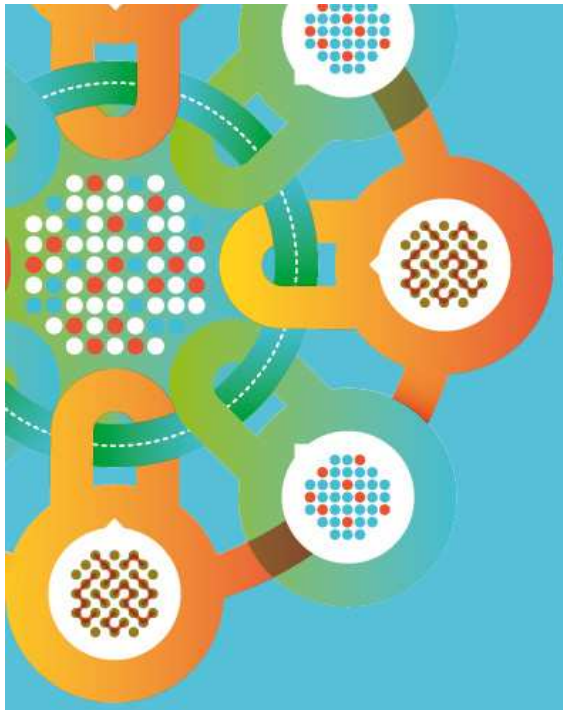


IBM Forum Segrate - Milano

18 settembre:
Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

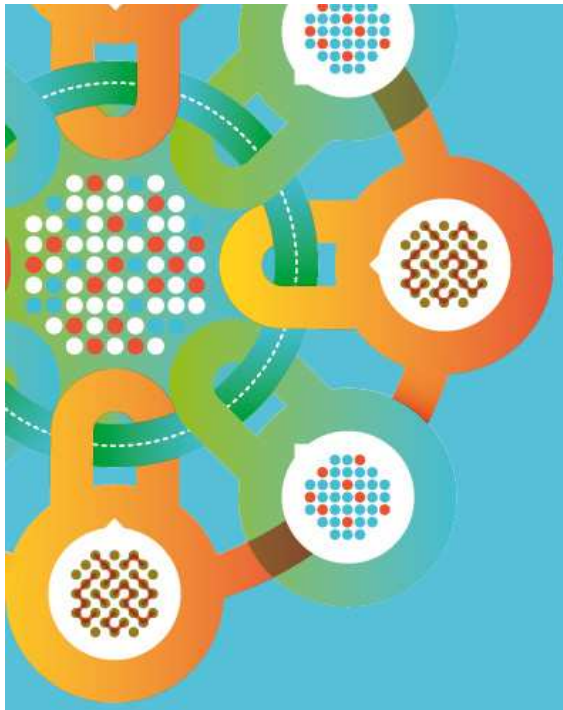
IBM Security Intelligence

- Technical Dive into QRadar

  Jean-Luc Labbe

- Disegno di una Soluzione SIEM

  Giovanni Abbadessa



IBM Forum Segrate - Milano

18 settembre:
Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

IBM Security Intelligence

- Technical Dive into QRadar

Jean-Luc Labbe

- Disegno di una Soluzione SIEM

Giovanni Abbadessa

The Challenges Organizations Are Facing

What Customers Struggle With Most

- Recently failed compliance audit or experienced security breach
- Manual data gathering for compliance reports & audits
- Unable to detect security breaches and anomalous activity quickly
- Unable to detect insider theft, fraud or malicious activity
- Unable to monitor social media and mobile activity for data security risks
- Unable to monitor network activity in virtual and cloud environments
- Existing log management or SIEM solution isn't flexible and scalable
- Unable to conduct effective forensic investigations after security breaches
- Misconfigured network & security devices create risks

The Challenges Organizations Are Facing

Protecting the perimeter is no longer enough…
…Silo'ed point products will not secure the enterprise

Advanced

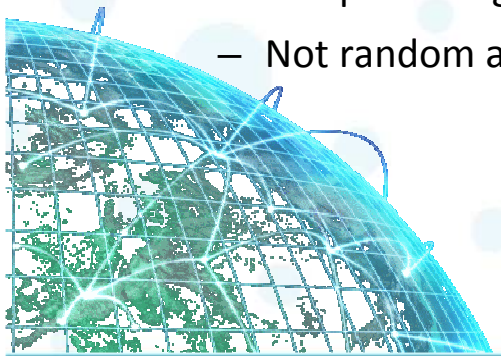
- Using exploits for unreported vulnerabilities, aka a "zero day"
- Advanced, custom malware that is not detected by antivirus products
- Coordinated attacks using a variety of vectors

Persistent

- Attacks lasting for months or years
- Attackers are dedicated to the target – they will get in
- Resistant to remediation attempts

Threat

- Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
- Not random attacks – they are actually "out to get you"



The APT techniques used by attackers have eroded the effectiveness of traditional defenses including firewalls, intrusion prevention systems and antivirus - ***leaving holes in the network***

Solving A Security Issue Requires Broader Context

The “Why More Context”

Organizations are failing at early breach detection, with more than 85% of breaches undetected by the breached organization.*

(...)

It is the **combination** of **real-time security monitoring**, **context** (threat, vulnerability, user, asset, data and application) and **"smart eyeballs"** on dally activity reports that will improve your chances of early breach detection beyond the current 15% success rate.

Gartner “Using SIEM for Targeted Attack Detection” (March 2012)

* 2011 Data Breach Investigations Report — Verizon Business Systems.

The Challenges Organizations Are Facing

Because Organizations Need To Address…

• Improve the overall visibility the Organization's Security & Compliance posture

• Improve the organization's ability to:

- Cost effectively minimize the possibility of regulatory non-compliance,
- Detect (advanced persistent) threats/attacks in real time,
- Have a proactive approach to security & compliance to protect their brand.

• Reduce proliferation of tools, vendors & technologies through consolidation

- Consolidate silos of network & security information to gain a single view across the enterprise.

The Challenges Organizations Are Facing

So How We Can Help?

A single integrated solution able to address the following two areas:

Compliance

- Lower the costs of managing audits and maintaining compliance with the full set of applicable regulations and policies.
- Minimize the possibility of regulatory non-compliance.

Security

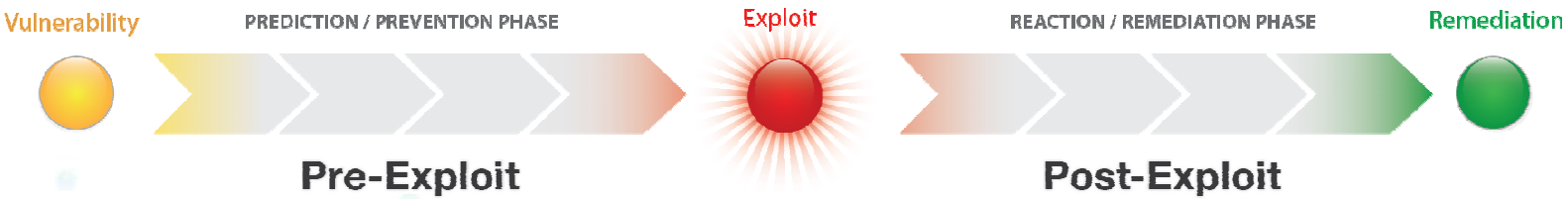
- Detect potential advanced threats and attacks in real-time via advanced analytics.
- Consolidate silos of network & security information to gain a single view across the enterprise.
- Answer the "What if" questions ahead of time to further minimize the risks.

The end Goal is to:
(Cost) Effectively protect the Organization brand and IP.

IBM Security Intelligence

Combat Advanced Threats With Pre&Post Exploit Intelligence

What are the external and internal threats?	Are we configured to protect against these threats?	What is happening right now?	What was the impact?



Risk Management. Vulnerability Management.
Configuration and Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Leak Prevention.
SIEM. Log Management. Incident Response.

QRadar is the anchor tenant, collecting and analyzing all telemetry and delivering information in context.

IBM Security Intelligence

Post Exploit Intelligence & Action

Context + Correlation = Deepest Insight

Prioritized Offenses

	Id	Description	Attacker/Src	Magnitude	Target (s)/Dest
	287	Local SSH Scanner Detected , Suspicious - Internal - Rejected...	10.100.50.81		Multiple (508)
	318	Remote FTP Scanner Detected , Excessive Firewall Denies Acros...	217.64.100.162		Local (99)
	274	DoS - External - Potential Unresponsive Service or Distribute...	Multiple (49)		WebApp-Serv
	308	Multiple Exploit/Malware Types Targeting a Single Source , Ex...	10.100.50.56		Local (8)
	309	Multiple Exploit/Malware Types Targeting a Single Source	10.100.50.85		Multiple (2)
		Remote FTP Scanner Detected , Excessive Firewall	81.240.89.210		Remote (226)
		...unication with BOT	10.100.100.208		Remote (2)

- Security Devices
- Network Devices
- Servers & Hosts
- Virtual Machines
- Applications
- Config Info
- Vulnerability Info

Event Correlation

- Logs
- Flows
- IP Location
- Geo Location

Anomaly Detection

Activity Baselining & Anomaly Detection

- User Activity
- Application Activity
- Network Activity

Offense Identification

- Credibility
- Severity
- Relevance

Offense

SUSPECTED INCIDENTS

Most Sources + Most Intelligence = Most Accurate & Actionable Insight

IBM Security Intelligence

Offenses are Real-Time

- Security Devices
- Network Devices
- Servers & Hosts
- Virtual Machines
- Applications
- Config Info
- Vulnerability Info

Event Correlation

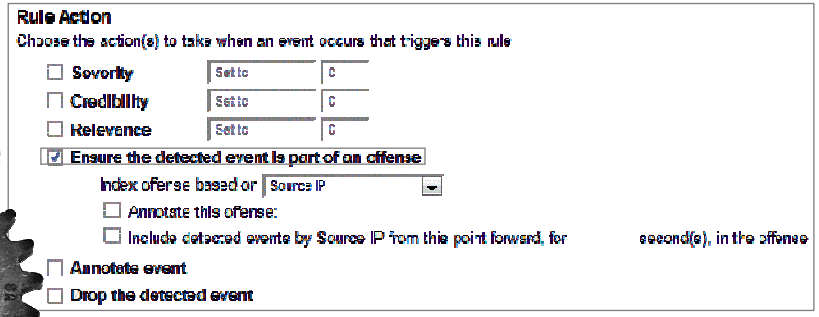
- Logs
- Flows
- IP Location
- Geo Location

Anomaly Detection

Activity Baselining & Anomaly Detection

- User Activity
- Application Activity
- Network Activity

Rules Engine



Offenses

ID	Description	Attacker(s)/Src	Magnitude	Target(s)/Dest
001	Remote FTP Scanner detected, Excessive Firewall Denies	217.64.100.162	8	Multiple (99)
002	Excessive Login Faliures, Login Success	81.240.89.210	9	10.100.50.81

The Key to Data Management:

System Summary

Flows (Past 24 Hours)	1.3M
New Events (Past 24 Hours)	677M
Updated Offenses (Past 24 Hours)	588
Data Reduction Ratio	10633 : 1

Most Recent Offenses

Offense Name	Magnitude
Local Web Scanner Detected containing Web.Image.GIF	
Potential P2P Traffic or VoIP Detected preceded by Local TCP Scanner Detected containing unknown	
Local Web Scanner Detected containing Web.Image.JPEG	
MS SMB2 Validate Provider Callback RCE	
Local Web Scanner Detected containing Web.HTTPWeb	

Reduction and Prioritization

IBM Security Intelligence

Actionable Information Not Just Alerts

Who is attacking?
What is being attacked?
What is the business impact?
Where do I investigate?

EXAMPLE OF AN OFFENSE

Summary | Targets | Categories | Annotations

Magnitude		Relevance	
Description	Exploit/Malware Events Across Multiple Targets preceded by Worm Events Detected containing HTTP: Nimda Worm - IIS Extended Unicode Directory Traversal Attack	Event count	549 events in 3 categories
Attacker/Src	10.100.50.30	Start	2007-02-17 23:44:06
Target(s)/Dest	10.100.50.21 Remote (47)	Duration	4m 38s
Network(s)	Multiple (2)	Assigned to	Not assigned
Notes			

Asset Profile

Security Incident

Supporting Events

Attacker Summary Details

Magnitude		User	dave.bolton
Description	10.100.50.30	MAC	
Vulnerabilities	0	Asset Weight	0
Location	Net-10-172-192.Net_10_0_0_0		

Top 5 Categories Categories

Name	Magnitude	Local Target Count	Events	Last Event
Worm Active		0	540	02-17 23:46:23
Misc Exploit		0	8	02-17 23:46:23
Firewall Session Closed		1	1	02-17 23:49:23

Top 5 Local Targets Targets

IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
10.100.50.21		Unknown	No	Unknown	Unknown	Net_10_0_0_0	0

Top 10 Events Events

Event Name	Magnitude	Device	Category	Destination	Start Time
Worm Active - Event CRE		eventprocessor0 :: demo	Worm Active	211.171.202.78:80	02-17 23:44:17
Worm Active - Event CRE		eventprocessor0 :: demo	Worm Active	211.171.202.78:80	02-17 23:44:27
Worm Active - Event CRE		eventprocessor0 :: demo	Worm Active	211.234.202.78:80	02-17 23:44:38
Worm Active - Event CRE		eventprocessor0 :: demo	Active	211.171.202.78:80	02-17 23:44:25
Worm Active - Event CRE		eventprocessor0 :: demo	Active	211.171.202.78:80	02-17 23:44:08
Worm Active - Event CRE		eventprocessor0 :: demo	Active	211.171.202.78:80	02-17 23:44:42
Worm Active - Event CRE		eventprocessor0 :: demo	Active	211.171.202.78:80	02-17 23:44:12
Worm Active - Event CRE		eventprocessor0 :: demo	Worm Active	211.171.202.78:80	02-17 23:44:54
Worm Active - Event CRE		eventprocessor0 :: demo	Worm Active	211.171.202.78:80	02-17 23:44:10
Worm Active - Event CRE		eventprocessor0 :: demo	Worm Active	211.171.202.78:80	02-17 23:44:45

Attacker Profile

Active Threats

Offense Targets

Top 5 Annotations Annotations

Annotation	Time	Weight
[8] "Target/Event Analysis". The number of events this attacker generated during this attack, was deemed worth a value of 8 on a scale of 0-10, with higher values indicating high volumes of events generated, and lower numbers indicating a smaller grade attack.	02-17 23:50:07	6
"CRE Event". CRE Rule description: Detected source IP address generating multiple (at least 5) exploits or malicious software (malware) events in the last 5 minutes. These events are not targeting hosts that are vulnerable and may indicate false positives generating from a device.	02-17 23:47:07	6
"CRE Event". CRE Rule description: Detected exploits or worm activity on a system for local-to-local or local-to-remote traffic.	02-17 23:45:07	6
[0] This attacker attempted to attack more hosts on the network then are known to exist. Approximatly 0% of the targets attacked, are thought to exist. The		

IBM Security Intelligence

Pre Exploit Intelligence & Action

Risk Management

QRadar Risk Manager

- Predictive threat modeling & simulation
- Scalable configuration monitoring and audit
- Advanced threat visualization and impact analysis

QRadar Risk Manager

While a SIEM is integral to a security safety net, it provides most of its value post-exploit.

QRadar Risk Manager provides detailed assessments of the network security risk using indicators such as :

What has happened?	From network activity data and behavior analytics
What can happen?	From configuration and topology
What has been attempted?	From events
What is vulnerable?	From VA scanners

QRadar Risk Manager provides an automated pre-exploit risk intelligence through the deliver of:

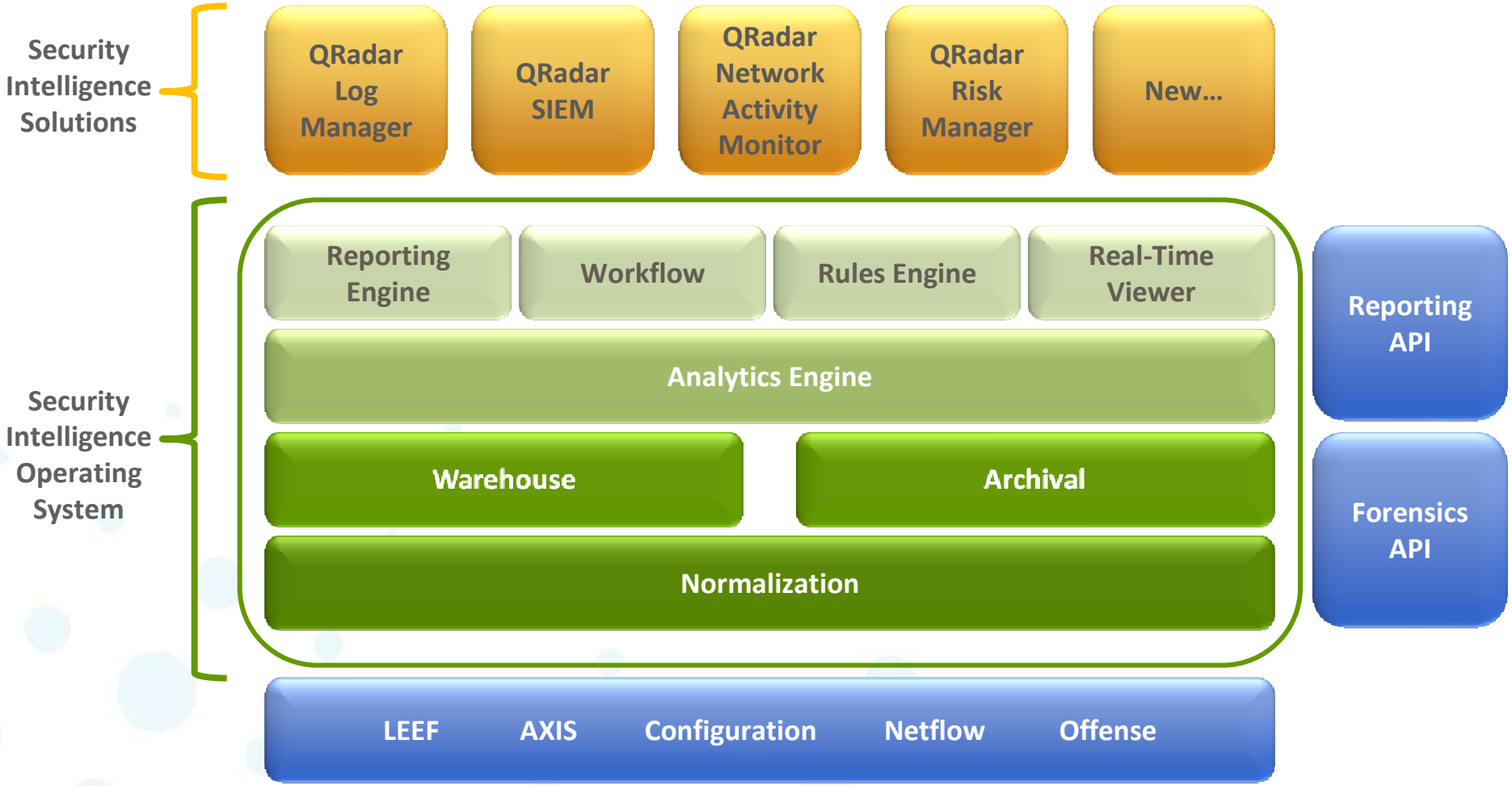
Intelligence – advanced risk policy monitoring and assessment, highly intelligent network and security visualizations

Integration – unparalleled risk analysis integrating configuration, network activity, events, and VA data

Automated-Unique and differentiated risk and compliance policy assessment

IBM Security Intelligence

QRadar Product Family



Built On a Common Foundation of QRadar SIOS

Intelligent + Integrated + Automated + One Console Security

IBM Security Intelligence

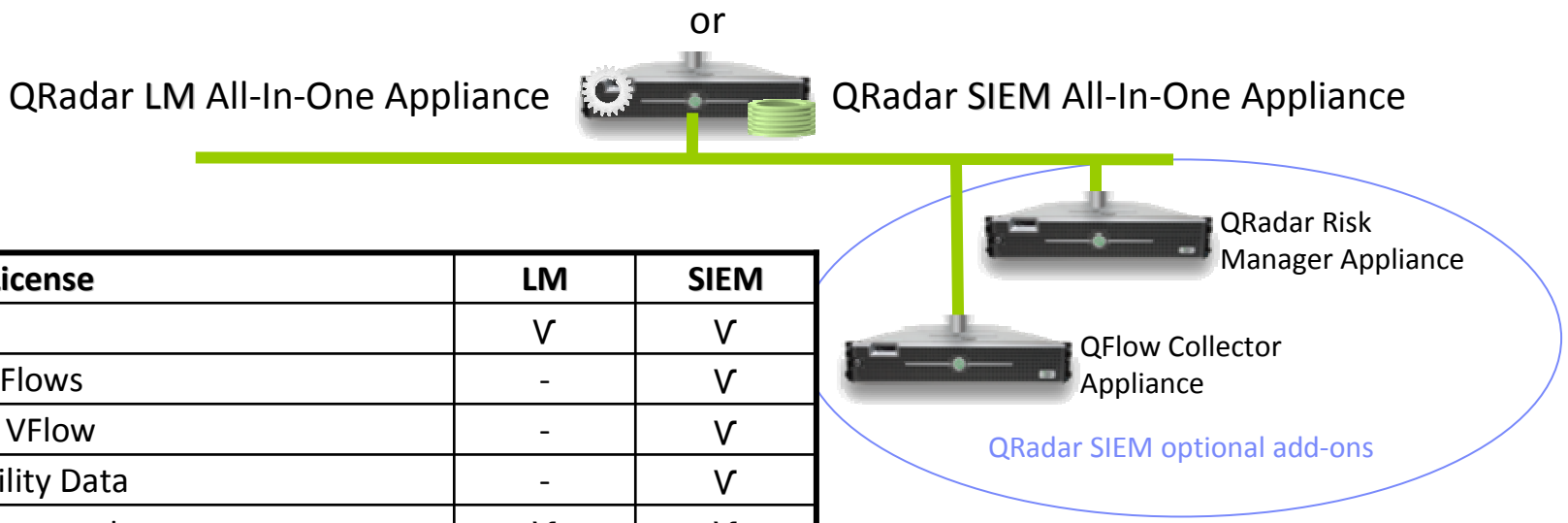
Deploy & Expand QRadar at Your Pace

- Log Management
- SIM/SEM
- Risk Management
- Scale
- Visibility/ Network Activity

One Security Console

IBM Security Intelligence

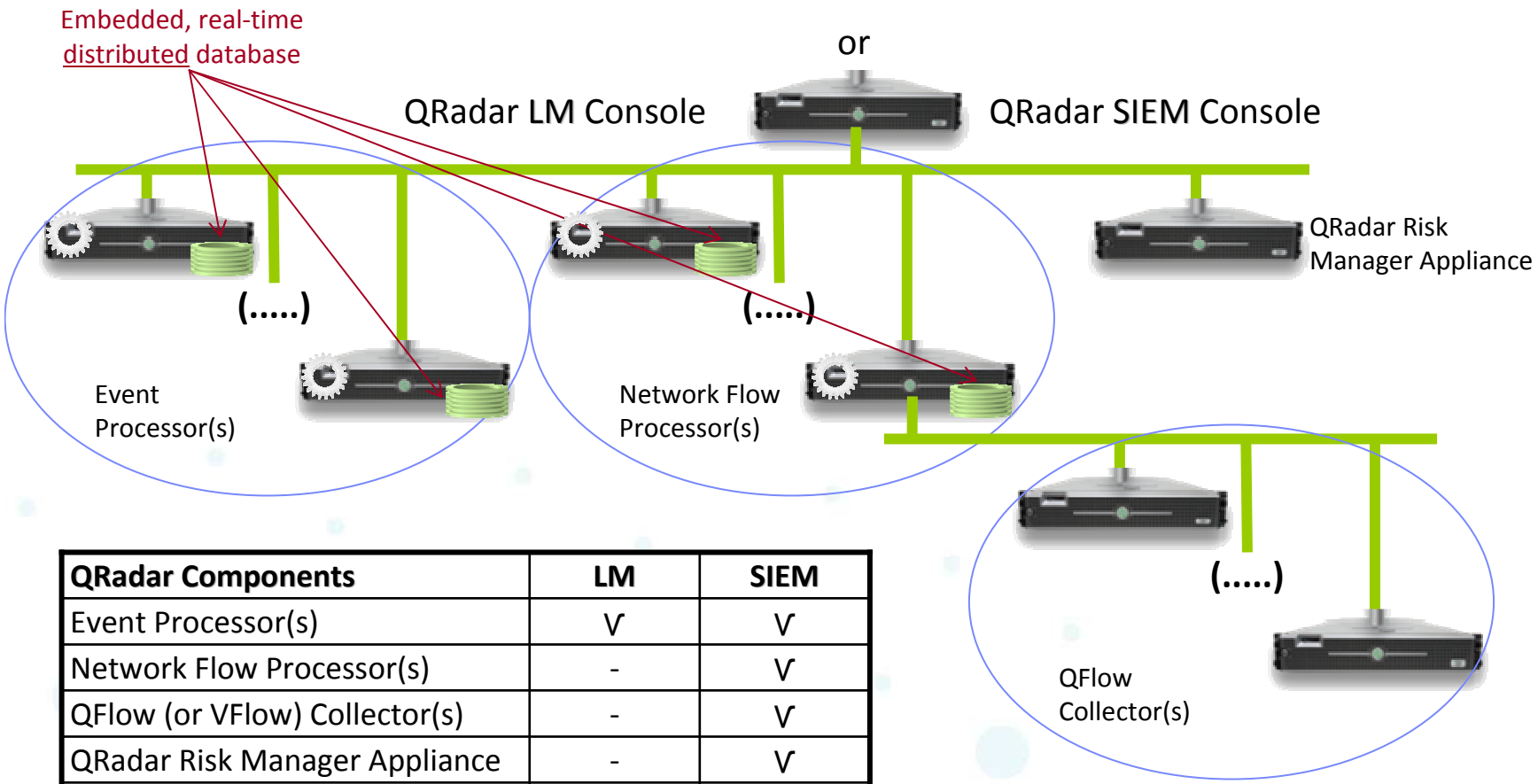
QRadar LM/SIEM Architecture – All-In-One



QRadar License	LM	SIEM
Events	√	√
Network Flows	-	√
QFlow or VFlow	-	√
Vulnerability Data	-	√
Log Management	√	√
Correlation Engine	√	√
Offenses	-	√
Risk Manager Option	-	√
Upgradable to SIEM	√	N/A
Migration to Distributed Architecture	√	√
Max EPS	5,000	5,000
Max FPI	N/A	200,000

IBM Security Intelligence

QRadar LM/SIEM Architecture – Distributed Architecture



QRadar Components	LM	SIEM
Event Processor(s)	√	√
Network Flow Processor(s)	-	√
QFlow (or VFlow) Collector(s)	-	√
QRadar Risk Manager Appliance	-	√
Max EPS	Unlimited*	Unlimited*
Max FPI	N/A	Unlimited*

* Unlimited as long as enough processors are deployed to support the required volume of events/flows.

IBM Security Intelligence

Key Differentiators

- Is much less complex and labor-intensive to manage
  - enabling faster time-to value and lower TCO
- Delivers out-of-the-box value
  - thousands of correlation rules, dashboard views and report templates
- Provides Layer 7 flow analytics for anomaly and threat detection and forensics
- Is highly scalable;
  - handle high event volumes
- Provides native [HA] High Availability.
- Provides comprehensive SIEM and log management
- Uses a single data architecture
  - unified correlation or analysis
- Offers a single user interface.
- Offers strong user identity analysis;

The Challenges Organizations Are Facing

So How We Can Help?

A single integrated solution able to address the following two areas:

From:

1- Compliance

- Lower the costs of managing audits and maintaining compliance with the full set of applicable regulations and policies.
- Minimize the possibility of regulatory non-compliance.

QRadar LM

2- Security

- Detect potential advanced threats and attacks in real-time via advanced analytics.
- Consolidate silos of network & security information to gain a single view across the enterprise.

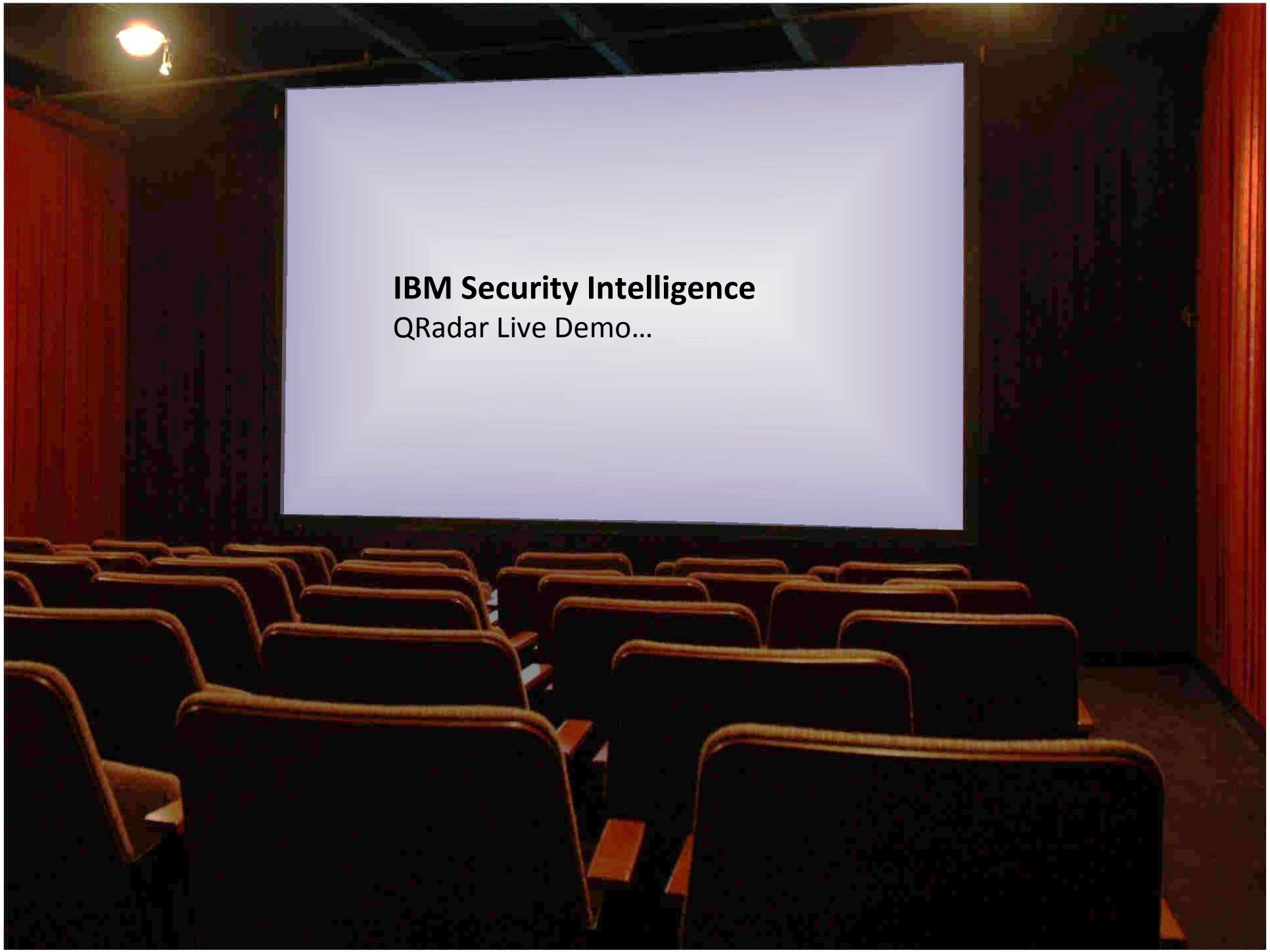
QRadar SIEM

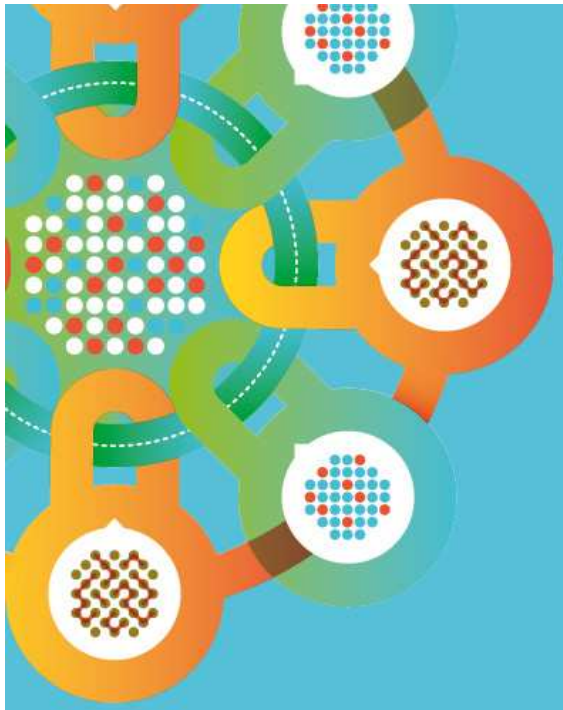
- Answer the "What if" questions ahead of time to further minimize the risks.

QRadar Risk Manager

To:

IBM Security Intelligence


IBM Security Intelligence
QRadar Live Demo…



IBM Forum Segrate - Milano

18 settembre:
Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

IBM Security Intelligence

- Technical Dive into QRadar

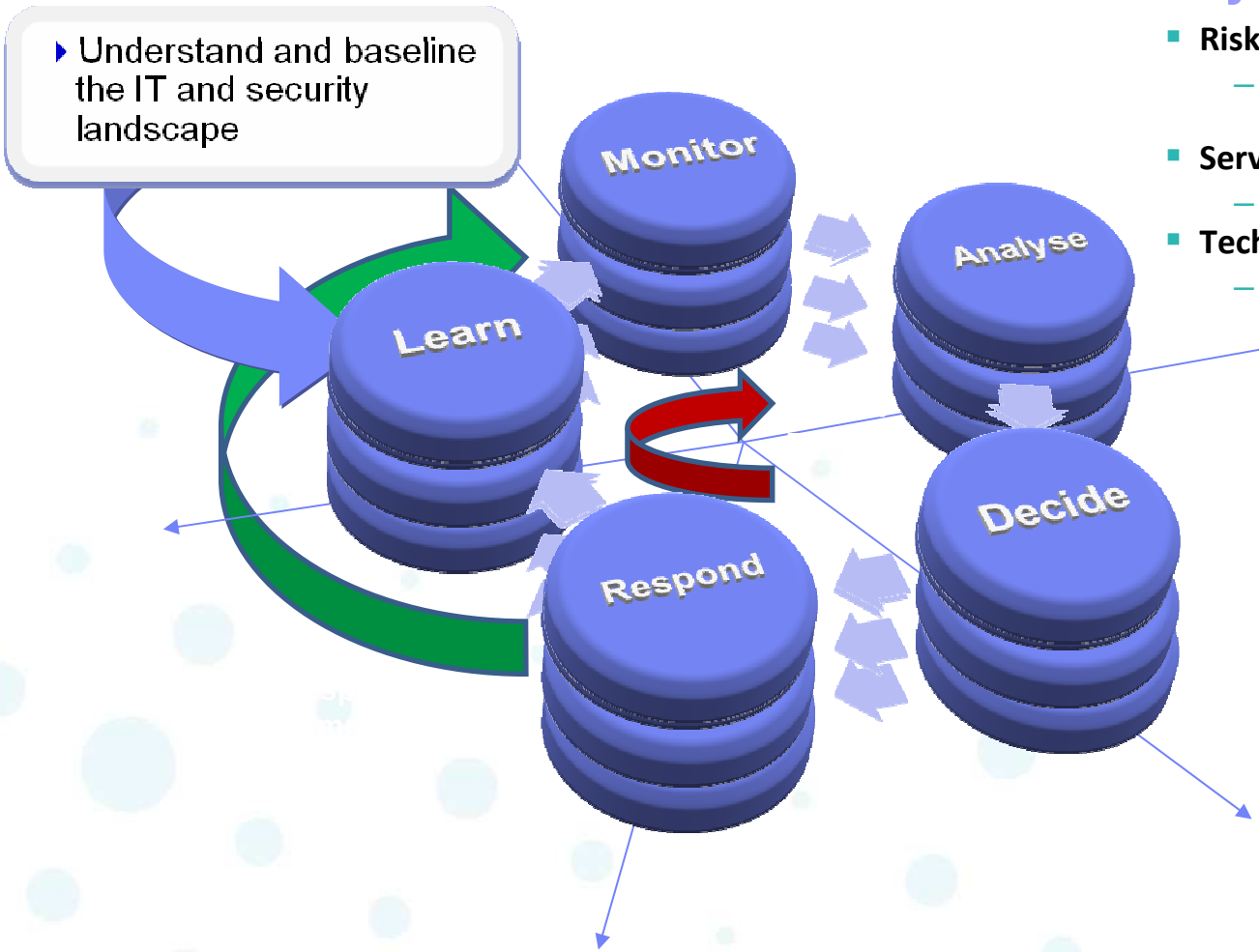
Jean-Luc Labbe

- Disegno di una Soluzione SIEM

Giovanni Abbadessa

L'utilizzo dell' IBM Cyber Security Lifecycle

Per scoprire e rispondere velocemente agli attacchi



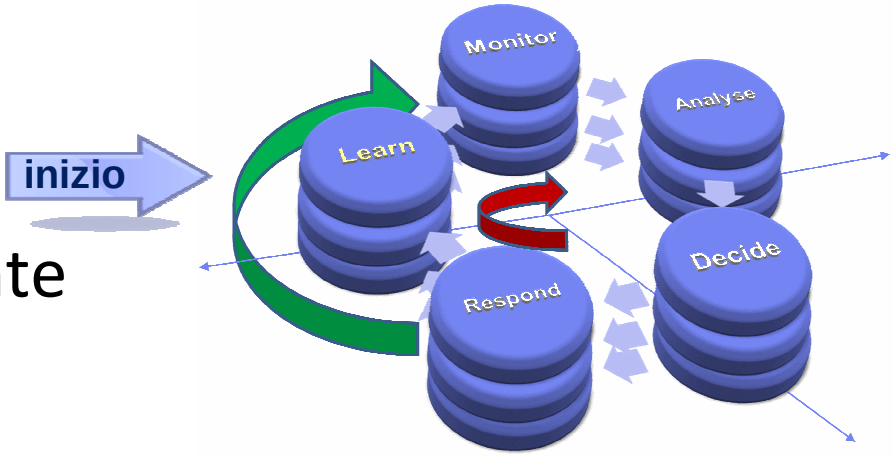
Layers

- **Risk**
  - Bilanciamento delle minacce delle risposte
- **Service management**
  - Processi
- **Technology**
  - Sicurezza, network, systems

L'utilizzo dell' IBM Cyber Security Lifecycle

Per scoprire e rispondere velocemente agli attacchi

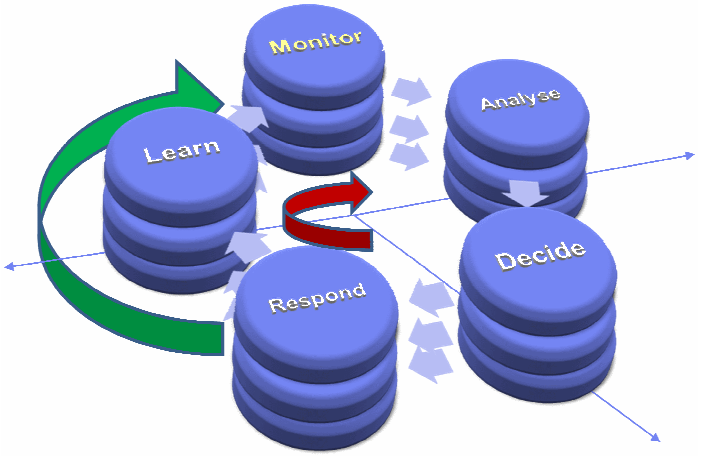
Learn:
Comprensione dell' ambiente



- Stabilire un regime di Governance, Risk and Compliance che bilanci le contromisure da approntare e con i rischi che sono stati determinati
- Identificazione, classificazione e catalogazione degli asset e servizi
- Educare a comportamenti sicuri i dipendenti, supportando processi lavorativi adeguati
- Conoscere la topologia del network, dei sistemi e delle applicazioni
  - Comprendere le reali capacità del mio service management
- Determinare le vulnerabilità del network, dei sistemi e delle applicazioni

L'utilizzo dell' IBM Cyber Security Lifecycle

Per scoprire e rispondere velocemente agli attacchi



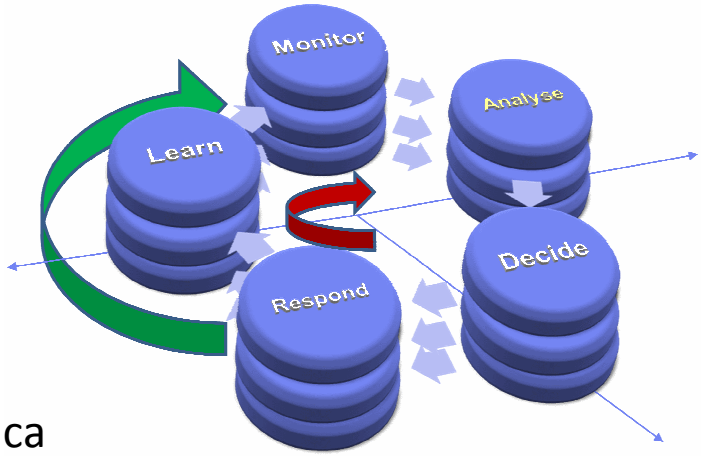
Monitor:
Comprendere cosa accade sulla rete e sull'infrastruttura IT in tempo reale

- Dipende da un una efficiente infrastruttura di protezione della rete
- Catturare gli eventi dai dispositivi di rete e altre infrastrutture IT
- Eseguire scansioni della rete (conoscenza della topologia e dei rischi associati alle vulnerabilità)
- Correlare un elevato numero di eventi per possedere la consapevolezza di quello che accade
- Individuare in tempo reale instrusioni, manipolazione di programmi o informazioni e attività sospette che deviano dal normale comportamento

L'utilizzo dell' IBM Cyber Security Lifecycle

Per scoprire e rispondere velocemente agli attacchi

Analyse:
Effettuare analisi avanzate in tempo reale

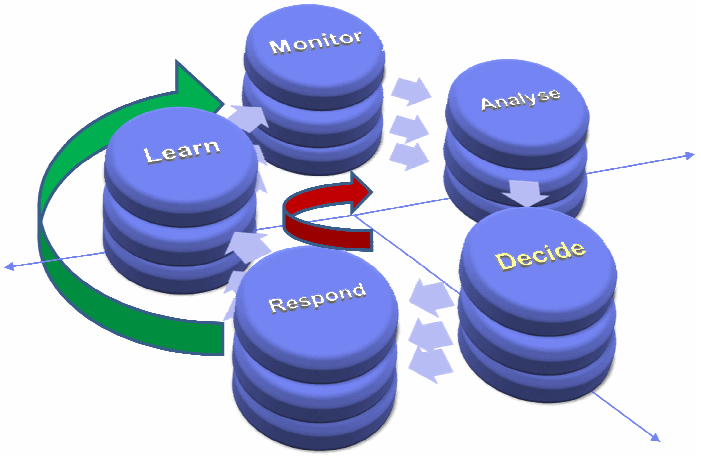


- La velocità di risposta è diventata sempre più critica
- IBM ha imparato che per lottare contro le minacce informatiche è necessario ricorrere all'ispezione e l'analisi continua di un enorme numero di dati che fluiscono attraverso la rete da sensori, sistemi di monitoraggio e altri dispositivi.
- L'analisi analitica fornisce indicazioni accurate sugli attacchi e sui sistemi compromessi
  - Ispezione di tutto il traffico di rete con vari algoritmi analitici per scoprire eventuali comportamenti anomali
  - Difesa (e reazione) veloce
- Riduzione del "rumore di fondo"
- Visualizzazione migliorata delle minacce e degli attacchi
- Analisi forense di un numero elevato di insiemi di dati complessi

L'utilizzo dell' IBM Cyber Security Lifecycle

Per scoprire e rispondere velocemente agli attacchi

Decide:
Determinare le caratteristiche dell'attacco per capire come rispondere al meglio

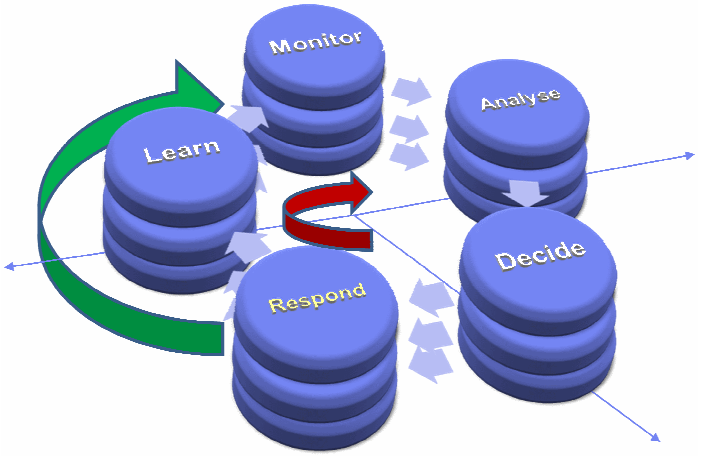


- Utilizzo delle informazioni di contesto per migliorare le decisioni
- Implementazione di un modello decisionale basato sui rischi
- Quando si è sotto attacco bisogna avere delle procedure ben definite che aiutino il personale del SOC nella risposta
- Definire processi di service management efficaci basati sulle decisioni
- L'optimum sarà legare funzioni avanzate di analisi a processi che facciano uso di strumenti automatici di riconfigurazione dell'infrastruttura IT

L'utilizzo dell' IBM Cyber Security Lifecycle

Per scoprire e rispondere velocemente agli attacchi

Respond:
Contenimento e risoluzione

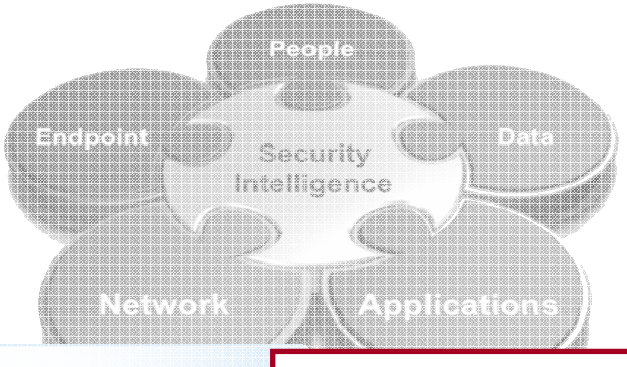


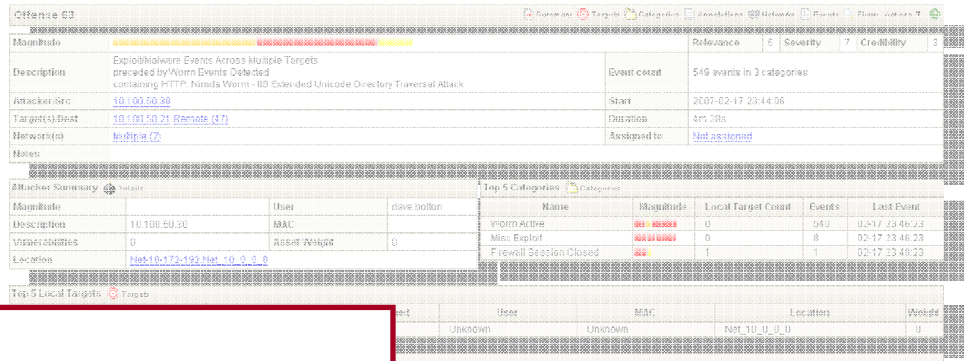
- Automatizzare i processi per adattarsi e rispondere agli attacchi dinamicamente
- Capacità di riconfigurazione automatica della rete per il contenimento degli attacchi
  - Mettere in quarantena un network; Detach virtual machines; rimozione delle workstation dalla rete
  - Abilitare re-configuration e re-provisioning automatici
- Problema !! Le risposte automatiche richiedono analisi degli alert che siano il più accurate possibili
- Imparare e sviluppare nuovi patter e capacità predittive dall'analisi avanzata.

Imparare dagli attacchi

L'utilizzo dell' IBM Cyber Security Lifecycle

L'analisi dei dati è il cuore Cyber Security Lifecycle





Security Devices

Network Devices

Servers & Hosts

Virtual Machines

Applications

Config Info

Vulnerability Info

La chiave è:

- Ridurre i miliardi di eventi a pochi probabili incidenti da analizzare
- Avere processi di analisi e gestione incidenti "robusti"

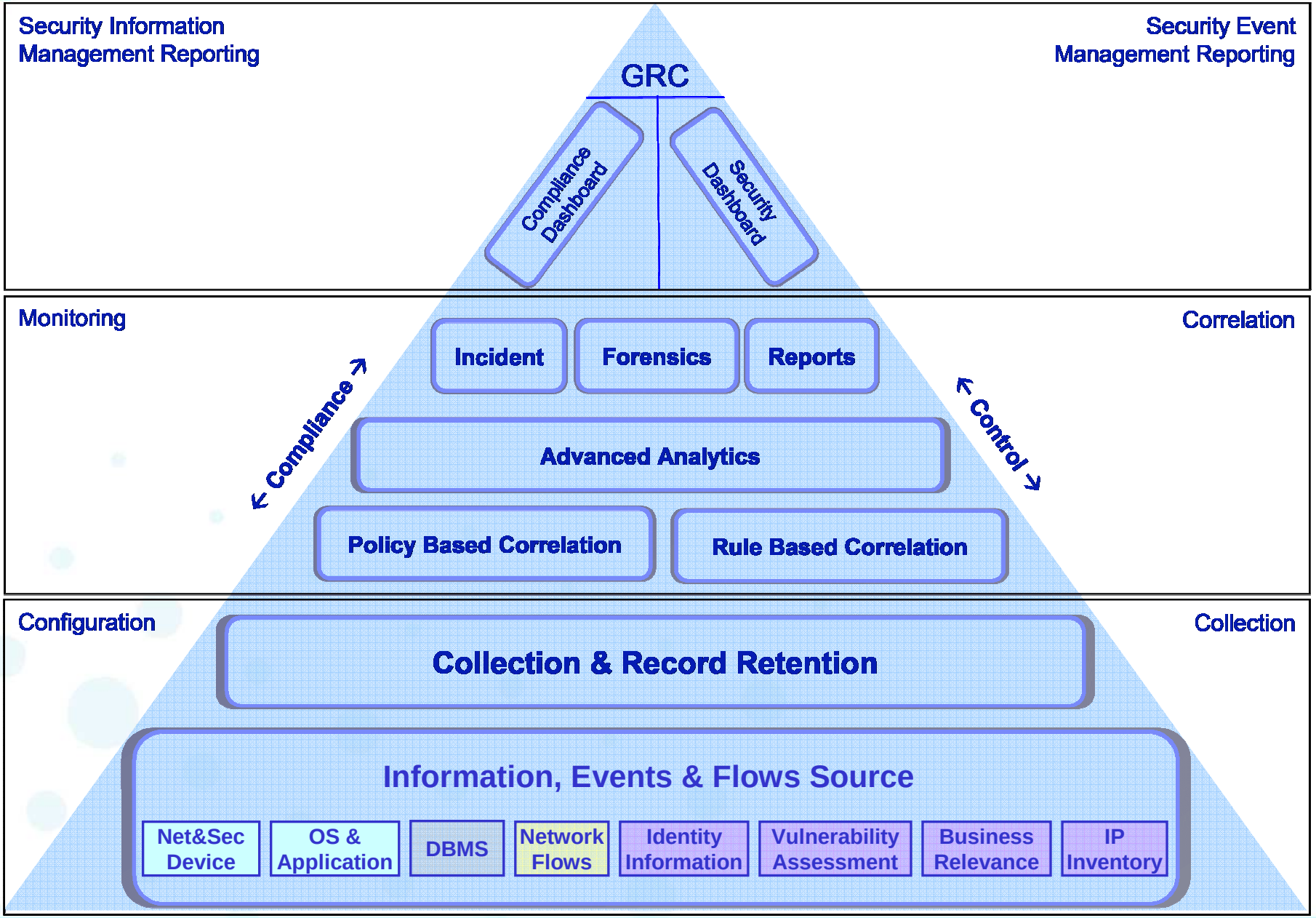
- User Activity
- Application Activity
- Network Activity

Offense

SUSPECTED INCIDENTS

Most Sources + Most Intelligence = Most Accurate & Actionable Insight

Il modello per l'analisi degli eventi di sicurezza secondo IBM



Disegno di una Soluzione SIEM

Obiettivo e Descrizione del Progetto

- Obiettivo
  - Sostituire l'attuale soluzione di auditing custom basata su SAS su Mainframe con una basata su prodotti di L&M di mercato
- Motivazioni
  - L'attuale soluzione:
    - è costosa;
    - non è facilmente modificabile (necessita di skill elevati)
    - consuma MIPS preziosi
    - non mantiene on line più di due settimane di dati
    - non è in grado di gestire il real-time
- Soluzione
  - Utilizzo di Qradar, per costruire una piattaforma di audting in grado di produrre le stesse tipologie di report e permettere future evoluzioni che riducano l'effort di auditing grazie alle funzionalità di analisi intelligente
- Prerequisito
  - Realizzare un PoC che dimostri le capacità della soluzione di produrre i report

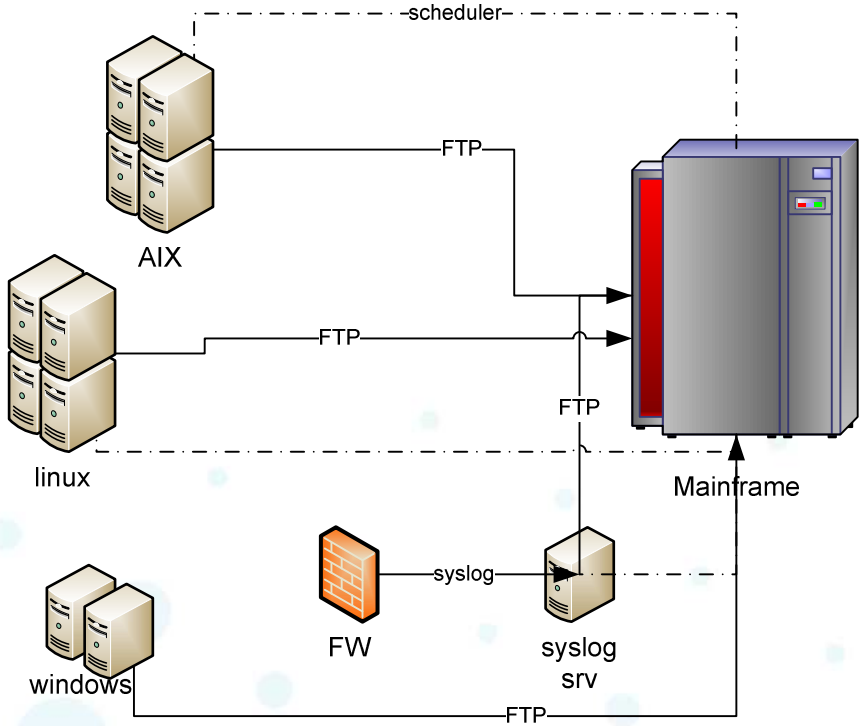
Disegno di una Soluzione SIEM

Soluzione attuale

- L'attuale soluzione permette solo la produzione di report statici a partire dai dati prodotti dagli audit trail dei vari sottosistemi
- I dati vengono trasferiti sul mainframe mediante protocollo FTP e le attività di trasferimento sono schedulate dal mainframe con delle finestre temporali di circa 12 ore
- E' stato necessario inserire dei controlli esterni per verificare eventuali problemi nella spedizione dei file
- I report devono essere esaminati visivamente
- E' possibile mantenere on line solo due settimane di dati

Disegno di una Soluzione SIEM

Infrastruttura attuale



Sul mainframe vengono raccolti gli audit trail dei sistemi:

- AIX
- Linux
- Firewall
- MS Windows
- DB2 (Mainframe)
- zOS
- RACF

Vengono poi prodotti i report di audit dal SAS su mainframe

I report vengono analizzati dagli operatori, per evidenziare eventuali anomalie e violazioni delle policy di sicurezza.

Gli operatori devono verificare anche eventuali problemi di trasmissione dell'infrastruttura FTP

Disegno di una Soluzione SIEM

La nuova soluzione basata su QRadar

- Nel PoC si è dimostrato la possibilità di catturare gli eventi di sicurezza di tutte le piattaforme in ambito e produrre un sottoinsieme dei report richiesti
  - Attività peculiari:
    - script per inviare l'audit trail AIX via syslog
    - configuare il Qradar per riconosce il contenuto semantico dei log di audit trail
    - partecipare al beta program IBM per integrare i messaggi di audit del mainframe

- La soluzione di produzione è basata su due appliance mod 1605 con funzioni di event processor in HA e di un appliance 3105 con funzioni di console.
- In produzione si dovranno integrare circa 100 sistemi linux/AIX, 10 windows, 4 partizioni zOS, 10 apparati di sicurezza che producono circa 50 GB/gg
- Il sistema dovrà essere in grado di scalare, con l'eventuale adozione di ulteriori event processor, fino al raddoppio del numero di sistemi e degli eventi di sicurezza da gestire
- In una fase successiva, la soluzione verrà utilizzata, per segnalare in tempo reale eventuali violazioni delle policy di sicurezza e individuare potenziali incidenti di sicurezza. Si passerà quindi dall'attuale sistema "statico" ad uno "reattivo"

Disegno di una Soluzione SIEM

Gli apparati utilizzati nel progetto

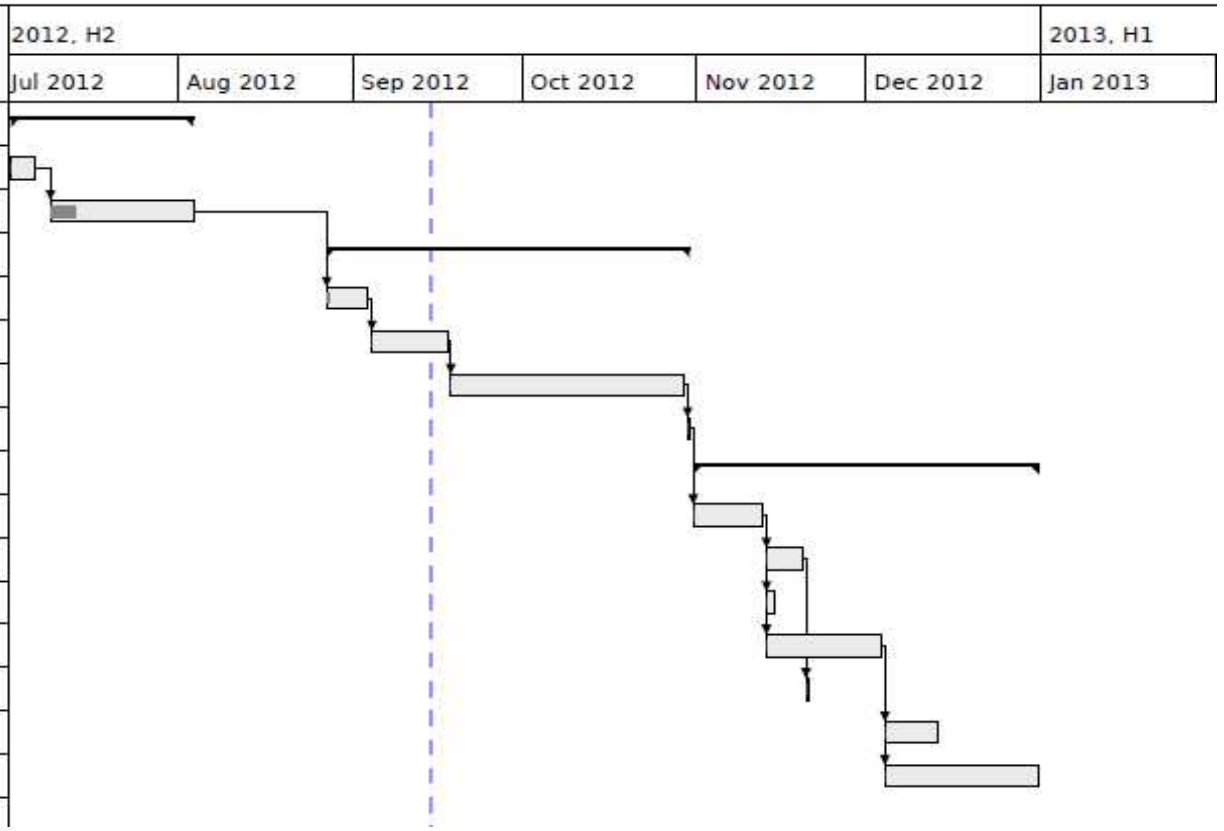
Console 3105	
Dimensioni	29.5" D x 19.2" W x 3.4" H (2RU)
CPU	2 x Intel Xeon Processor E5620 4C 2.40GHz
RAM	48 GB
Storage	9 TB (6,5 TB dedicati per i dati di Qradar
Network Interface	4 x 10/100/1000 Base-T
Power	Dual Redudant 675 W Power Supply

EP1605	
Dimensioni	29.5" D x 19.2" W x 3.4" H (2 RU)
CPU	2 x Intel Xeon Processor E5620 4C 2.40GHz
RAM	48 GB
Storage	9 TB (6,5 TB dedicati per i dati di Qradar
Network Interface	4 x 10/100/1000 Base-T
Power	Dual Redudant 675 W Power Supply
EPS Sustained	fino a 20.000
EPS Burst	fino a 75.000
Event Storage	fino a 90 giorni @ 10.000 EPS sustained

Disegno di una Soluzione SIEM

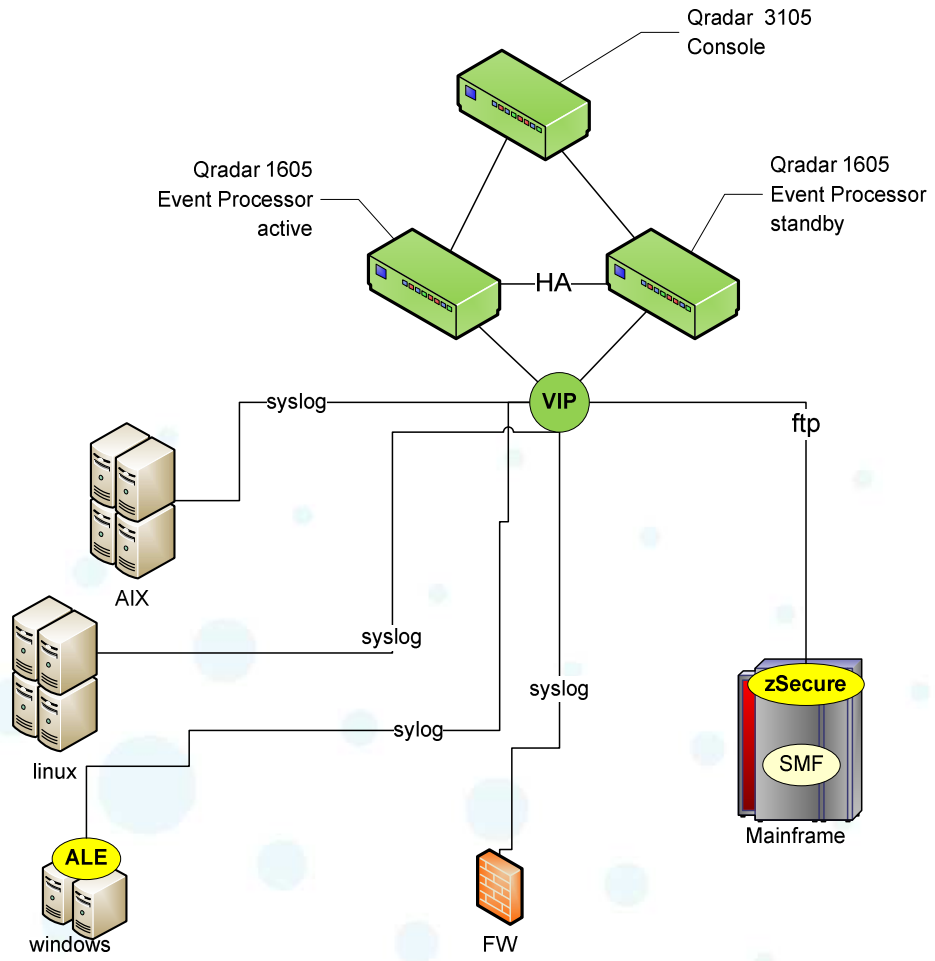
Il GANTT di progetto

Name	Work
PoC	**25d**
Disegno PoC	5d
Realizzazione PoC	20d
Pre Pilota	**47d**
Disegno Soluzione	6d
Implem. pre Pilota	10d
disegno report	30d
collaudo	1d
Produzione	**60d**
sorgenti AIX	9d
sorgenti linux	5d
sorgenti windows	2d
setup zSecure	15d
sorgenti FW	1d
regression test	8d
tuning e support prod	20d



Disegno di una Soluzione SIEM

Nuova infrastruttura di audit basata su QRadar



L'agent **ALE** trasforma gli eventi windows e li trasferisce con prot. syslog

Sul mainframe zSecure Audit è utilizzato per convertire SMF (ed altri) dati nel formato LEEF (Log Event Enhanced Format).

zSecure Audit arricchisce gli eventi con informazioni dal security database e dal system snapshot (CKFREEZE) information

L'aggiunta di eventuali eventi custom per il MF è supportata In maniera analoga a quanto avviene per il TSIEM.

Disegno di una Soluzione SIEM

Risultati del progetto

- PoC completato con successo
- Aumento del retention period live da due settimane a 230 gg
- Riduzione dei costi di esercizio
- Si stanno producendo tutti i report, circa 50, che il Cliente realizzava con il sistema precedente, per motivi di compliance interna
- Il Cliente, comprendendo le funzionalità avanzate di analisi possedute da Qradar, sta cominciando a ridisegnare la modalità di lavoro, finora basata sull'analisi manuale di tabelle di report.
- Completata la produzione dei report, si implementeranno delle query per produrre dei report molto più sintetici con informazioni immediatamente utilizzabili dagli analisti
- Si ritiene che a regime l'attuale impegno di un FTE dedicato interamente all'analisi dei report, possa essere ridotto della metà

Disegno di una Soluzione SIEM

Evoluzioni future identificate dal Cliente

- Raddoppio della capacità di analisi del sistema con la duplicazione delle sorgenti dati (non sarà necessario acquistare altro HW, ma basterà un semplice upgrade di licenza per passare dagli attuali 5.000 EPS a 10.000 EPS)
- Implementazione della funzione di D/R
- Utilizzo delle offense per analizzare in tempo reale eventuli incidenti di sicurezza
- Arricchimento delle informazini di contesto mediante l'integrazione di:
  - informazioni proveniente dal sistema di Vulnerability Analisys
  - QFlow e Network Flow per potere attivare le funzioni di **Network Behavior Analysis**

IBM Forum Segrate - Milano

18 settembre: Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

IBM Security Systems

Grazie

Organizations taking a Smarter Approach to Security