



SIEM EVOLUTION

A day in the life of a Security Architect

Stijn Vande Castele

9 September 2009



What do I do?



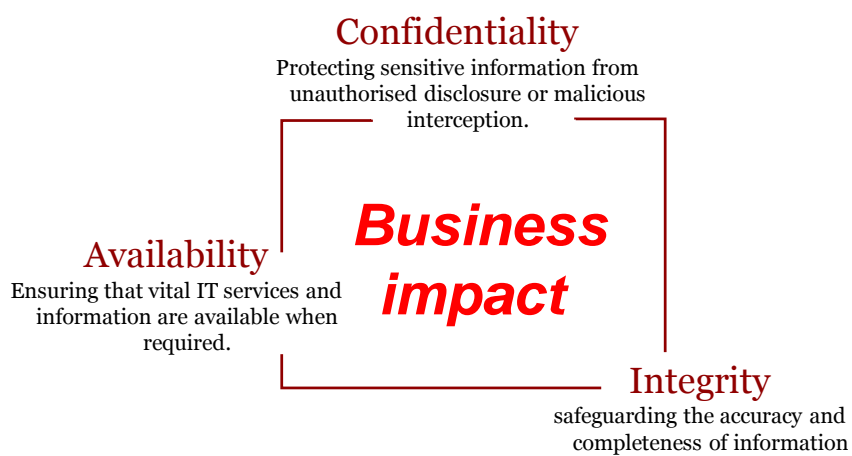
- My team provides solutions to underpin the on-site and managed SIEM services, with a focus on the what and the **how!**
- Engineer a grid/cloud/infrastructure to deliver these services to customers (enterprises) with a focus on security operations.
- Steer the service catalogue with fresh use cases (add value).
- Integrate technologies with our architecture to build automations and enhance the richness of our private SIEM clouds based on ArcSight technologies.
 - Data sources configuration documents
 - Automatic ticket creation
 - Portal visualizations
 - Self monitoring
- 3rd line support for security management related infrastructure problems (application/systems) and forensic security investigations.
- Advice in general on a diverse range of pre-sales and service questions within this domain.
- **Objective:** centre of excellence (SIEM think-thank for the BGC group)

Agenda

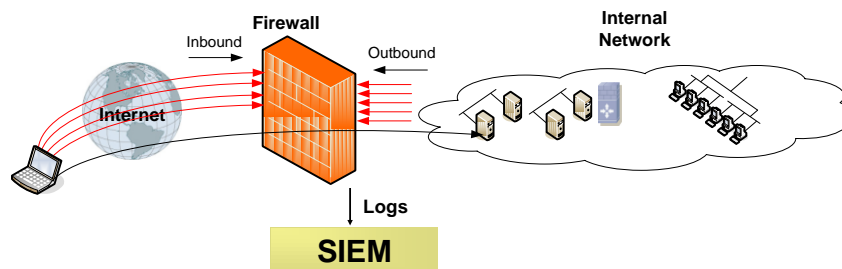


- **Security Monitoring**
- SIEM architectures
- Situational awareness
- Use Cases

The **three** key principles



Firewall Security Monitoring



Inbound Top Drops

- Active list with confirmed scanners from Internet
- If firewall accepts from IP addresses in the active list, increase event priority

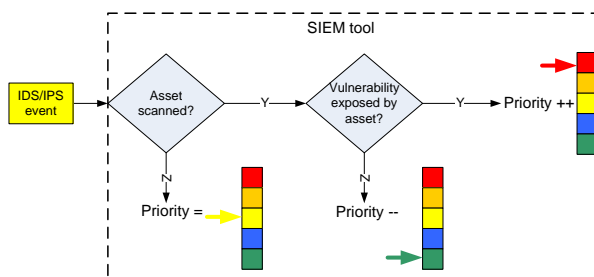
Outbound Top Drops

- Can spot infected internal systems or configuration errors (eg. wrong DNS or NTP client configuration)

Security Analysis



- Unlike firewalls, IDS/IPS provides information up to OSI layer 7 via signature based detection methods
- Typical attacks detected by IDS/IPS: Worms, Exploits, Brute force attacks, Backdoors, Cover channels.
- IDS/IPS are best placed where “threat x asset value” is high (eg. DMZ, server farm)
- IDS/IPS provide input for SIEM tools to correlate with Vulnerability and Asset (VA) data


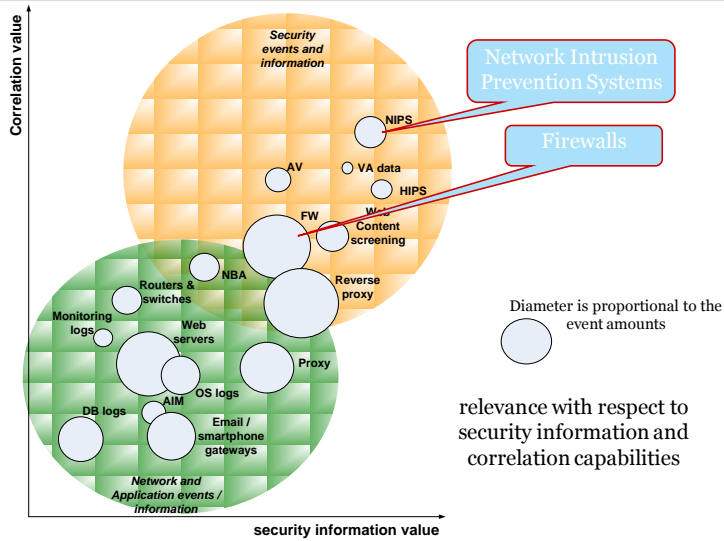


IAS Security Monitoring



Connectors Matrix				
Device vendor	Device product	Event Transfer Method	Service	Connector type
Arcsight	ArcSight Manager	Arcsight login	443/TCP	SuperConnector
Arcsight	ArcSight Database	Local ArcSight DB connection	443/TCP	Partition_archiver
Juniper	SBR	FTP (Device -> TSP) + File Reader	21/TCP	SBR
Juniper	SA, ISG, IPS, IDP, Netscreen			
Infoblox	Infoblox	Syslog (Device -> TSP)	514/UDP	Syslog daemon
Cisco	ASA, PIX, FWSM			
Cisco	Ironport	FTP (Device -> TSP) + File reader	21/TCP	IronPort
CheckPoint	FireWall-1, VPN-1, SmartDefense	LEA connection (TSP -> Device)	18184/TCP	CheckPoint
BlueCoat	Proxy SG (includes AV)	FTP (Device -> TSP) + File Reader	21/TCP	BlueCoat
Microsoft	Windows	SMB (Device <-> TSP) + File Reader	137,138/UDP ; 135,139,445/TCP	Windows Unified
Cisco	IPS, IDS, IDSM-2	SDEE connection (TSP -> Device)	443/TCP	Cisco SDEE

Log Sources

Agenda



- Security Monitoring
- **SIEM architectures**
- Situational awareness
- Use Cases

Security Information & Event Management



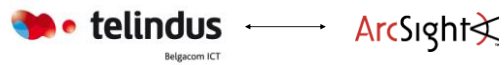
The SIEM platform is used for the *Security Analysis & Security Reporting* services.

The SIEM has the following functions:

- Collection, Normalize and Event categorization
- Threat priority evaluation and asset categorization
- Advanced real-time correlation capability
- Forensics-on-the-fly (monitor, analysis and action)
- Database partitions and archiving
- Extended and flexible log retention *



Some history...



ArcSight 2.1 (Sept 2003)

ArcSight 2.2 (POC)

ArcSight 2.5 (Production Jan 2004)

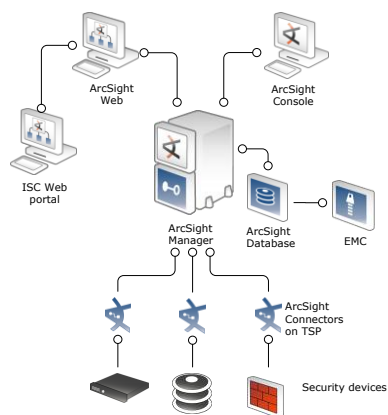
ArcSight 3.0 (Production Oct 2004)

ArcSight 3.5 (Production Mar 2006)

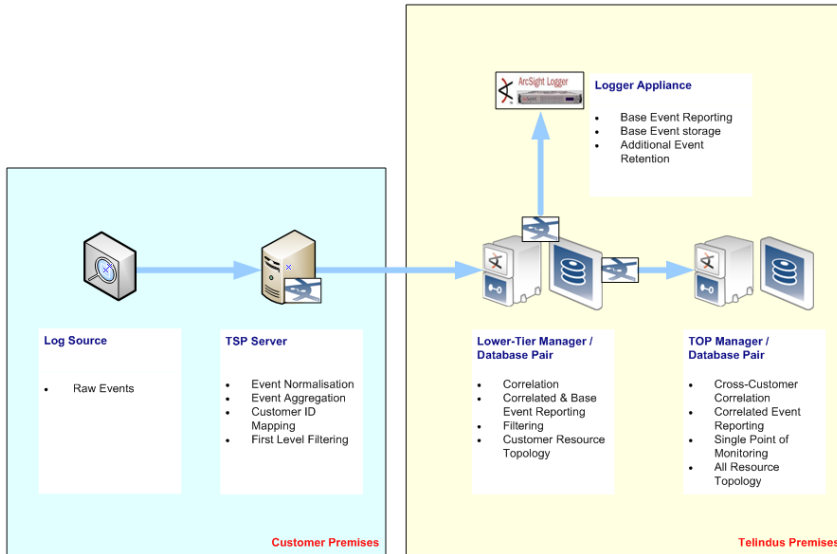
ArcSight 4.0 (Production Sept 2007)



MONOLITIC PLATFORM



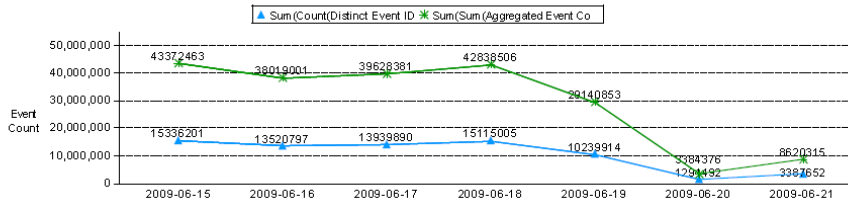
Security Event Lifecycle



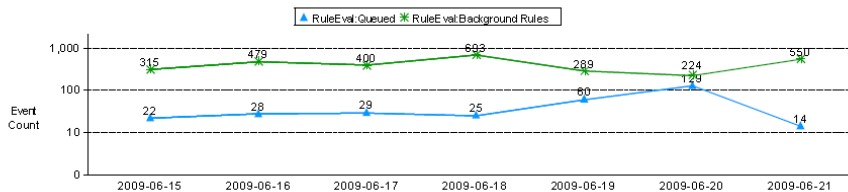
SIEM audit report



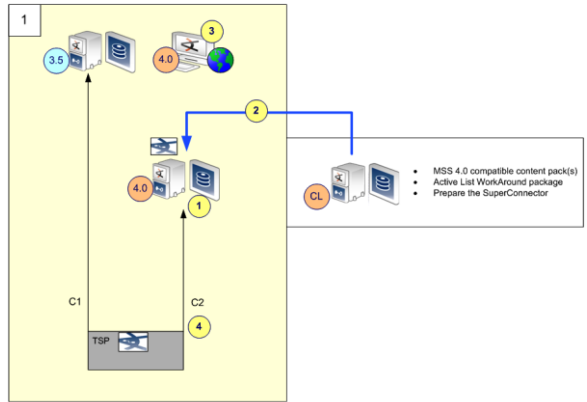
Base Event Count Chart



EOI Count Chart

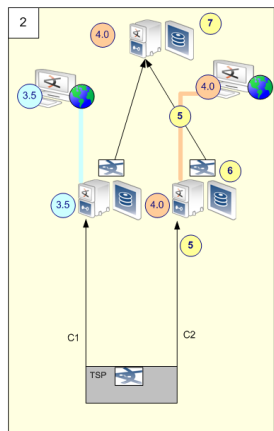


Bubble Migration

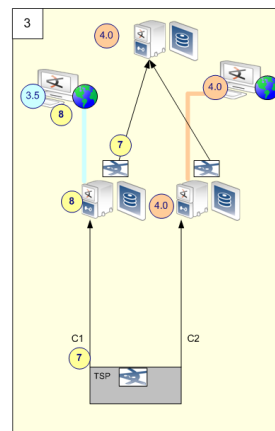


- 1 Stage MGR/DB (OS/ArcSight)
- 2 Deploy MSS content
- 3 Add 4.0 ArcSight WEB instance
- 4 Activate C2 (second ESM destination)

Bubble Migration ctd.



- 5 Integrate 4.0 MSS with ASWeb and TOP
- 6 Fine-tune MSS content
- 7 Operational Shadow



- 7 Remove C1 & Remove SuperConnector filter
- 8 Bring down systems

Agenda



- Security Monitoring
- SIEM architectures
- **Situational awareness**
- Use Cases

Example of event context

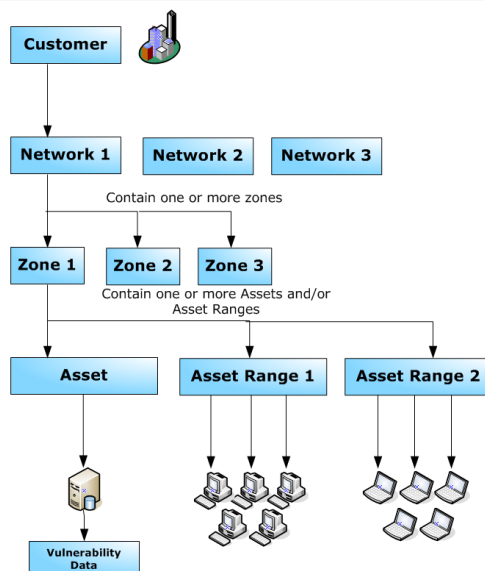


**Does this event
threaten business?**

SIEM security topology



Integrator
with



Security Topology



Integrator
with



- Topology provides :
 - Information about the « context »
 - Understanding on Business logic
 - Information about the target and it's environment
 - Relevance factor in the Threat formula (low or high priority events)
- A good (descriptive) topology implies :
 - Less false positives
 - More accurate true positives
 - Increased information level in the tickets
 - Better incident handling
- Initial Audit and Strategy assignment, but then...
- Keeping up-to-date through technologies?

Agenda



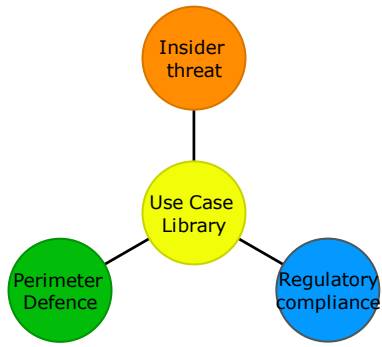
- Security Monitoring
- SIEM architectures
- Situational awareness
- **Use Cases**

Use Case approach



“How raw event data is processed into actionable information and how this information is utilized and delivered as output is at the heart of the SIEM Use Case development.”

Use Case library



MSS Malware Datamonitor sample



Top 20 Denied malware destinations							
AttackerAddress	Request Url Host	Total	Very High	High	Medium	Low	Very Low
	217.170.77.150	7000	0	7000	0	0	0
	62.176.16.161	6996	0	6996	0	0	0
	85.255.120.254	6996	0	6996	0	0	0
	update.thunderdownloads.com	3000	0	3000	0	0	0
	partners.hotbar.com	1811	0	1811	0	0	0
	update.thunderdownloads.com	1629	0	1629	0	0	0
	archive.easydownloadsoft.com	1393	0	1393	0	0	0
	archive.easydownloadsoft.com	1386	0	1386	0	0	0
	partners.hotbar.com	1330	0	1330	0	0	0
	77.91.227.179	584	0	584	0	0	0
	webssoftcodecdriver.com	522	0	522	0	0	0
	alapp.whenu.com	490	0	490	0	0	0
	updates.hotbar.com	480	0	480	0	0	0
	alapp.whenu.com	408	0	408	0	0	0
	alapp.whenu.com	348	0	348	0	0	0
	updates.hotbar.com	340	0	340	0	0	0
	ping.180solutions.com	319	0	319	0	0	0
	updates.hotbar.com	295	0	295	0	0	0
	archive.easydownloadsoft.com	279	0	279	0	0	0
	app.whenu.com	273	0	273	0	0	0
others		5856	0	5856	0	0	0

5/22/2008 10:00:00 AM GMT - 5/23/2008 9:27:15 AM GMT


Conclusions



- Carefully plan your SIEM migrations with business and operations!
- Make checklists, cheat sheets and technical notes to educate your security analysts on new evolutions.
- Keep a change log for SIEM content adaptations. Automate!
- Think out of the box, SIEM has a lot of potential but KISS towards the outside.
- Request (simple) KPI's on how your application/service is evolving.
- Learn and measure how your implementation evolves over time!
- Follow a use case framework!
- Use intake templates to facilitate the scoping exercise towards your client.
- Centralize your efforts, look for partners and create centre of excellence in your organization around security monitoring.

Questions?



 stijn.vandecasteele@telindus.be

 <http://www.linkedin.com/in/ictsecurity>

 <http://www.twitter.com/securityworld>