van de gegenereerde meldingen, bijvoorbeeld:
    - doorsturen van meldingen naar de outsourcing partner (push);
    - de outsourcing partner de meldingen kunnen laten ophalen (pull).
- de outsourcing partner moet geverifieerde meldingen kunnen aanleveren aan het SIM-systeem van Univé, zodat daar eventuele verdere correlatie mogelijk is.

4.7 Conclusie

"Is SIM echt wel nodig bij Univé en uiteindelijk in het belang van leden? En IDP? Kan hetzelfde doel worden bereikt met minder?"

De bovenstaande vragen zijn geïnspireerd door Focus Verscherpt [Unive2]. SIM mag worden beschouwd als een wenselijke toevoeging aan de beveiligingsarchitectuur van Univé en kan zowel de centrale als de decentrale beheerder zicht verschaffen in wat er op de infrastructuur plaatsvindt. SIM consolideert en analyseert meldingen van o.a. servers, routers, firewalls en IDP systemen om zodoende beveiligingsproblemen vroegtijdig te kunnen onderkennen. Het tijdig onderkennen van zulke problemen is in het belang van haar leden, omdat het uiteindelijk bijdraagt aan bescherming van persoons- en verzekeringsgegevens. Een knelpunt bij implementatie van SIM is het opstellen en naleven van het logging en alerting beleid – er zal menskracht voor moeten worden ingezet om dat beleid op te stellen en een bedrijfsproces voor moeten worden ingericht om dat beleid na te leven. Er zal een procedure moeten worden bedacht voor het afhandelen van incidenten en er zal iemand verantwoordelijk moeten worden gesteld voor het toezicht op het SIM systeem. Er zijn geen andere middelen waarmee hetzelfde doel kan worden bereikt – SIM is de enige mogelijkheid om een holistisch beeld te krijgen van de beveiliging van de infrastructuur. IBM Risk Manager is een product dat SIM kan realiseren en dat goed lijkt te passen binnen de bestaande infrastructuur van Univé (incl. de beheerprocessen). Het bezoek van IBM-consultant Marcel Snippe, de handleidingen van Risk Manager en de artikelen die zijn gepubliceerd door onderzoekers die verbonden zijn aan IBM's lab in Zürich suggereren dat Risk Manager kan voorzien in de behoefte die Security Management heeft geformuleerd - SIM met geavanceerde correlatie. Het was niet mogelijk om binnen de beschikbare onderzoekstijd een Proof-of-Concept te realiseren met Risk Manager. In plaats daarvan is een alternatief product geëvalueerd, NetIQ Security Manager. Een verslaglegging van die Proof-of-Concept is beschikbaar als apart document. De Proof-of-Concept werd afgesloten met de conclusie dat NetIQ Security Manager een uitstekend product is voor consolidatie van loggegevens, maar dat de correlatiefunctie tamelijk beperkt is. Als Univé de correlatiefunctie inderdaad als belangrijk selectiecriterium beschouwt (zoals dit rapport adviseert), dan lijkt NetIQ Security Manager niet een juiste productkeuze. Mocht Univé besluiten dat een SIM omgeving moet worden opgezet, dan wordt aangeraden om Risk Manager alsnog serieus te overwegen en te evalueren in een apart Proof-of-Concept. Bij die evaluatie kan dezelfde aanpak worden gehanteerd als bij de evaluatie van NetIQ; de hack scenario's hoeven daarvoor niet te worden aangepast.

Het is zinvol om IDP te overwegen voor de systemen die zijn ontsloten via Internet, met name voor de systemen waarbij het denkbaar is dat de bestaande network-based firewalls niet kunnen beschermen tegen de huidige generatie van bedreigingen. Het gaat daarbij in eerste instantie om 'het gezicht' van Univé naar de klanten, www.unive.nl, bij het e-Business domein in Amsterdam. Daar loopt inmiddels al een proef met een Symantec SNS7100 NIPS appliance, ter controle op bijvoorbeeld SQL injectie en exploits op Microsoft IIS. Een ander toepassingsgebied voor IDP zijn de diensten voor de eigen medewerkers, waaronder de SSL-VPN dienst en de e-mailservers. Op alle productiesystemen waarvan via Internet functionaliteit wordt ontsloten wordt HIPS

aangeraden, simpelweg omdat network-based firewalls niet beschermen tegen remote exploits en andere vormen van compromittering die zich boven de applicatielaag afspelen en die niet kunnen worden uitgesloten door andere maatregelen.

Uit het vooronderzoek volgde dat er weinig maatregelen zijn genomen tegen bedreigingen van binnenuit [Unive1]. Zolang de communicatiestromen van de interne systemen niet adequaat zijn gedocumenteerd, heeft IDP daar nauwelijks zin. Een betere eerste stap voor bescherming tegen bedreigingen van binnenuit is die communicatiestromen te documenteren en het netwerk daarna verder te segmenteren, zodat niet alle werkstations zonder enige belemmering kunnen communiceren met alle back-end servers (zelfs de servers die alleen diensten verlenen aan andere servers). Daarbij kan uiteindelijk gebruik worden gemaakt van de reeds aanwezige firewalls. Er hoeven dan geen nieuwe ICT-componenten te worden aangeschaft en onderhouden, terwijl er wel een duidelijke verbetering plaatsvindt in de beveiliging van de interne systemen.

Begrippen

Alert

Een event of combinatie van events die dienen te worden gerapporteerd, omdat het alerting beleid dat voorschrijft. Dat rapporteren kan gebeuren aan een persoon (via e-mail of naar een console), maar ook aan een ander systeem dat de alert voor verdere analyse gebruikt.

Alerting beleid

Het alerting beleid schrijft voor welke events of combinaties van events relevant zijn voor de beveiligingsstatus van een component. Het alerting beleid vloeit voort uit het logging beleid en combineert best practices op het gebied van alerting met de eisen die een organisatie aan de alerting stelt.

De beveiligingscontext is een belangrijke factor: een enkele mislukte inlogpoging op een server in een testomgeving heeft bijvoorbeeld weinig betekenis, maar dezelfde event kan in een high-security omgeving wel degelijk belangrijk zijn en direct tot een alert moeten leiden.

Anomaly-based detectie

Anomaly-based detectie is een vorm van detectie waarbij misbruik wordt geprobeerd te herkennen op basis van afwijkingen op normale gebruikspatronen. Een systeem dat normaliter geen of nauwelijks ICMP verkeer genereert en ineens duizenden ICMP pakketten verstuurt kan zo worden herkend als potentiële bron van een worm of DDoS bot. Pattern-based detectie zou het bovengenoemde scenario niet hebben opgemerkt, omdat de inhoud van het netwerkverkeer niet wijst op misbruikt.

Consolidatie

In de context van loganalyse omvat consolidatie het normaliseren en centraliseren van meldingen (events of alerts) van heterogene componenten.

Correlatie

In de context van loganalyse omvat correlatie het ontdekken van verbanden tussen verschillende meldingen (events of alerts), waarbij typisch op basis van eigenschappen als tijd en ruimte wordt gekeken naar causale verbanden. Door correlatie kan automatisch worden geabstraheerd over low-level meldingen, waardoor het aantal meldingen wordt gereduceerd en de overgebleven meldingen van hogere kwaliteit zijn. Door IDP-meldingen passief te correleren aan een actuele hardware/software inventory of actief te correleren aan real-time informatie van een verondersteld slachtoffer kan het aantal false positives worden gereduceerd.

Event

Een event is een transactie die in een lokaal logboek of op afstand is geregistreerd, omdat het logging beleid dat voorschrijft. Voorbeelden van typische events zijn inlogpogingen, het uitlezen en opslaan van systeembestanden en het blokkeren van netwerkverkeer door een firewall. Voorbeelden van registratie in een lokaal logboek zijn het Windows Event

Log en Unix syslog. Voorbeelden van registratie op afstand zijn Unix remote syslog en SNMP.

False negative

Een false negative is het onjuist of ongewenst uitblijven van de beoordeling van sensorinput als een beveiligingsprobleem door een IDP – ofwel: een inbraakpoging waarbij geen alarm is afgegaan|.

False positive

Een false positive is een onjuiste of ongewenste beoordeling van sensorinput als een beveiligingsprobleem door een IDP – ofwel: vals alarm.

Intrusion Detection/Prevention (IDP)

IDP is de verzamelterm voor intrusion detection en intrusion prevention.

Intrusion Detection System (IDS)

Een intrusion detection

Intrusion Prevention System (IPS)

Een anti-virus appliance

Logging beleid

Het logging beleid schrijft voor welke transacties dienen te worden geregistreerd. Het logging beleid vloeit voort uit een combinatie van de eisen die een organisatie zelf stelt aan de logging en (misschien belangrijker) de voorschriften in best practices op het gebied van logging:

- NSA's Security Configuration Guides (www.nsa.gov/snac)
- Best practices van de fabrikanten zelf (www.microsoft.com, www.ibm.com)
- Publicaties van PI (www.platforminformatiebeveiliging.nl)
- Publicaties van NIST (www.nist.gov)

Normalisatie

Onder normalisatie wordt de vertaling verstaan van een inkomende melding (event of alert) naar een (standaard)formaat dat een SIM systeem begrijpt. Daarbij wordt zowel gekeken naar de syntaxis als de semantiek van de melding.

Pattern-based detectie (alias mis-use detectie)

Pattern-based detectie is een vorm van detectie waarbij op basis van bekende signaturen wordt geprobeerd misbruik te herkennen. Typische voorbeeld is de aanwezigheid van bepaalde tekenreeksen in HTTP verzoeken.

Security Information Management (SIM)

Security Information Management duidt de ontwikkelingen aan die een holistisch beeld beogen van de beveiligingsstatus van ICT- en eventueel andersoortige componenten binnen een totale infrastructuur. Allerlei componenten in een infrastructuur genereren meldingen of kunnen meldingen genereren; om SIM mogelijk te maken moeten al die meldingen worden geconsolideerd en centraal worden verwerkt.

Transactie

Een transactie is de kleinste logische verwerkingseenheid waarvan een systeem of component het voorkomen kan registreren of laten registreren, typisch in een logboek. In principe is *alles* dat zich binnen een computer afspeelt een potentiële transactie.

Literatuuropgave

Bedrijfsdocumenten

[Unive1] Titel : "Vooronderzoek – Beveiliging tegen bedreigingen van Internet"
Auteur(s) : Matthijs Koot
Versie : 0.7 (18 maart 2005)

[Unive2] Titel : "Focus Verscherpt!"
Auteur(s) : Bestuur Univé Verzekeringen
Versie : versie 5, 2004

Drukwerk

[Endorf1] Titel : "Intrusion Detection & Prevention"
Auteur(s) : Carl Endorf, dr. Eugene Schultz en Jim Mellander
Druk : 1ste druk, 2004
Uitgever : McGraw-Hill
ISBN : 0072229543

[IEEE1] Titel : "Defending Yourself: The Role of Intrusion Detection Systems" (artikel in IEEE Software, vakblad voor software engineers)
Auteur(s) : John McHugh, Alan Christie en Julie Allen (SEI, CERT)
Bezocht op : 19 maart 2005
Dateert van : september/oktober 2000

[Overbeek1] Titel : "Informatiebeveiliging in de praktijk" (cursusmateriaal)
Auteur(s) : Dr. Ir. P.L. Overbeek RE en Dr. E. Roos Lindgreen RE
Druk : 12de druk, 2001
Uitgever : International Management Forum
ISBN : niet beschikbaar

[Wieringa1] Titel : "e-Security deel II – Beveiligingsarchitectuur"
Auteur(s) : drs. D.M. Wieringa RE
Druk : 10de druk, 2005
Uitgever : International Management Forum, Eindhoven
ISBN : niet beschikbaar

Internet

[ACM1] Titel : "Intrusion Detection Systems and Multisensor Data Fusion" (artikel in *Communications of the ACM*, april 2000, vol. 43, nr. 4)
Auteur(s) : Tim Bass
Bezocht op : 23 maart 2005

	Dateert van	: April 2000
	URI	: http://www.silkroad.com/papers/pdf/acm-p99-bass.pdf
[Anderson1]	Titel	: "Computer Security Threat Monitoring and Surveillance"
	Auteur(s)	: James Anderson
	Bezocht op	: 23 maart 2005
	Dateert van	: 15 april 1980
	URI	: http://csrc.nist.gov/publications/history/ande80.pdf
[Angelino1]	Titel	: "Using events-per-second as a factor in selecting SEM tools"
	Auteur(s)	: Robert Angelino
	Bezocht op	: 26 maart 2005
	Dateert van	: 23 november 2004
	URI	: http://www.infosecwriters.com/text_resources/pdf/events_per_second.pdf
[Axelsson1]	Titel	: "Intrusion Detection Systems: A Survey and Taxonomy"
	Auteur(s)	: Stefan Axelsson
	Bezocht op	: 19 mei 2005
	Dateert van	: 14 maart 2000
	URI	: http://www.mnlab.cs.depaul.edu/seminar/spr2003/IDSSurvey.pdf
[Barbara1]	Titel	: "Detecting Novel Network Intrusions Using Bayes Estimators"
	Auteur(s)	: Daniel Barbará, Ningning Wu en Sushil Jajodia
	Bezocht op	: 3 april 2005
	Dateert van	: februari 2001
	URI	: http://www.siam.org/meetings/SDM01/pdf/sdm01_29.pdf
[Barrus1]	Titel	: "A Distributed Autonomous-Agent Network-Intrusion Detection and Response System"
	Auteur(s)	: Joseph Barrus en Neil C. Rowe
	Bezocht op	: 28 maart 2005
	Dateert van	: juni 1998
	URI	: http://www.cs.nps.navy.mil/people/faculty/rowe/barruspap.html
[Carey1]	Titel	: "Attack Signature Matching and Discovery in Systems Employing Heterogeneous IDS"
	Auteur(s)	: Nathan Carey, George Mohay en Andrew Clark
	Bezocht op	: 27 maart 2005
	Dateert van	: 19 september 2003
	URI	: http://www.acsac.org/2003/papers/62.pdf
[Chuvakin1]	Titel	: "Event Correlation in Security"
	Auteur(s)	: dr. Anton Chuvakin GCIA GCIH
	Bezocht op	: 31 maart 2005
	Dateert van	: 2001

URI : http://www.tisc2001.com/newsletters/57.html

[Cisco1] Titel : "Configuring Cisco IOS Firewall Intrusion Detection System"
Auteur(s) : -
Bezocht op : 18 maart 2005
Dateert van : 4 augustus 2004
URI : http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfids.htm

[Cisco2] Titel : "SAFE: IDS Deployment, Tuning and Logging in Depth [SAFE Blueprint"
Auteur(s) : Ido Dubrawsky en Roland Saville
Bezocht op : 28 maart 2005
Dateert van : -
URI : http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/safwp_wp.pdf

[Citec1] Titel : "DDoS attacks now a growing menace"
Auteur(s) : -
Bezocht op : 18 april 2005
Dateert van : 3 maart 2005
URI : http://www.citec.com.au/news/featureNews/2005/March/ddos_attacks.shtml

[Crossroads1] Titel : "IBM Tivoli Risk Manager" (winnaar Crossroads A-List award 2003)
Auteur(s) : -
Bezocht op : 29 maart 2005
Dateert van : januari 2003
URI : http://www.crossroads-osa.com/research/company/2003%20Brief%20Tivoli%20Security%20Event%20Management%20Final.pdf

[CompWkly1] Titel : "Microsoft security chief backs users on need to 'deperimeterise' network security"
Auteur(s) : -
Bezocht op : 2 februari 2005
Dateert van : 1 februari 2005
URI : http://www.computerweekly.com/Article136445.htm

[Counterpane1] Titel : "Security Alert: Multiple Buffer Overruns in Microsoft SQL Server"
Auteur(s) : -
Bezocht op : 23 maart 2005
Dateert van : 30 juli 2002
URI : http://www.counterpane.com/alert-v20020730001.html

[Cunningham1] Titel : "Building Scenarios from a Heterogeneous Alert Stream"
Auteur(s) : Robert K. Cunningham en Oliver M. Dain
Bezocht op : 14 maart 2005

	Dateert van	: december 2001
	URI	: http://www.ll.mit.edu/IST/pubs/2002_Building.pdf
[Cunningham2]	Titel	: "Fusing a Heterogeneous Alert Stream into Scenarios"
	Auteur(s)	: Robert K. Cunningham en Oliver M. Dain
	Bezocht op	: 3 april 2005
	Dateert van	: november 2001
	URI	: http://www.ll.mit.edu/IST/pubs/acm_02_omd_rkc.pdf
[Cuppens1]	Titel	: "Preventing coordinated attacks via alert correlation"
	Auteur(s)	: Frédéric Cuppens et al.
	Bezocht op	: 2 april 2005
	Dateert van	: 11 april 2004
	URI	: http://www.tml.hut.fi/Nordsec2004/Presentations/autrel.pdf
[Cuppens2]	Titel	: "Managing Alerts in a Multi-Intrusion Detection Environment"
	Auteur(s)	: Frédéric Cuppens et al.
	Bezocht op	: 2 april 2005
	Dateert van	: december 2001
	URI	: http://www.tml.hut.fi/Nordsec2004/Presentations/autrel.pdf
[Cuppens3]	Titel	: "Alert Correlation in a Cooperative Intrusion Detection Framework"
	Auteur(s)	: Frédéric Cuppens en Alexander Miège
	Bezocht op	: 3 april 2005
	Dateert van	: 2002
	URI	: http://4lx.free.fr/articles/CM02.pdf
[Debar1]	Titel	: "M2D2: A Formal Data Model for IDS Alert Correlation"
	Auteur(s)	: Benjamin Morin, Ludovic Mé, Hervé Debar en Mireille Ducassé
	Bezocht op	: 27 maart 2005
	Dateert van	: oktober 2002
	URI	: http://perso.rd.francetelecom.fr/debar/papers/MoMeDuDe02.pdf
[Debar2]	Titel	: "Aggregation and Correlation of Intrusion Detection Alerts"
	Auteur(s)	: Hervé Debar en Andreas Wespi
	Bezocht op	: 27 maart 2005
	Dateert van	: oktober 2001
	URI	: http://perso.rd.francetelecom.fr/debar/papers/DebWes01.pdf
[Debar3]	Titel	: "Correlation of Intrusion Symptoms: an Application of Chronicles"
	Auteur(s)	: Hervé Debar en Benjamin Morin
	Bezocht op	: 29 maart 2005
	Dateert van	: 2003
	URI	: http://perso.rd.francetelecom.fr/debar/papers/MorDeb03.pdf
[Debar4]	Titel	: "Intrusion detection alerts"

	Auteur(s)	: Hervé Debar
	Bezocht op	: 2 april 2005
	Dateert van	: 13 januari 2004
	URI	: http://seclab.cs.ucdavis.edu/seminars/Herve-slides.pdf
[DeBoer1]	Titel	: "A Generic Framework for Fusion-Based Intrusion Detection Systems" (master thesis)
	Auteur(s)	: Remco de Boer
	Bezocht op	: 28 maart 2005
	Dateert van	: oktober 2002
	URI	: http://www.xs4all.nl/~rcdeboer/rcdb_thesis.pdf
[Deeter1]	Titel	: "APHIDS: A Mobile Agent-Based Programmable Hybrid Intrusion Detection System"
	Auteur(s)	: Ken Deeter, Kapil Singh, Steve Wilson, Luca Filipozzi en Son Vuong
	Bezocht op	: 3 april 2005
	Dateert van	: augustus 2004
	URI	: http://www.cs.ubc.ca/~singh/publication/aphids_cameraready.pdf
[Denning1]	Titel	: "An Intrusion-Detection Model"
	Auteur(s)	: dr. Dorothy Denning en Peter Neumann
	Bezocht op	: 23 maart 2005
	Dateert van	: februari 1987
	URI	: http://www.cs.georgetown.edu/~denning/infosec/ids-model.rtf
[DMTF1]	Titel	: "Common Information Model (CIM) Standards"
	Auteur(s)	: -
	Bezocht op	: 23 maart 2005
	Dateert van	: -
	URI	: http://www.dmtf.org/standards/cim/
[Duffy1]	Titel	: "Intrusion Detection Exchange Architecture"
	Auteur(s)	: Ian Duffy BSc.
	Bezocht op	: 21 maart 2005
	Dateert van	: 9 november 2003
	URI	: http://idea-arch.sourceforge.net/
[Garfinkel1]	Titel	: "Traps and Pitfalls: Practical Problems in System Call Interposition Based Security Tools"
	Auteur(s)	: Tal Garfinkel (PhD student)
	Bezocht op	: 18 maart 2005
	Dateert van	: 2003
	URI	: http://www.cs.fit.edu/~pkc/id/related/garfinkel03ndss.pdf
[Gartner1]	Titel	: "The Future of Information Security" (Gartner)
	Auteur(s)	: Jeffrey Zimmerman, VP bij Gartner

	Bezocht op	: 9 maart 2005
	Dateert van	: maart 2004
	URI	: http://www.richtech.com/events/zimmerman.ppt
[Gartner2]	Titel	: "Gartner Says System Downtime Caused by Software Vulnerabilities will Triple by 2008 for Firms that Don't Take Proactive Security Steps"
	Auteur(s)	: -
	Bezocht op	: 3 maart 2005
	Dateert van	: 13 september 2004
	URI	: http://www3.gartner.com/press_releases/asset_104887_11.html
[Gomez1]	Titel	: "[prelude-devel] IDS vs. SIM/company contributions" (mailinglist)
	Auteur(s)	: Gene Gomez
	Bezocht op	: 11 april 2005
	Dateert van	: 16 april 2004
	URI	: http://www.prelude-ids.org/pipermail/prelude-devel/2004-April/000257.html
[Gorton1]	Titel	: "Extending Intrusion Detection with Alert Correlation and Intrusion Tolerance" (licentiate thesis)
	Auteur(s)	: Dan Gorton
	Bezocht op	: 5 april 2005
	Dateert van	: 2003
	URI	: http://www.ce.chalmers.se/~daane/LicentiateThesis_031209.pdf
[Hofmeyr1]	Titel	: "Intrusion Detection using Sequences of System Calls"
	Auteur(s)	: Steven A. Hofmeyr, Stephanie Forrest en Anil Somayaji
	Bezocht op	: 19 maart 2005
	Dateert van	: 18 augustus 1998
	URI	: http://www.cse.ogi.edu/~jin/papers/jcs-accepted.pdf
[MAFTIA1]	Titel	: "MAFTIA Conceptual Model"
	Auteur(s)	: Robert Stroud (IBM Research Lab, Zürich)
	Bezocht op	: 27 maart 2005
	Dateert van	: februari 2003
	URI	: http://www.maftia.org/presentations/papers/WP1.pdf
[MAFTIA2]	Titel	: "Intrusion Detection: Eliminating False Alarms"
	Auteur(s)	: Andreas Wespi et al (IBM Research Lab, Zürich)
	Bezocht op	: 27 maart 2005
	Dateert van	: februari 2003
	URI	: http://www.maftia.org/presentations/papers/wp3.pdf
[IBM1]	Titel	: "IBM Tivoli Risk Manager – Product overview"
	Auteur(s)	: -

	Bezocht op	: 11 april 2005
	Dateert van	: -
	URI	: http://www.ibm.com/software/tivoli/products/risk-mgr/
[IBM2]	Titel	: "IBM e-business on demand: bedrijfsvoering"
	Auteur(s)	: -
	Bezocht op	: 18 april 2005
	Dateert van	: -
	URI	: http://www-5.ibm.com/e-business/nl/evolving/ondemand/operating/automation_off08.html
[IBM3]	Titel	: "Towards a Taxonomy of Intrusion Detection Systems and Attacks"
	Auteur(s)	: D. Alessandri, C. Cachin, M. Dacier, O. Deak, K. Julisch, B. Randell, J. Riordan, A. Tscharner, A. Wespi, C. Wüest
	Bezocht op	: 23 maart 2005
	Dateert van	: 6 september 2001
	URI	: http://domino.watson.ibm.com/library/cyberdig.nsf/papers/5FA980EB952E09D085256AC600535997/$File/rz3366.pdf
[ICSA1]	Titel	: "ICSA Labs IDS Consortium develops Alert Specification - SDEE"
	Auteur(s)	: -
	Bezocht op	: 11 april 2005
	Dateert van	: -
	URI	: http://www.icsalabs.com/html/communities/ids/sdee/
[ICSA2]	Titel	: "IDSC Membership Page"
	Auteur(s)	: -
	Bezocht op	: 11 april 2005
	Dateert van	: 11 april 2003
	URI	: http://www.icsalabs.com/html/communities/ids/membership/index.shtml
[IEEE2]	Titel	: "Validation of Sensor Alert Correlators"
	Auteur(s)	: Joshua Haines, Dorene Ryder, Laura Tinnel en Stephen Taylor
	Bezocht op	: 23 maart 2005
	Dateert van	: januari 2003
	URI	: http://www.cs.utk.edu/~ltinnel/papers/200301IEEESecurityPrivacy_Validation.pdf
[IETF1]	Titel	: "The Intrusion Detection Message Exchange Format"
	Auteur(s)	: B. Feinstein , H. Debar en D.Curry en (idwg)
	Bezocht op	: 18 maart 2005
	Dateert van	: 27 januari 2005
	URI	: http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-14.txt
[IETF2]	Titel	: "The Intrusion Detection Message Exchange Format"
	Auteur(s)	: B. Feinstein, G. Matthews en J. White (idwg)

	Bezocht op	: 23 maart 2005
	Dateert van	: 22 oktober 2002
	URI	: http://www.ietf.org/internet-drafts/draft-ietf-idwg-beep-idxp-07.txt
[InfoWorld1]	Titel	: "Managing it all"
	Auteur(s)	: David L. Margulius
	Bezocht op	: 23 maart 2005
	Dateert van	: 10 januari 2003
	URI	: http://www.infoworld.com/articles/fe/xml/ 03/01/13/030113fenexttci.html
[Ingram1]	Titel	: "Autonomous Agents for Distributed Intrusion Detection in a Multi-host Environment" (master thesis)
	Auteur(s)	: Dennis J. Ingram
	Bezocht op	: 20 maart 2005
	Dateert van	: september 1999
	URI	: http://www.csee.umbc.edu/cadip/docs/NetworkIntrusion/ ingramthesis.htm
[Innella1]	Titel	: "The Evolution of Intrusion Detection Systems"
	Auteur(s)	: Paul Innella CISSP
	Bezocht op	: 23 maart 2005
	Dateert van	: 16 november 2001
	URI	: http://www.securityfocus.com/infocus/1514
[Innella2]	Titel	: "Managing Intrusion Detection Systems in Large Organizations"
	Auteur(s)	: Paul Innella CISSP, Oba McMillan CISSP en David Trout CISA CISSP
	Bezocht op	: 27 maart 2005
	Dateert van	: 9 april 2002
	URI	: http://www.securityfocus.com/infocus/1564 (deel 1)
	URI	: http://www.securityfocus.com/infocus/1567 (deel 2)
[ISI1]	Titel	: "Common Intrusion Detection Framework"
	Auteur(s)	: -
	Bezocht op	: 18 maart 2005
	Dateert van	: 10 september 1999
	URI	: http://www.isi.edu/gost/cidf
[Julisch1]	Titel	: "Clustering Intrusion Detection Alarms to Support Root Cause Analysis"
	Auteur(s)	: dr. Klaus Julisch
	Bezocht op	: 2 april 2005
	Dateert van	: november 2003
	URI	: http://www.zurich.ibm.com/~kju/tissec.pdf
[Kang1]	Titel	: "Benchmark Data sets for Intrusion Detection System in Bag of

		System Calls representation”
	Auteur(s)	: Dae-Ki Kang (PhD student)
	Bezocht op	: 18 maart 2005
	Dateert van	: 7 maart 2005
	URI	: http://www.cs.iastate.edu/~dkkang/IDS_Bag/
[Keldsen1]	Titel	: “Security Management Systems:An ‘Oversite Layer’ for Layers of Defense”
	Auteur(s)	: David Keldsen GSEC
	Bezocht op	: 27 maart 2005
	Dateert van	: augustus 2003
	URI	: http://www.intrusic.com/Images/Keldsen_Dan_GSEC.pdf
[Kemmerer1]	Titel	: “State Transition Analysis: A Rule-Based Intrusion Detection System”
	Auteur(s)	: R. Kemmerer, E. Ilgun en P. Porras
	Bezocht op	: 27 maart 2005
	Dateert van	: maart 1995
	URI	: http://www.csl.sri.com/papers/stat-paper/stat-paper.ps.gz
[King1]	Titel	: “CIDS: Causality-based Intrusion Detection System”
	Auteur(s)	: Samuel T. King, Z. Morley Mao en Peter M. Chen
	Bezocht op	: 2 april 2005
	Dateert van	: 2004
	URI	: http://www.eecs.umich.edu/techreports/cse/2004/CSE-TR-493-04.pdf
[Kruegel1]	Titel	: “Distributed Pattern Detection for Intrusion Detection”
	Auteur(s)	: Christopher Kruegel en Thomas Toth
	Bezocht op	: 28 maart 2005
	Dateert van	: 30 april 2002
	URI	: http://www.infosys.tuwien.ac.at/Staff/tt/publications/Distributd_Pattern_Detection_for_Intrusion_Detection.pdf
[Lemonnier1]	Titel	: “Protocol Anomaly Detection in Network-based IDSs”
	Auteur(s)	: Erwan Lemmonier
	Bezocht op	: 31 maart 2005
	Dateert van	: 28 juni 2001
	URI	: http://erwan.lemonnier.free.fr/exjobb/report/protocol_anomaly_detection.pdf
[Li1]	Titel	: “UCLog: A Unified, Correlated Logging Architecture for Intrusion Detection”
	Auteur(s)	: Zhenmin Li, Jed Taylor, Elizabeth Partridge, Yuanyuan Zhou, William Yurcik, Cristina Abad, James J. Barlow en Jeff Rosendale
	Bezocht op	: 2 april 2005
	Dateert van	: 2004

	URI	: http://www.ncassr.org/projects/sift/papers/uclog.pdf
[Locasto1]	Titel	: "Collaborative P2P Intrusion Detection"
	Auteur(s)	: Michael E. Locasto, Janak J. Parekh, Sal Stolfo, Angelos D. Keromytis, Tal Malkin, Vishal Misra
	Bezocht op	: 31 maart 2005
	Dateert van	: September 2004
	URI	: http://fae.cs.columbia.edu/media/main.pdf
[Maglaris1]	Titel	: "A Distributed Intrusion Detection Prototype using Security Agents"
	Auteur(s)	: B. Maglaris, V. Chatzigiannakis, G. Androulidakis en M. Grammatikou
	Bezocht op	: 30 maart 2005
	Dateert van	: juni 2004
	URI	: http://www.hpovua.org/PUBLICATIONS/PROCEEDINGS/11_HPOVUAWS/HP-OVUA%202004%20Papers/Wednesday%20June%2023,%202004/3.2%20S%20Session%20-%20Security/S_5_A%20Distributed%20Intrusion%20Detection%20.pdf
[Mell1]	Titel	: "A denial-of-service resistant intrusion detection architecture" (artikel in Elsevier Science's Computer Networks, nr. 34)
	Auteur(s)	: Peter Mell, Donald Marks en Mark McLarnon
	Bezocht op	: 28 maart 2005
	Dateert van	: 2000
	URI	: http://downloads.securityfocus.com/library/article.pdf
[Mitre1]	Titel	: "Common Vulnerabilities and Exposures"
	Auteur(s)	: -
	Bezocht op	: 27 maart 2005
	Dateert van	: -
	URI	: http://www.cve.mitre.org/
[Nan1]	Titel	: "Distributed Intrusion Detection Systems"
	Auteur(s)	: Tjerk Nan en Jeroen van Beek
	Bezocht op	: 19 maart 2005
	Dateert van	: 2 juli 2004
	URI	: http://www.os3.nl/jvb/docs/DistributedIntrusionDetectionPlatform.pdf
[Ning1]	Titel	: "Alert Correlation through Triggering Events and Common Resources"
	Auteur(s)	: Peng Ning en Dingbang Xu
	Bezocht op	: 20 maart 2005
	Dateert van	: 30 oktober 2004
	URI	: http://discovery.csc.ncsu.edu/~pning/pubs/acsac04b.pdf
[Ning2]	Titel	: "Building Attack Scenario's though Integration of Complementary

		Alert Correlation Methods”
	Auteur(s)	: Peng Ning, Dingbang Xu, Christopher G. Healey en Robert St. Amant
	Bezocht op	: 16 maart 2005
	Dateert van	: februari 2004
	URI	: http://www.isoc.org/isoc/conferences/ndss/04/ proceedings/Papers/Ning.pdf
[Ning3]	Titel	: “Techniques and Tools for Analyzing Intrusion Alerts”
	Auteur(s)	: Peng Ning, Dingbang Xu, Yun Cui en Douglas S. Reeves
	Bezocht op	: 31 maart 2005
	Dateert van	: mei 2004
	URI	: http://discovery.csc.ncsu.edu/~pning/pubs/tissec04.pdf
[Ning4]	Titel	: “Constructing Attack Scenarios through Correlation of Intrusion Alerts”
	Auteur(s)	: Peng Ning, Yun Cui en Douglas S. Reeves
	Bezocht op	: 31 maart 2005
	Dateert van	: november 2002
	URI	: http://discovery.csc.ncsu.edu/~pning/pubs/ccs02.pdf
[Ning5]	Titel	: “TIAA: A Toolkit for Intrusion Alert Analysis”
	Auteur(s)	: Peng Ning, Yun Cui en Douglas S. Reeves
	Bezocht op	: 3 april 2005
	Dateert van	: 12 februari 2005
	URI	: http://discovery.csc.ncsu.edu/~pning/software/correlator/
[NSS1]	Titel	: “Intrusion Prevention Systems (IPS)”
	Auteur(s)	: -
	Bezocht op	: 18 maart 2005
	Dateert van	: januari 2004
	URI	: http://www.nss.co.uk/WhitePapers/intrusion_prevention_systems.htm
[NWFusion1]	Titel	: “SIM (security information management)”
	Auteur(s)	: -
	Bezocht op	: 5 maart 2005
	Dateert van	: 30 september 2002
	URI	: http://www.nwfusion.com/details/814.html
[NWFusion2]	Titel	: “An XML firewall and more”
	Auteur(s)	: -
	Bezocht op	: 19 maart 2005
	Dateert van	: 17 maart 2004
	URI	: http://www.nwfusion.com/newsletters/web/2004/0315web2.html
[OSSIM1]	Titel	: “Open Source Security Information Managementt”
	Auteur(s)	: -

	Bezocht op	: 7 maart 2005
	Dateert van	: onbekend
	URI	: http://www.ossim.net
[Payer1]	Titel	: "Realtime Intrusion-Forensics A First Prototype Implementation"
	Auteur(s)	: Udo Payer
	Bezocht op	: 2 april 2005
	Dateert van	: mei 2004
	URI	: http://www.terena.nl/library/tnc2004-proceedings/papers/payer.pdf
[Perumal1]	Titel	: "Boar: An Autonomous Agent for Network Intrusion Detection Analysis" (master thesis)
	Auteur(s)	: Archana Perumal
	Bezocht op	: 20 maart 2005
	Dateert van	: december 2004
	URI	: http://csis.pace.edu/thesis/PerumalArchana.pdf
[Prelude1]	Titel	: "Prelude Hybrid Intrusion Detection System"
	Auteur(s)	: Yoann Vandoorselaere
	Bezocht op	: 23 maart 2005
	Dateert van	: onbekend
	URI	: http://www.prelude-ids.org/
[Reactivity1]	Titel	: "Reactivity: The Secure Web Services Deployment System"
	Auteur(s)	: -
	Bezocht op	: 19 maart 2005
	Dateert van	: -
	URI	: http://www.reactivity.com
[Rieck1]	Titel	: "An Intelligent Host-Based Intrusion Detection System"
	Auteur(s)	: Konrad Rieck (Universiteit van Berlijn)
	Bezocht op	: 22 maart 2005
	Dateert van	: april 2004
	URI	: http://people.roqe.org/kr/docs/ml-ids-talk.pdf
[SFocus1]	Titel	: "Intrusion Detection Terminology (Part Two)"
	Auteur(s)	: Andy Cuff
	Bezocht op	: 23 maart 2005
	Dateert van	: 24 september 2003
	URI	: http://www.securityfocus.com/infocus/1733
[SFocus2]	Titel	: "IDS Correlation of VA Data and IDS Alerts"
	Auteur(s)	: Neil Desai
	Bezocht op	: 23 maart 2005
	Dateert van	: 30 juni 2003
	URI	: http://www.securityfocus.com/infocus/1708

[Sielken1] Titel : "Application Intrusion Detection" (masterscriptie)
Auteur(s) : Robert S. Sielken
Bezocht op : 18 maart 2005
Dateert van : mei 1999
URI : http://www.cs.virginia.edu/~jones/IDS-research/Documents/MCS-9905-Sielken.doc

[Snort1] Titel : "Construction and use of a passive ethernet tap"
Auteur(s) : Michael Peters
Bezocht op : 18 maart 2005
Dateert van : onbekend
URI : http://www.snort.org/docs/tap/

[Snort2] Titel : "Bleeding Snort rules."
Auteur(s) : -
Bezocht op : 23 maart 2005
Dateert van : 2005
URI : http://www.bleedingsnort.com/bleeding-all.rules

[Spitzner1] Titel : "The Honeynet Project"
Auteur(s) : -
Bezocht op : 18 maart 2005
Dateert van : onbekend
URI : http://www.honeynet.org

[STAT1] Titel : "State Transition Analysis Technique"
Auteur(s) : -
Bezocht op : 23 maart 2005
Dateert van : onbekend (activiteit bekend tussen 1992 en 2002)
URI : http://www.cs.ucsb.edu/~rsg/STAT/projects.html

[Steffen1] Titel : "E-Security und Datenschutz V"
Auteur(s) : dr. Andreas Steffen
Bezocht op : 20 februari 2005
Dateert van : 2003
URI : http://security.zhwin.ch/crm/pdf/NDS_CRM_Security_5.pdf

[Stillerman1] Titel : "Intrusion Detection for Distributed Applications"
Auteur(s) : Matthew Stillerman, Carla Marceau en Maureen Stillman
Bezocht op : 26 maart 2005
Dateert van : 1999
URI : http://www.atc-nycorp.com/papers/Stillerman_CACM_1999.pdf

[SURFnet1] Titel : "DIDS"
Auteur(s) : -

	Bezocht op	: 22 maart 2005
	Dateert van	: onbekend
	URI	: http://beveiliging.surfnet.nl/info/innovatie/dids.jsp
[Symantec1]	Titel	: "Symantec Enterprise Security Architecture"
	Auteur(s)	: -
	Bezocht op	: 23 maart 2005
	Dateert van	: onbekend
	URI	: http://www.dlt.com/security/pdf/WP-sym-EnterpriseSecurityArchitecture.pdf
[Templeton1]	Titel	: "A Requires/Provides Model for Computer Attacks"
	Auteur(s)	: Steven J. Templeton en Karl Levitt
	Bezocht op	: 3 april 2005
	Dateert van	: november 2001
	URI	: http://dependability.cs.virginia.edu/bibliography/p31-templeton.pdf
[Qin1]	Titel	: "Attack Plan Recognition and Prediction Using Causal Networks"
	Auteur(s)	: Xinzhou Qin en Winke Lee
	Bezocht op	: 2 april 2005
	Dateert van	: 29 september 2004
	URI	: http://www.acsac.org/2004/papers/147.pdf
[Undercoffer1]	Titel	: "Modeling Computer Attacks: A Target-Centric Ontology for Intrusion Detection"
	Auteur(s)	: Jeffrey Undercoffer en John Pinkston
	Bezocht op	: 29 maart 2005
	Dateert van	: 2002
	URI	: http://www.csee.umbc.edu/cadip/2002Symposium/Ont-for-IDS.pdf
[Valdes1]	Titel	: "Probablistic Alert Correlation"
	Auteur(s)	: Alfonso Valdes en Keith Skinner
	Bezocht op	: 11 maart 2005
	Dateert van	: 2001
	URI	: http://www.sdl.sri.com/papers/r/a/raid2001-pac/prob_corr.pdf
[Valeur1]	Titel	: "A Comprehensive Approach to Intrusion Detection Alert Correlation"
	Auteur(s)	: F. Valeur, G. Vigna, C. Kruegel en R. A. Kemmerer
	Bezocht op	: 23 maart 2005
	Dateert van	: mei 2004
	URI	: http://www.cs.ucsb.edu/~rsg/Hidra/Papers/correlation.pdf
[Wikipedia1]	Titel	: "Intrusion-detection system"
	Auteur(s)	: -
	Bezocht op	: 19 maart 2005

	Dateert van	: 9 maart 2005
	URI	: http://en.wikipedia.org/wiki/Intrusion-detection_system
[Yin1]	Titel	: "Selecting Log Data Sources to Correlate Attack Traces for Computer Network Security: Preliminary Results"
	Auteur(s)	: Xiaoxin Yin, Kiran Lakkaraju, Yifan Li en William Yurcik
	Bezocht op	: 2 april 2005
	Dateert van	: 2003
	URI	: http://www.ncassr.org/projects/sift/papers/ictsm03.ppt
[Yoo1]	Titel	: "Protocol Anomaly Detection and Verification"
	Auteur(s)	: InSeon Yoo (PhD student)
	Bezocht op	: 18 maart 2005
	Dateert van	: juni 2004
	URI	: http://diuf.unifr.ch/people/yoois/papers/reviewed/isyoo-IAW04paper443.pdf
[Yoo2]	Titel	: "Adaptive Firewall Model to Detect Email Viruses"
	Auteur(s)	: InSeon Yoo (PhD student)
	Bezocht op	: 19 maart 2005
	Dateert van	: oktober 2004
	URI	: http://diuf.unifr.ch/people/yoois/papers/reviewed/isyoo-iccst04.pdf
[Yu1]	Titel	: "A Novel Framework for Alert Correlation and Understanding"
	Auteur(s)	: Dong Yu en Deborah Frincke
	Bezocht op	: 19 maart 2005
	Dateert van	: april 2004
	URI	: http://www.cs.indiana.edu/~doyu/listenrain/ACNS2004.pdf
[Zimmerman1]	Titel	: "Experimenting with a Policy-Based HIDS Based on an Information Flow Control Model"
	Auteur(s)	: Jacob Zimmerman, Ludovic Mé en Christophe Bidan
	Bezocht op	: 29 maart 2005
	Dateert van	: februari 2004
	URI	: http://www.rennes.supelec.fr/ren/rd/ssir/publis/acsac03_zimmermann_me_bidan.pdf

Bijlage 1: Ontwerpcriteria

Citaat uit [Overbeek1], deel VII, p.9/10/11:

"Voor het toepassen en ontwerpen van technische beveiligingsmaatregelen bestaat een aantal richtlijnen of ontwerpcriteria. Een aantal van deze criteria is al in het begin van de jaren zeventig beschreven (in: Saltzer & Schroeder, 1975).

- Isolatie
  Dit principe houdt in dat hardware en software die relevant zijn voor de beveiliging – de 'Trusted Computing Base' of TCB – altijd zo klein en compact mogelijk gehouden moeten worden. Hoe groter de TCB, hoe moeilijker het zal zijn om te verifiëren of de beveiliging van de TCB voldoende gewaarborgd is. Dit principe wordt onder meer toegepast in reference monitors, security kernels en firewalls; zie hoofdstuk 5.

- Veilige defaults
  Volgens dit principe mag toegang alleen door het systeem worden verleend na expliciete permissie; alles wat niet expliciet is toegestaan, is verboden.

- Volledigheid
  Elke vorm van toegang mag pas plaatsvinden na autorisatie door het systeem. Gebruikers en processen dienen zich daartoe altijd eerst te legitimeren.

- Open ontwerp
  Een goede beveiligingsarchitectuur is niet gebaseerd op het geheimhouden van de gebruikte interne mechanismen ('security by obscurity'), maar gaat juist uit van een open ontwerp. Bij een gesloten ontwerp bestaat het risico dat de werking van internet mechanismen op den duur toch aan het licht komt, bijvoorbeeld door het toepassen van 'reverse engineering' en het uitlekken van ontwerpdocumenten. Het voordeel van een open ontwerp is bovendien dat het intensiever kan worden getest en eenvoudiger kan worden verbeterd.

- Functiescheiding
  Waar mogelijk moeten functies in het systeem worden gesplitst, waarbij de onderscheiden deelfuncties aan verschillende functionarissen moeten worden toegewezen. Gevoelige handelingen mogen alleen door meerdere functionarissen tegelijk worden uitgevoerd (het 4 ogen-principe).

- Beperking
  Het systeem moet zo opgezet zijn, dat gebruikers en processen niet meer functies mogen uitvoeren dan strikt noodzakelijk is. Dit principe staat ook bekend onder de namen 'least privilege' en 'need to know'.

- Compartimenten
  Het systeem moet bestaan uit verschillende compartimenten of modules, waarbij de koppelingen tussen de modules omwille van de controleerbaarheid zo slank mogelijk gehouden worden. Hierdoor neemt de robuustheid en daarmee ook de veiligheid van het systeem toe.

- Ergonomie
  Het systeem moet zo ontworpen zijn dat de kans op menselijke fouten zo klein mogelijk is. Beveiliging moet als het ware geïntegreerd zijn in de systemen en werkprocessen.

Daarnaast is het volgende criterium van belang.

- Redundantie
  De beveiligingsarchitectuur moet bestaan uit een combinatie van maatregelen, zodat de beveiliging niet afhankelijk is van één enkele maatregel.

Omdat men bij informatiebeveiliging niet alleen te maken heeft met onopzettelijke bedreigingen, maar ook met tegenstanders die beveiligingsmaatregelen willens en wetens proberen te omzeilen, kan dit criterium nog verder worden aangescherpt door eisen te stellen aan de diversiteit van de getroffen beveiligingsmaatregelen.

- Diversiteit
  De beveiligingsarchitectuur moet bestaan uit meerdere maatregelen die wezenlijk van elkaar verschillen, zodat het doorbreken van één beveiligingsmaatregel niet automatisch leidt tot de val van het gehele systeem."

Bijlage 2: Voorbeeld beveiligingsarchitectuur (deel 1)

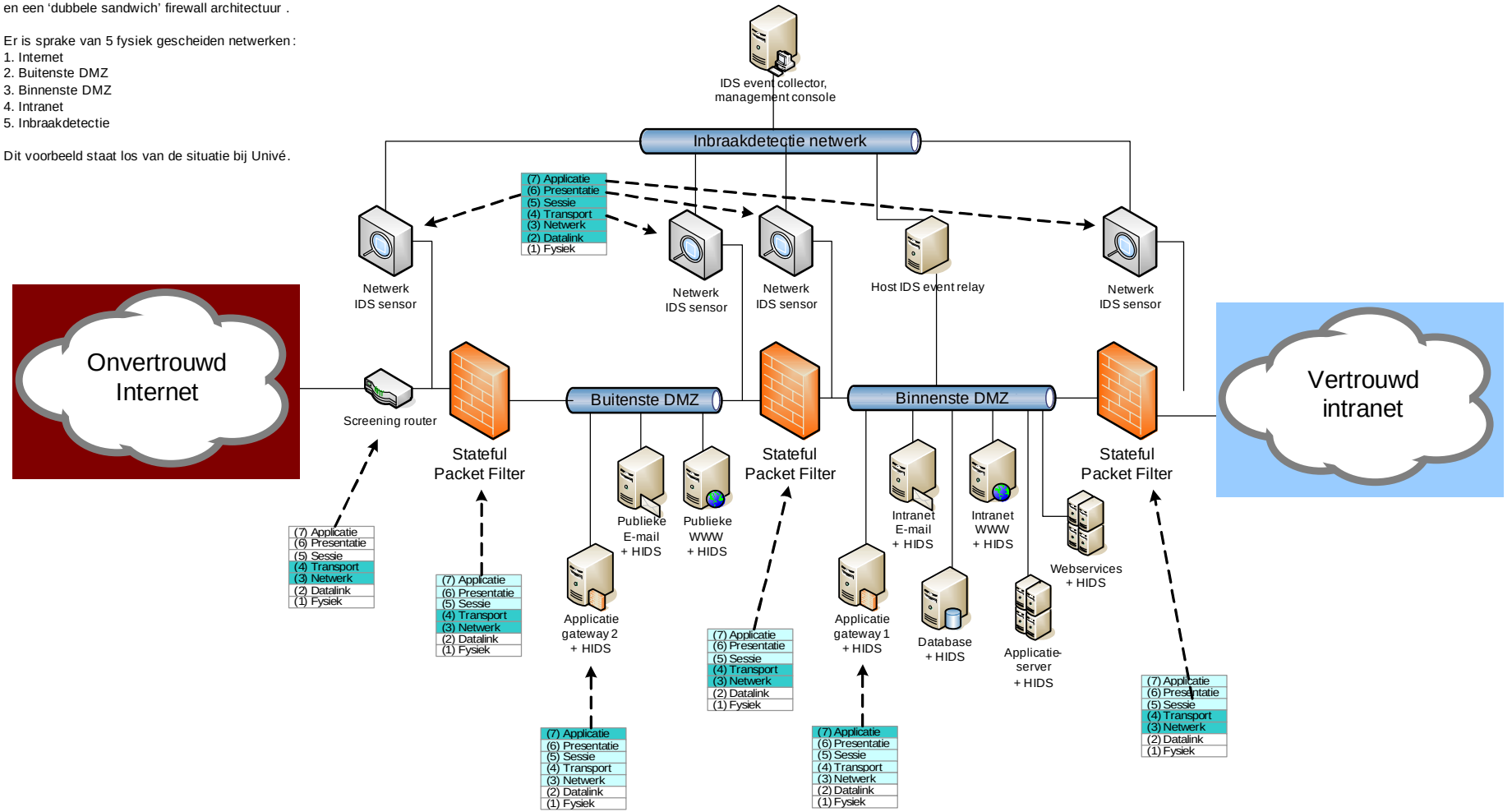
Beveiligingsarchitectuur (externe netwerken)

Monday, March 21, 2005

Dit schema is een weergave van hoe netwerkbeveiliging in het algemeen in een topologie kan worden ingebed door gebruik van IDP en een 'dubbele sandwich' firewall architectuur .

Er is sprake van 5 fysiek gescheiden netwerken:
1. Internet
2. Buitenste DMZ
3. Binnenste DMZ
4. Intranet
5. Inbraakdetectie

Dit voorbeeld staat los van de situatie bij Univé.



Bijlage 3: Voorbeeld beveiligingsarchitectuur (deel 2)

Monday, March 21, 2005

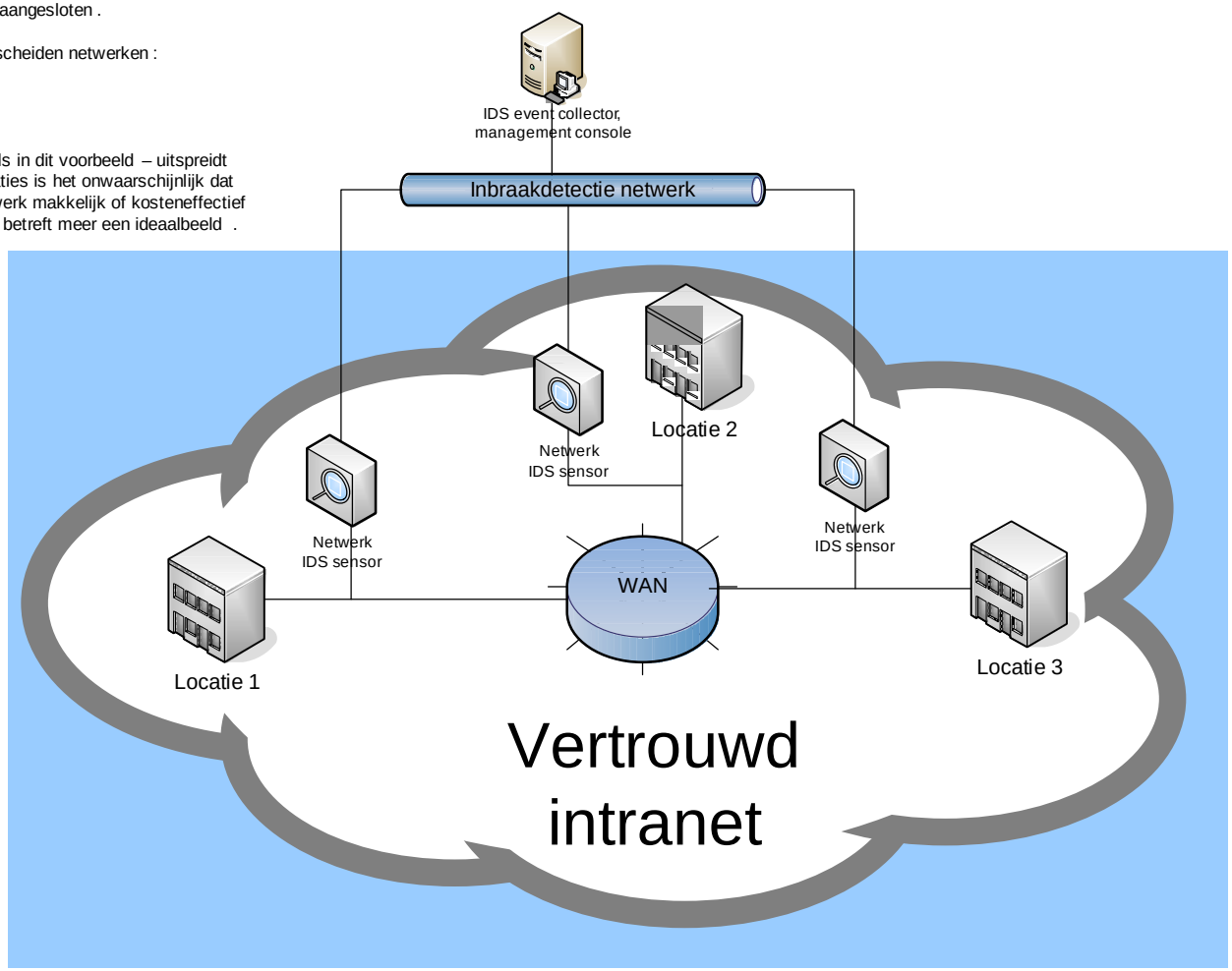
Beveiligingsarchitectuur (interne netwerken)

Dit schema is een weergave van de 'Vertrouwd intranet' -wolk uit het andere schema en staat eveneens los van de situatie bij Univé. Het interne netwerk verspreidt zich via een WAN over meerdere geografische locaties . NIDP is ingezet op de punten waar locaties aan het WAN zijn aangesloten .

Er is sprake van twee fysiek gescheiden netwerken :

1. Intern netwerk
2. Inbraakdetectie netwerk

Bij een intern netwerk dat – zoals in dit voorbeeld – uitspreidt over meerdere geografische locaties is het onwaarschijnlijk dat een fysiek gescheiden IDP-netwerk makkelijk of kosteneffectief realiseerbaar is ; deze weergave betreft meer een ideaalbeeld .



Bijlage 4: Beveiligingsarchitectuur bij Univé (deel 1)

(vertrouwelijk)

Bijlage 5: Beveiligingsarchitectuur bij Univé (deel 2)

(vertrouwelijk)

Bijlage 6: Beveiligingsarchitectuur bij Univé (deel 2 + domeinen)

(vertrouwelijk)

Bijlage 7: Interview met SecMgmt

(vertrouwelijk)

Bijlage 8: Top 20 Questions for your IPS vendor

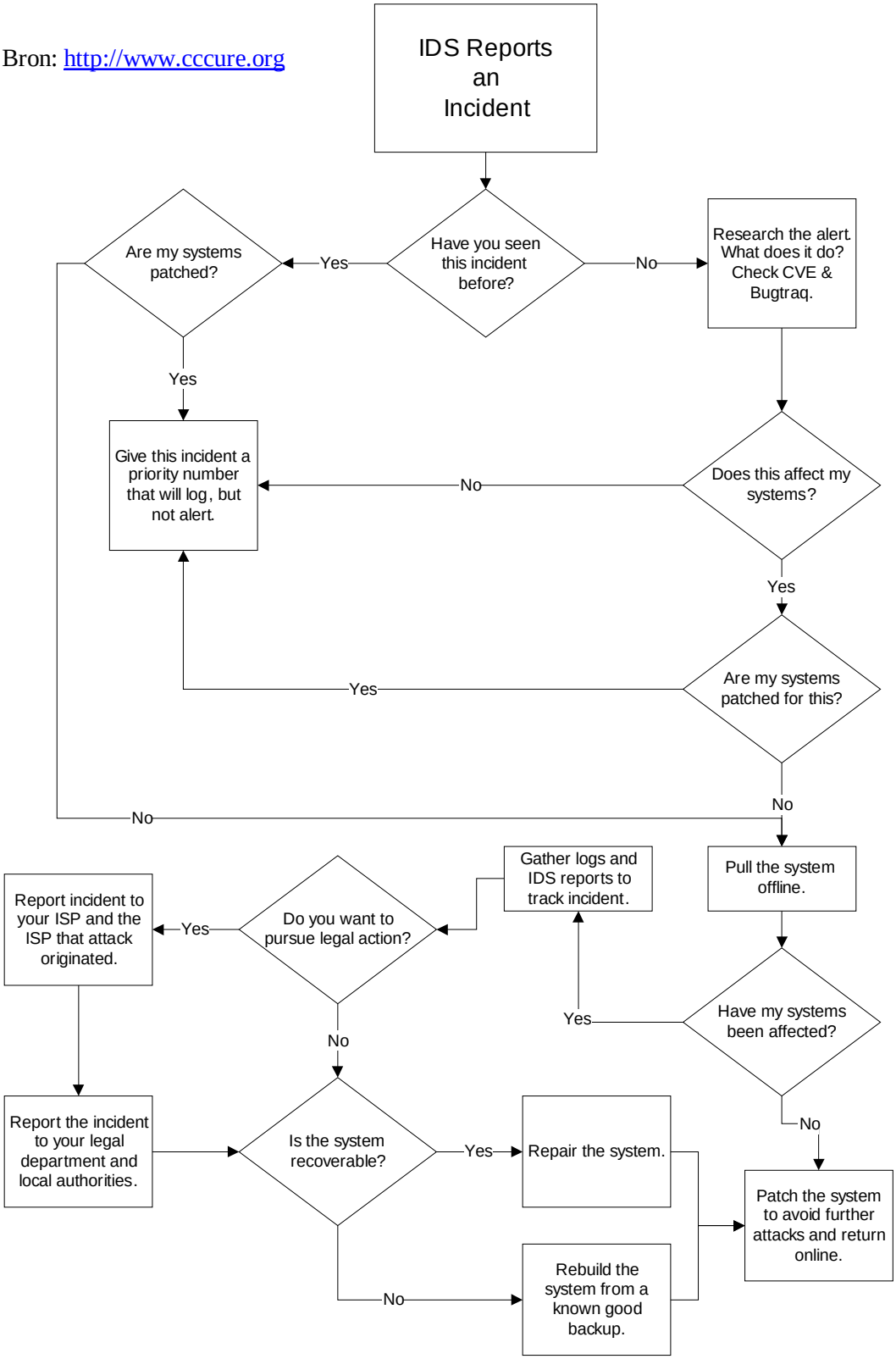
Bron: http://www.nwfusion.com/reviews/2004/0216ips20qs.html (dateert van 16 februari 2004)

Top 20 (or there abouts) Questions for your IPS vendor

1.	Where is this product designed to sit on the network?	
2.	What are the latency, throughput, and jitter claims you make regarding this product and how did you arrive at those numbers? (See Issues with IPS performance numbers.)	
3.	Is this product primarily designed to mitigate attacks with rate-based mechanisms or content/anomaly-based mechanisms?	
	Rate-based products	Content/anomaly-based products
4.	What additional content-based features does this product offer?	What additional rate-based features does this product offer?
5.	What tools does this product offer that let you measure baseline traffic norms?	What is the underlying IDS system in this product?
6.	How granularly can you define which incoming traffic the IPS is going to examine and, eventually, limit or block?	How big is the signature database? Which of those signatures are turned on by default? What is the update mechanism for new signatures?
7.	How sophisticated are the rate detection and control mechanisms offered? (For example, can they detect just a flood or can they track potentially malicious single connections over time?)	How do you see, enable, disable, and modify attributes of bad traffic signatures?
8.	How does this product discover machines and services running on the network that need IPS protection?	
9.	Does your product have a learning mode, how long does it take, and how do you recommend running it in learning mode?	
10.	How easily can you run this product in an alert-only mode?	
11.	What kinds of traffic can this product block (DoS attack UDP protocol attacks, buffer overflow attacks, fragmentation attacks, spoofing attacks (inbound/outbound), application-layer attacks, for example?	
12.	What are the action options offered by this product once malicious traffic is discovered (drop-only, pass and track, pass and alert, pass but limit, for example).	
13.	What kind of communication happens between this IPS device and either my installed firewall or a built-in one?	
14.	Does the product provided centralized configuration and/or management capabilities?	
15.	What are your configuration options (rules per port, per system, for example.)?	
16.	Does the product provided centralized configuration and/or management capabilities?	
17.	What is the overall strategy for alert you of both malicious activity and of blocked traffic?	
18.	What are the product's reporting capabilities?	
19.	Does this product have the ability to connect to a Security Event Management system via some event reporting mechanism?	
20.	If this device's log fills, will it continue to operate without logging?	
21.	Does the vendor offer log analysis tools for forensics and capacity planning?	
22.	What secure management access methods does this device support, such as SNMPv3 or SSHv2? Are these the only methods enabled by default?	

Bijlage 9: Incident Response Flowchart

Bron: http://www.cccure.org



Bijlage 10: Kruisverwijzing onderzoeksvragen

Voorafgaand aan dit vooronderzoek zijn de onderstaande onderzoeksvragen geformuleerd. Achter elke vraag staat het hoofdstuk waarin die vraag wordt geadresseerd.

---

1. Wat is intrusion detection/prevention?	H2
a) Wat is intrusion detection/prevention?	H2.1
b) Hoe werkt intrusion detection?	
I. Welke detectiemethoden zijn er?	H2.3
II. Hoe ziet een intrusion detection architectuur er uit?	H2.2
c) Hoe werkt intrusion prevention?	
I. Hoe kan preventie worden gerealiseerd?	H2.2
II. Hoe ziet een intrusion prevention architectuur er uit?	H2.2
2. Wat is geconsolideerde logging?	H3
a) Wat is geconsolideerde logging?	H3.1.3
b) Wat is de relatie van logging met intrusion detection?	H3.4
c) Hoe werkt consolidatie van logging?	
I. Wat is aggregatie, normalisatie, correlatie?	H3.5
II. Hoe worden loggegevens verkregen?	H3.1
d) Hoe kunnen meldingen van verschillende bronnen worden gecorreleerd?	H3.6
I. Welke bronnen leveren beveiligingsgerelateerde informatie?	H3.2
II. Welke methoden bestaan er voor correlatie?	H3.6
III. Hoe werken die methoden en wat zijn de beperkingen?	H3.6.1 t/m H3.6.4
3. Wat zijn de randvoorwaarden voor de inzet van beide maatregelen bij Univé?	H4
a) Wat zijn de randvoorwaarden voor intrusion detection/prevention?	H4.4
I. Wat zijn de technische randvoorwaarden?	H4.4.1
à Op welke punten in de infrastructuur is intrusion detection of prevention wenselijk? (business eisen, technisch/operationele eisen)	
à Hoe kan intrusion detection/prevention op elk punt worden ingezet?	
II. Wat zijn de beheermatige randvoorwaarden?	H4.4.2
à Welk kennisniveau is beschikbaar voor onderhoud/beheer?	
à Hoeveel tijd /is beschikbaar voor onderhoud/beheer?	
b) Wat zijn de randvoorwaarden voor geconsolideerde logging?	H4.4
I. Wat zijn de technische randvoorwaarden?	H4.4.1
à Van welke systemen dienen bij Univé de logs te worden gemonitord?	
à Welke mogelijkheden/interfaces bieden die systemen tot logging?	
II. Wat zijn de beheermatige randvoorwaarden?	H4.4.2
à Welk kennisniveau is beschikbaar voor onderhoud/beheer?	
à Hoeveel tijd is beschikbaar voor onderhoud/beheer?	
c) Welke oplossing voldoet aan die randvoorwaarden?	H4.5, H4.6