UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 4

Always A Pioneer, Always Ahead

Enterprise Security Management (ESM)

Dr. Zaheera Zainal Abidin

zaheera@utem.edu.my

MyUTeM

By the end of the lesson, the student will be able to:

a. understand the concept of enterprise security management (ESM)
b. understand the ESM Architecture and Component
c. Understand the ESM services and deployment

CONTENT

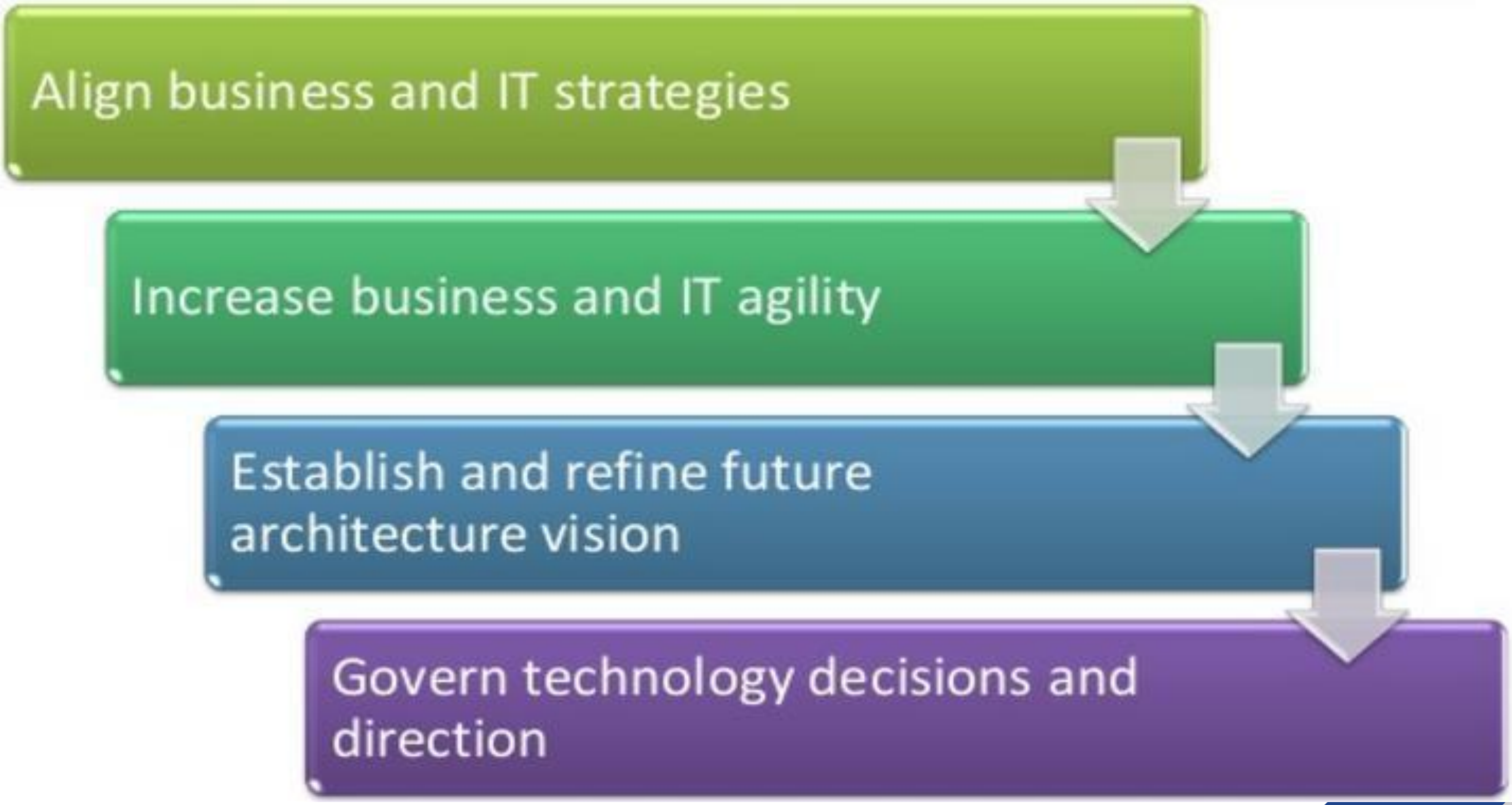
- Introduction to ESM
- ESM Architecture
- More about the enterprise security management (ESM)
- ESM is a center of physical and logical security
- ESM Services
- ESM deployment strategy
- The convergence of network operations and security operations in ESM implementation

INTRODUCTION TO ESM

ENTERPRISE SECURITY MANAGEMENT

- Enterprise networks expand nationally and globally to include Internet access, cloud services, intranets, extranets and e-commerce activities. Therefore, computer networks are vulnerable to threats from both inside and outside the organization. To protect the enterprise networks, the higher level of security management need to determine the policy and initiate the security policy enforcement.
- Enterprise Security Management (ESM) is the process of controlling configuration, deployment, and monitoring of **security policy** across multiple platforms and security point products.
- Thus, enterprise security management is a holistic approach to integrate guidelines, policies and proactive measures for various threats of detection.

OBJECTIVE OF ESM



Align business and IT strategies

Increase business and IT agility

Establish and refine future architecture vision

Govern technology decisions and direction

THE IMPORTANCE OF ESM

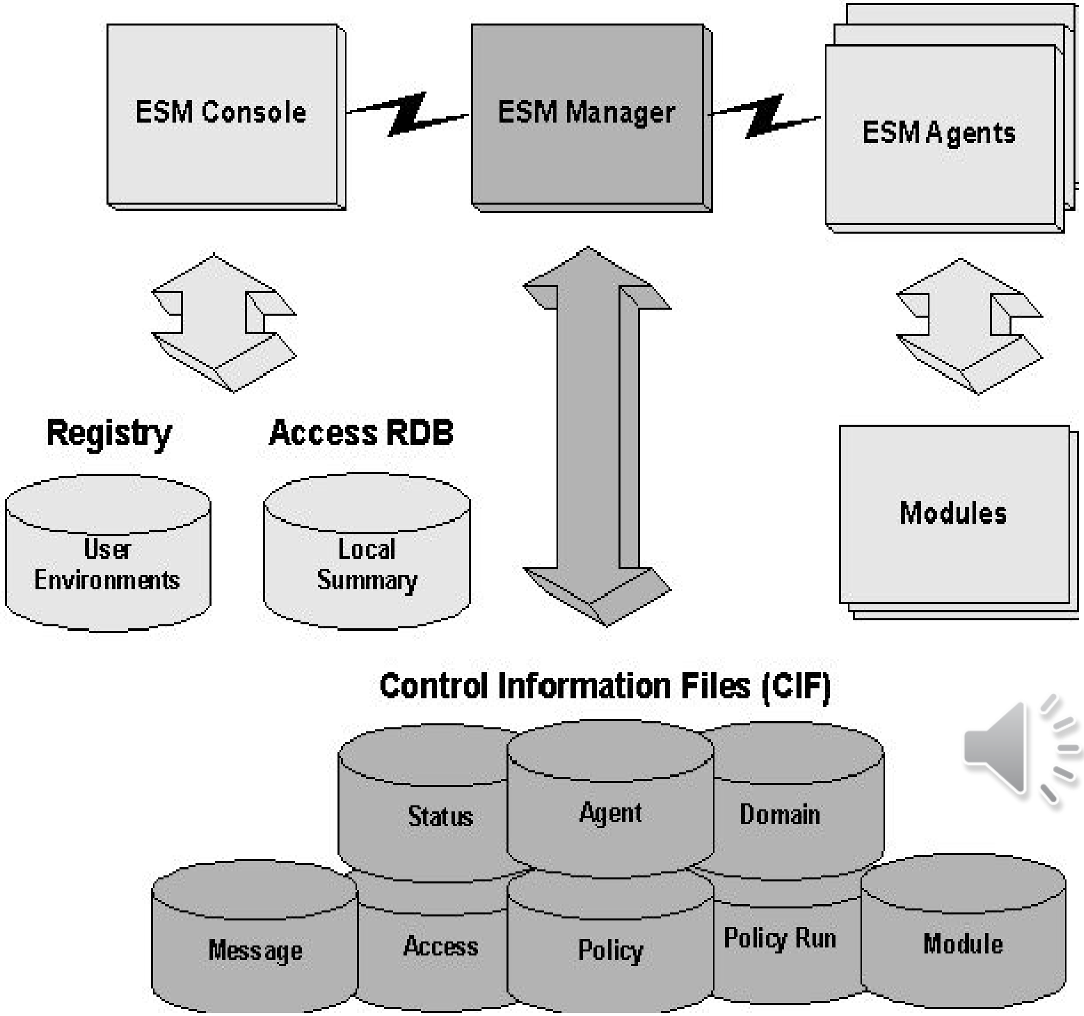
- Growing and evolving cyber security threats
  - Cyber terrorism, cyber crime, cyber vandalism, cyber espionage, cyber war
- Evolution to support and enable for the next generation of existing enterprise system
  - Increased levels of network connectivity (from point to point to net centricity
  - Newer technologies (satellite based surveillance and navigation)
  - Increased complexity from interoperability needs (legacy systems and new implementation)
- Security is based around individual systems
  - Non uniform security, the weakest link paradigm applies
  - Costly to implement
  - Individual system security never intended to mitigate the advanced threats

ESM ARCHITECTURE

ESM ARCHITECTURE

The ESM architecture consists of :

- Open e-Security **Platform – hundreds on proprietary and open source tools.**
- An **agent** that need to be configured and monitored the security policy on managed assets. Managed assets means firewalls, IDS or VPN.
- **Server** or Manager is configured to manage and monitor the agent. Example of Server is the application server, database server, web server and legacy system (such as mainframes).
- **Console** is a web interface that enables and manage security events, monitor endpoint health and, configure policy rules from web browser. The installation of the ESM console either on cloud-based, separate ESM server or on the ESM server itself. Example dashboard monitoring system.



ESM MANAGER AND ESM DATABASE

- ESM Manager acts as a brain of the architecture
  - It is a central location for everything, from correlation and analysis, through case management and alerting process.
- Leverage the ESM Database
  - An enterprise level database such as Oracle for forensic analysis.

- All logs that entering the ESM system are processed in memory and in real time. However, for forensic analysis process, historical analysis and reporting phase, previous logs are desired. Thus, ESM system retrieves logs from databases.

ESM CONSOLE AND ESM WEB

- ESM allows several forms of interaction – Console and Website.
- ESM Console is a software loaded, more features that allow administrative tasks (creating original content rules, reports and dashboards, and defining user access privileges).
- ESM Web requires a Web browser to connect ESM Manager, using HTTPS.
- Both solutions (ESM Console and ESM Web) provide granular access controls for users (LDAP, PKI, TACACS, RADIUS). It is easy to add and remove privileges across various disciplines.

MORE ABOUT THE ESM

MORE ABOUT ESM

- ESM is a combination method from guideline, standard, planning and preventive measures in combating various types of threat in organization. The alert and notification for communication in ESM using the log or syslog.
- Logs come from multiple number of sources, including:

  1. Traditional security products - firewalls, intrusion detection & prevention systems, VPN, antivirus software, identify management systems.
  2. Network devices routers, switches, wireless access point.
  3. Mainframe, server and workstation information OS & application.
  4. Physical security solutions - badge readers, video camera, HVAC system
  5. Others Scanners, policy managers, asset managers, mobile devices, telephony system.
- Beyond Log Collection
  - Once ESM collected the logs, it uses real time, automate technique (correlation, anomaly detection, pattern discovery & visualization) to reduce false positive.

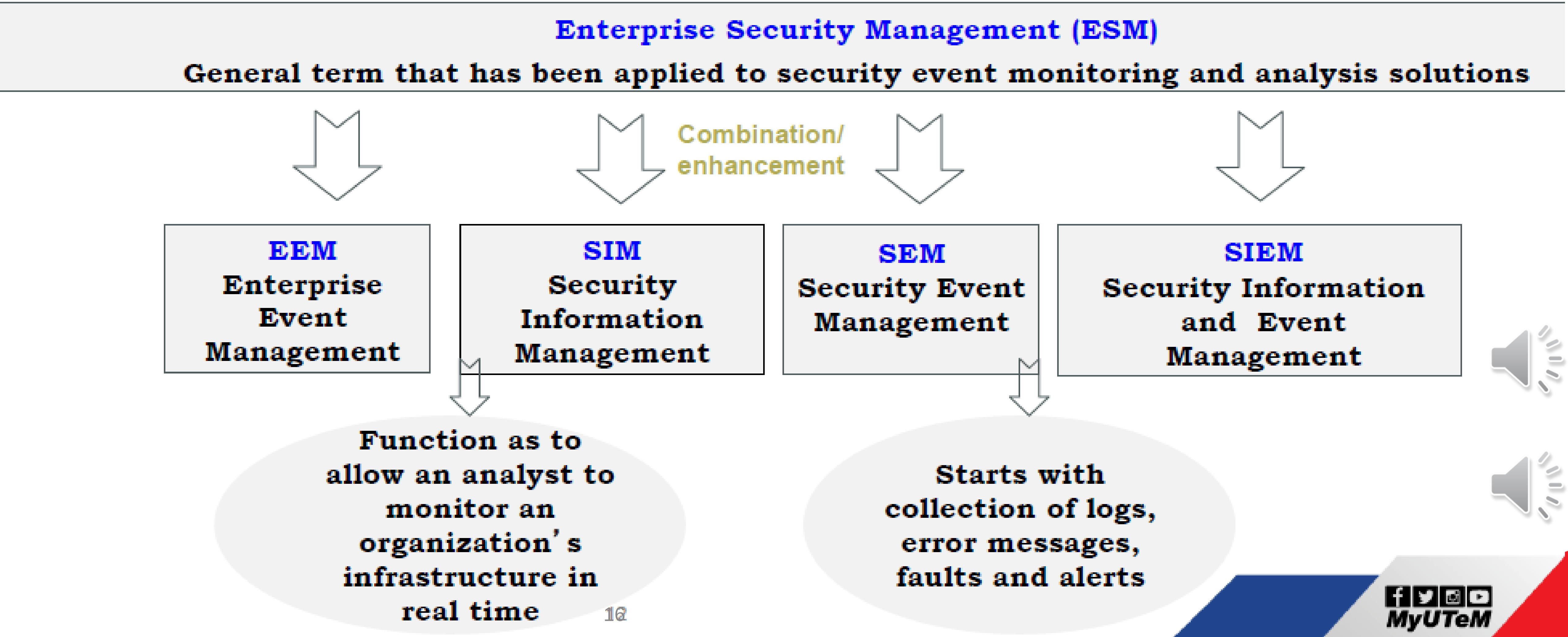
THE PURPOSE OF ESM

- **Facilitates** a framework for **security analysts** to apply human intuition to issues through interactive charts, visual tools and investigation techniques.
- Offer a number of **forensics analysis** and **incident management**. It supports advanced discovery techniques, reporting and analysis applied against data.
- Offer case management and integration with third party.
- Provides **alerting** and escalation feature, which configure organizational processes such as management procedures.

THE PURPOSE OF ESM

- Capability to actually modify devices settings with or without human intervention in order to stop an attack or threat in the cyber world.
- Disabling user accounts who is unknown and anonymous to the organization.
- Filtering the Internet Protocol (IP) address on firewall, layer 3 switches and routers.
- Terminating sessions on VPNs, wireless access points, and intrusion detection systems.
- Quarantining devices to separate and control VLANs.
- Stopping access at layer 2 by applying MAC address filters or disabling a physical port on a switch.

THE COMPONENT OF ESM



Enterprise Security Management (ESM)

General term that has been applied to security event monitoring and analysis solutions

Combination/ enhancement

EEM
Enterprise Event Management

SIM
Security Information Management

SEM
Security Event Management

SIEM
Security Information and Event Management

Function as to allow an analyst to monitor an organization's infrastructure in real time

Starts with collection of logs, error messages, faults and alerts

EEM - Enterprise Event Management

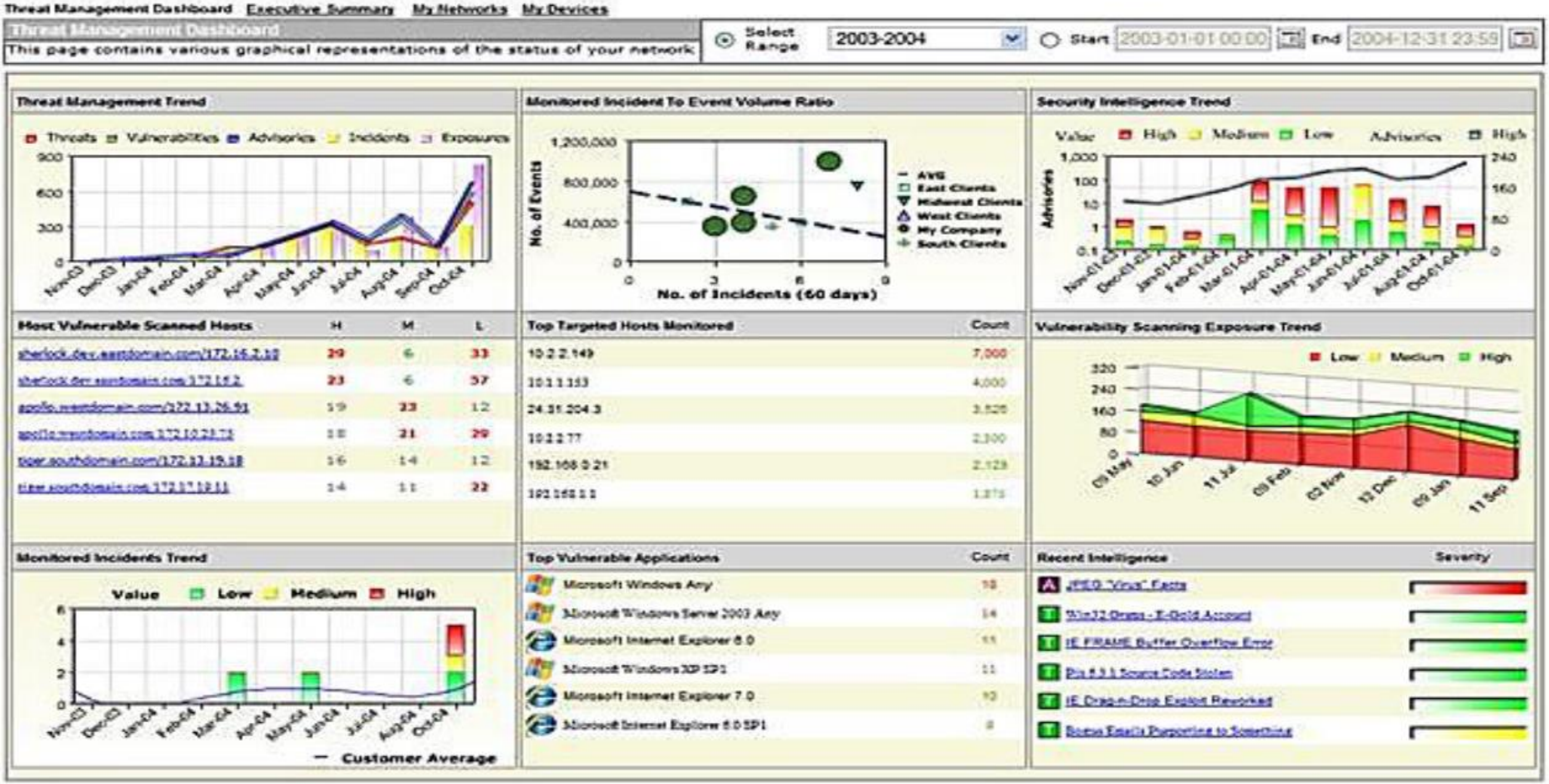
- EEM provides registration to the event in a private access and authentication through a gateway.
- Password with Smartcard or Biometrics (example face and thumbprint recognition) are used for verification in order to access the system.
- Event analytics monitors the event's progress and reports that are retrieved from multiple devices using MIB (Management Information Base) protocol.

EEM - Enterprise Event Management

Commercial EEM	Open Source EEM
CISCO IOS Embedded Event Manager	SNMP Notif
	Syslog

SIM - Security Information Management

- SIM is systems of management framework facilitating the collection, retention and translation of security control data into relevant risk management information.
- SIM includes log data generated from antivirus, IDS, IPS file systems, firewalls, routers, switches and servers to discover problems within a system
- SIM performs historical analysis and reporting for security events so that enables incident response and Forensic Programs
- SIM monitors compliance, manages risk from control breaches and reduce risk from technical control failures
- SIM Architecture consists of a) event consolidation, b) event management, b
- 1) analysis, b 2) reporting and b 3) tracking escalation and event archiving.



This page contains various graphical representations of the status of your network

Most Vulnerable Scanned Hosts	H	M	L
sherlock.dev.eastdomain.com/172.16.2.10	29	6	33
sherlock.dev.eastdomain.com/172.16.2	23	6	57
apollo.westdomain.com/172.13.26.91	19	23	12
apollo.westdomain.com/172.10.23.73	18	21	29
tiger.southdomain.com/172.13.19.18	16	14	12
tiger.southdomain.com/172.17.19.11	14	11	22

Top Targeted Hosts Monitored	Count
10.2.2.149	7,000
10.1.1.153	4,000
24.31.204.3	3,525
10.2.2.77	2,300
192.168.0.21	2,129
192.168.1.1	1,375

Top Vulnerable Applications	Count
Microsoft Windows Any	18
Microsoft Windows Server 2003 Any	14
Microsoft Internet Explorer 6.0	11
Microsoft Windows XP SP1	11
Microsoft Internet Explorer 7.0	10
Microsoft Internet Explorer 6.0 SP1	8

Recent Intelligence	Severity
A JPEG "Virus" Facts	
T Win32.Grams - E-Gold Account	
T IE FRAME Buffer Overflow Error	
T Pix 6.3.1 Source Code Stolen	
T IE Drag-n-Drop Exploit Reworked	
T Bogus Emails Purporting to Something	

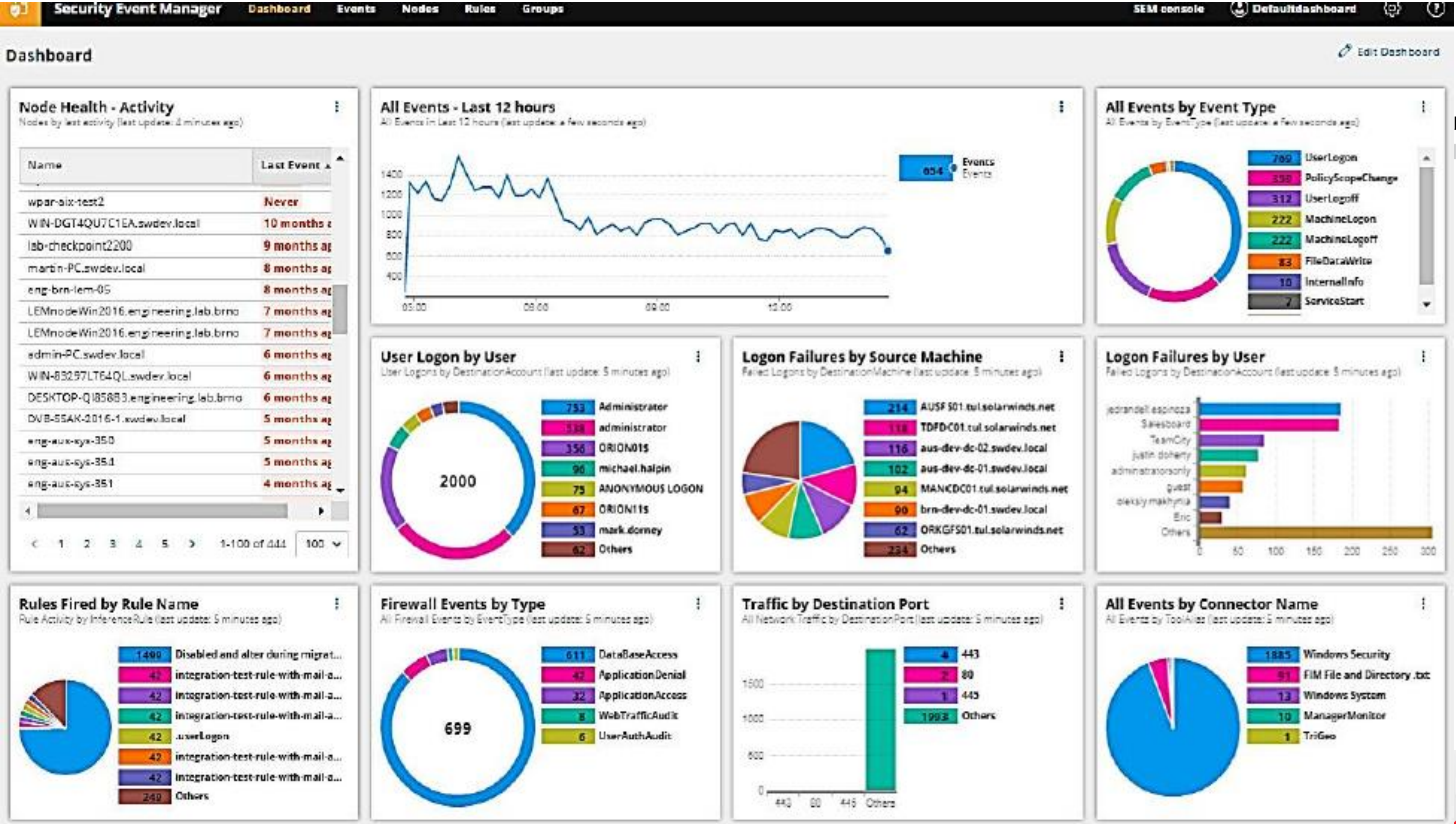
SIM - Security Information Management

Commercial SIM	Open Source SIM
ArchSight ESM	OSSIM
nFX’s	Prelude from PreludeIDS
SIM One	
SenSage Enterprise Security Analytics	
Network Intelligence envision	
Symantec SIM 9500	
CISCO Security MARS	
Snare	

SEM - Security Event Management

- SEM is a real time monitoring and event management to support IT security operations.

- SEM notifies network administrators about potential issues.



Dashboard

Node Health - Activity

Nodes by last activity (last update: 4 minutes ago)

Name	Last Event
wpar-aix-test2	Never
WIN-DGT4QU7C1EA.swdev.local	10 months a
lab-checkpoint2200	9 months ag
martin-PC.swdev.local	8 months ag
eng-brn-lem-05	8 months ag
LEMnodeWin2016.engineering.lab.brno	7 months ag
LEMnodeWin2016.engineering.lab.brno	7 months ag
admin-PC.swdev.local	6 months ag
WIN-83297LT64QL.swdev.local	6 months ag
DESKTOP-QI85883.engineering.lab.brno	6 months ag
DVB-SSAK-2016-1.swdev.local	5 months ag
eng-aus-sys-350	5 months ag
eng-aus-sys-354	5 months ag
eng-aus-sys-351	4 months ag

‹ 1 2 3 4 5 › 1-100 of 444 100

All Events - Last 12 hours

All Events in Last 12 hours (last update: a few seconds ago)

654 Events

All Events by Event Type

All Events by EventType (last update: a few seconds ago)

709	UserLogon
339	PolicyScopeChange
312	UserLogoff
222	MachineLogon
222	MachineLogoff
83	FileDataWrite
10	InternalInfo
7	ServiceStart

User Logon by User

User Logons by DestinationAccount (last update: 5 minutes ago)

2000

753	Administrator
338	administrator
356	ORION01$
96	michael.halpin
75	ANONYMOUS LOGON
67	ORION11$
53	mark.dorney
62	Others

Logon Failures by Source Machine

Failed Logons by DestinationMachine (last update: 5 minutes ago)

214	AUSFS01.tul.solarwinds.net
118	TDFDC01.tul.solarwinds.net
116	aus-dev-dc-02.swdev.local
102	aus-dev-dc-01.swdev.local
94	MANCDC01.tul.solarwinds.net
90	brn-dev-dc-01.swdev.local
62	ORKGFS01.tul.solarwinds.net
234	Others

Logon Failures by User

Failed Logons by DestinationAccount (last update: 5 minutes ago)

Rules Fired by Rule Name

Rule Activity by InferenceRule (last update: 5 minutes ago)

1499	Disabled and alter during migrat...
42	integration-test-rule-with-mail-a...
42	integration-test-rule-with-mail-a...
42	integration-test-rule-with-mail-a...
42	.userLogon
42	integration-test-rule-with-mail-a...
42	integration-test-rule-with-mail-a...
249	Others

Firewall Events by Type

All Firewall Events by EventType (last update: 5 minutes ago)

699

611	DataBaseAccess
42	ApplicationDenial
32	ApplicationAccess
8	WebTrafficAudit
6	UserAuthAudit

Traffic by Destination Port

All Network Traffic by DestinationPort (last update: 5 minutes ago)

4	443
2	80
1	445
1993	Others

All Events by Connector Name

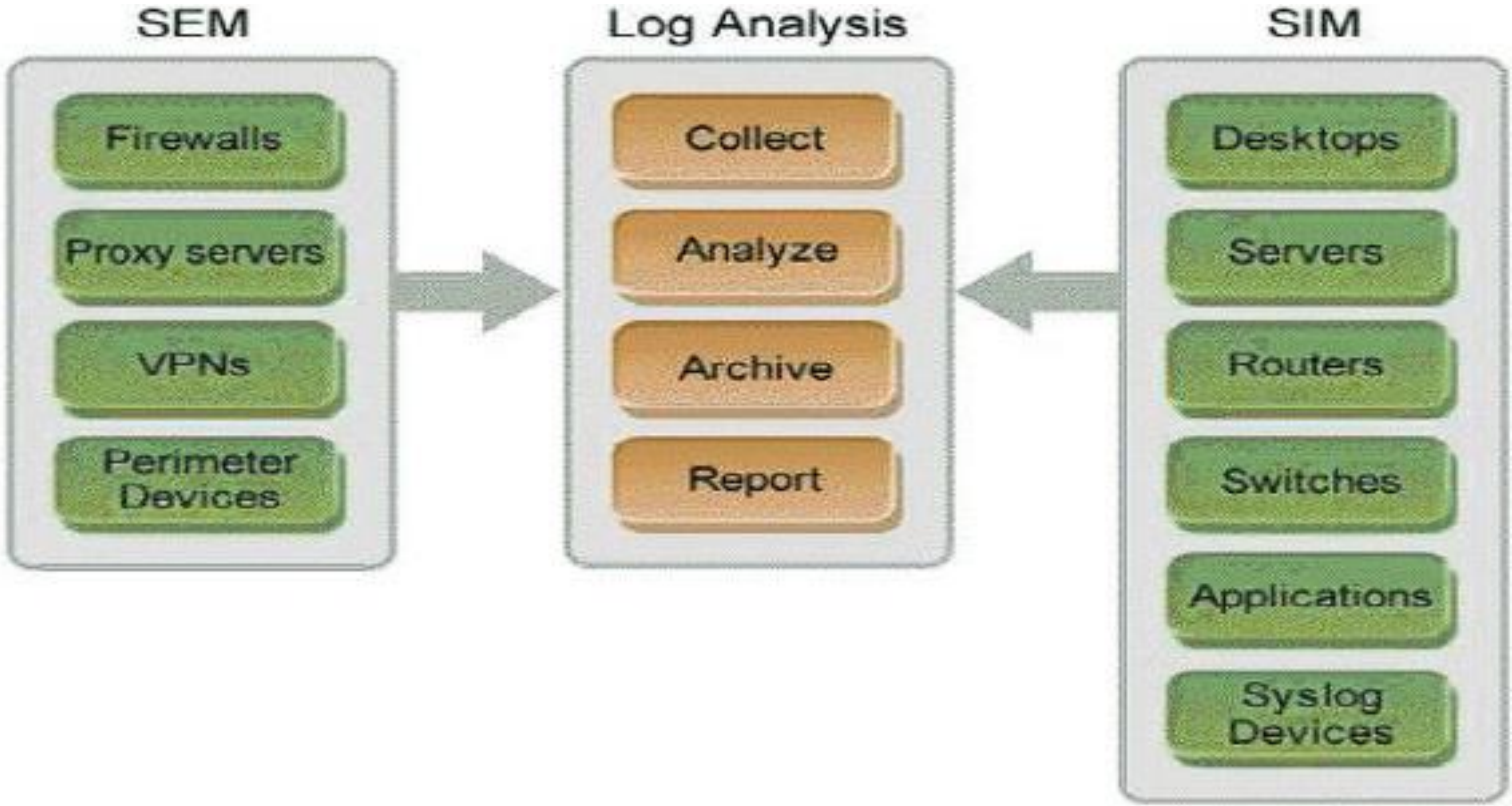
All Events by ToolAlias (last update: 5 minutes ago)

1885	Windows Security
91	FIM File and Directory .txt
13	Windows System
10	ManagerMonitor
1	TriGeo

head

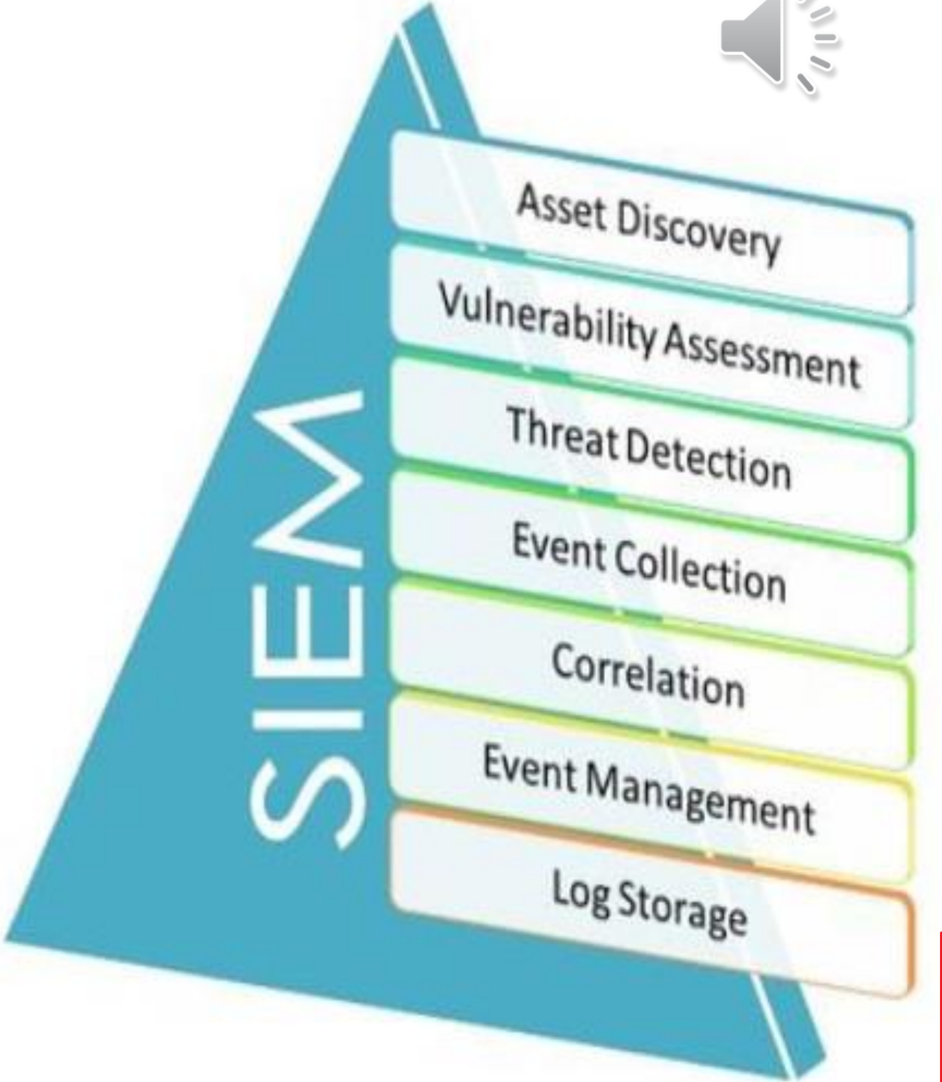
SEM - Security Event Management

Commercial SEM	Open Source SEM
NetIQ Sentinel	
Solar Winds	
Sonic Wall	


SEM
Firewalls
Proxy servers
VPNs
Perimeter Devices
Log Analysis
Collect
Analyze
Archive
Report
SIM
Desktops
Servers
Routers
Switches
Applications
Syslog Devices

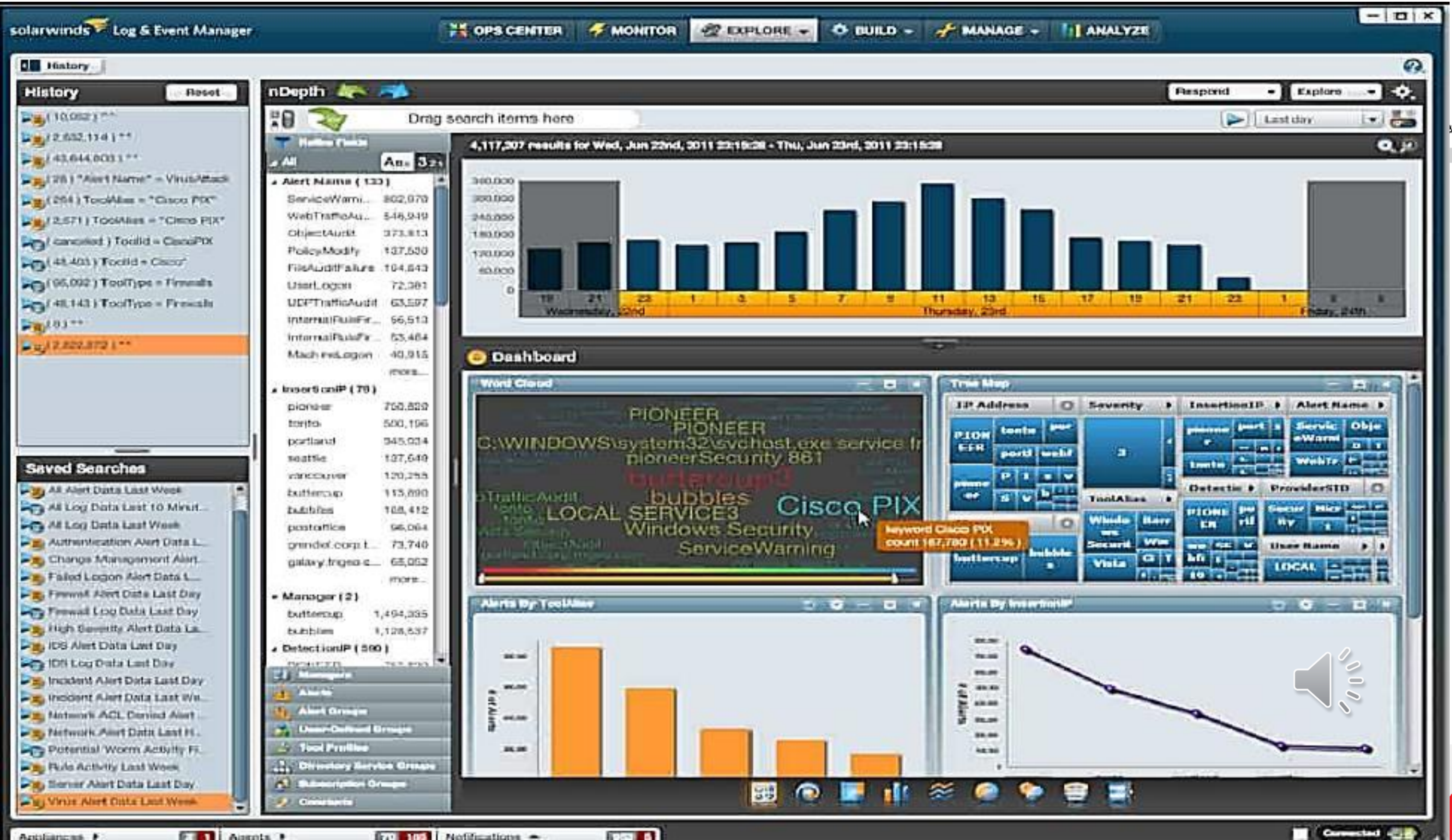
SIEM - Security Info Event Management

- SIEM = SIM + SEM
- SIEM is a set of tools that combine SIM and SEM
- SIEM provides centralize storage, interpretation and analysis of logs, events and other generated logs executed from various of devices.
- SIEM is crucial because user or tracker leaves behind a virtual trail in a network's log data, thus SIEM able to reverse the process of finding the user who commit to crime.



SIEM - Security Info Event Management

Commercial SIEM	Open Source SIEM
SolarWinds Log & Event Manager	OSSEC (HIPS) – host based Now WAZUH
Splunk Enterprise Security	
LogRhythm	
AlienVault Unified Security Management	
McAfee Enterprise Security Manager	



History

- (10,092) **
- (2,632,114) **
- (43,644,803) **
- (28) "Alert Name" = VirusAttack
- (264) ToolAlias = "Cisco PIX"
- (2,571) ToolAlias = "Cisco PIX"
- (canceled) ToolId = CiscoPIX
- (48,403) ToolId = Cisco"
- (96,092) ToolType = Firewalls
- (48,143) ToolType = Firewalls
- (0) **
- (2,822,372) **

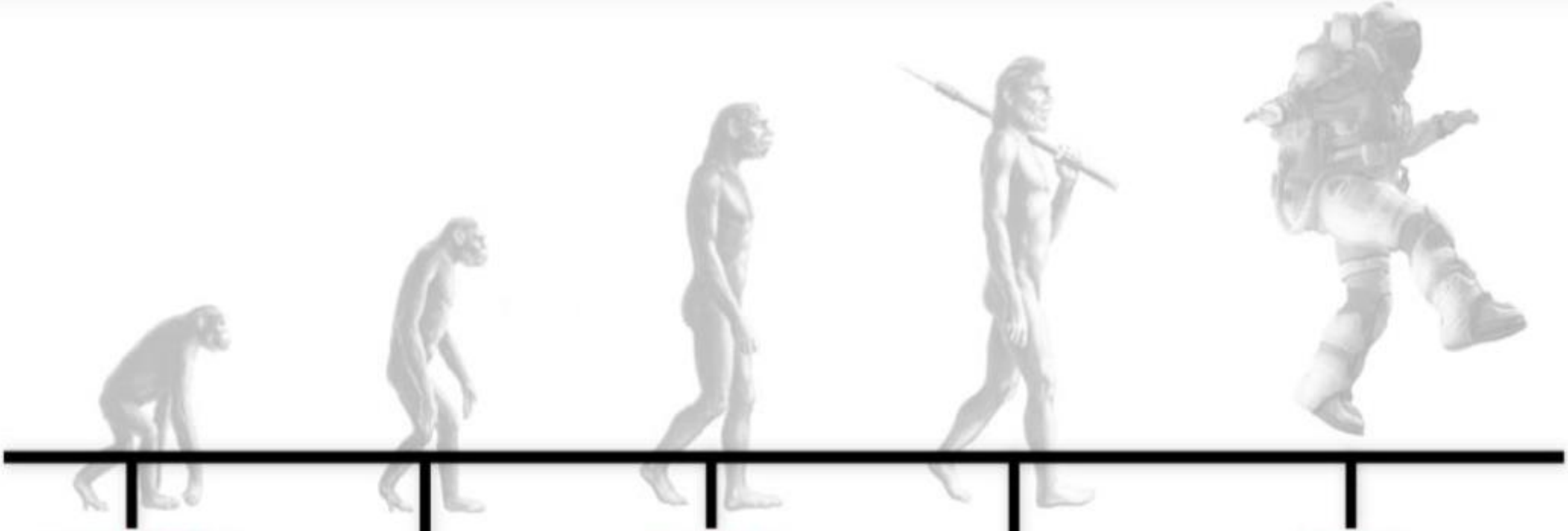
4,117,207 results for Wed, Jun 22nd, 2011 23:15:28 - Thu, Jun 23rd, 2011 23:15:28

Alert Name (133)	
ServiceWarni...	802,070
WebTrafficAu...	546,949
ObjectAudit	373,813
PolicyModify	137,530
FileAuditFailure	104,643
UserLogon	72,381
UDPTrafficAudit	63,597
InternalRuleFir...	56,513
InternalRuleFir...	53,464
MachineLogon	40,915
	more...
InsertionIP (78)	
pioneer	750,829
tonto	500,196
portland	345,024
seattle	137,649
vancouver	120,255
buttercup	115,890
bubbles	108,412
postoffice	96,064
grendel.corp.t...	73,740
galaxy.trigeo.c...	65,052
	more...
Manager (2)	
buttercup	1,494,335
bubbles	1,128,537
DetectionIP (500)	

Saved Searches

- All Alert Data Last Week
- All Log Data Last 10 Minut...
- All Log Data Last Week
- Authentication Alert Data L...
- Change Management Alert...
- Failed Logon Alert Data L...
- Firewall Alert Data Last Day
- Firewall Log Data Last Day
- High Severity Alert Data La...
- IDS Alert Data Last Day
- IDS Log Data Last Day
- Incident Alert Data Last Day
- Incident Alert Data Last We...
- Network ACL Denied Alert...
- Network Alert Data Last H...
- Potential Worm Activity Fi...
- Rule Activity Last Week
- Server Alert Data Last Day
- Virus Alert Data Last Week

ad



TROUBLE TICKETING

1980s/Early 1990s

Early days of security was a help desk taking calls and creating tickets to address an issue.

SIM & SEM

Late 1990s

Security Information Management & Security Event Management are the primary cybersecurity measures.

SIEM

2005 - Present

The term SIEM was coined by Mark Nicolett and Amrit Williams of Gartner combining SIM & SEM. Creating a more complete security solutions.

SOAR

2016 - Present

Security Orchestration, Automation and Response, or SOAR aggregates security intelligence and context from disparate systems. It uses machine intelligence to reduce the time of incident detection and response process.

COAR

2019

Cloud Orchestration, Automation and Response, or COAR aggregates cloud applications and security intelligence using machine learning to automate data compliance.

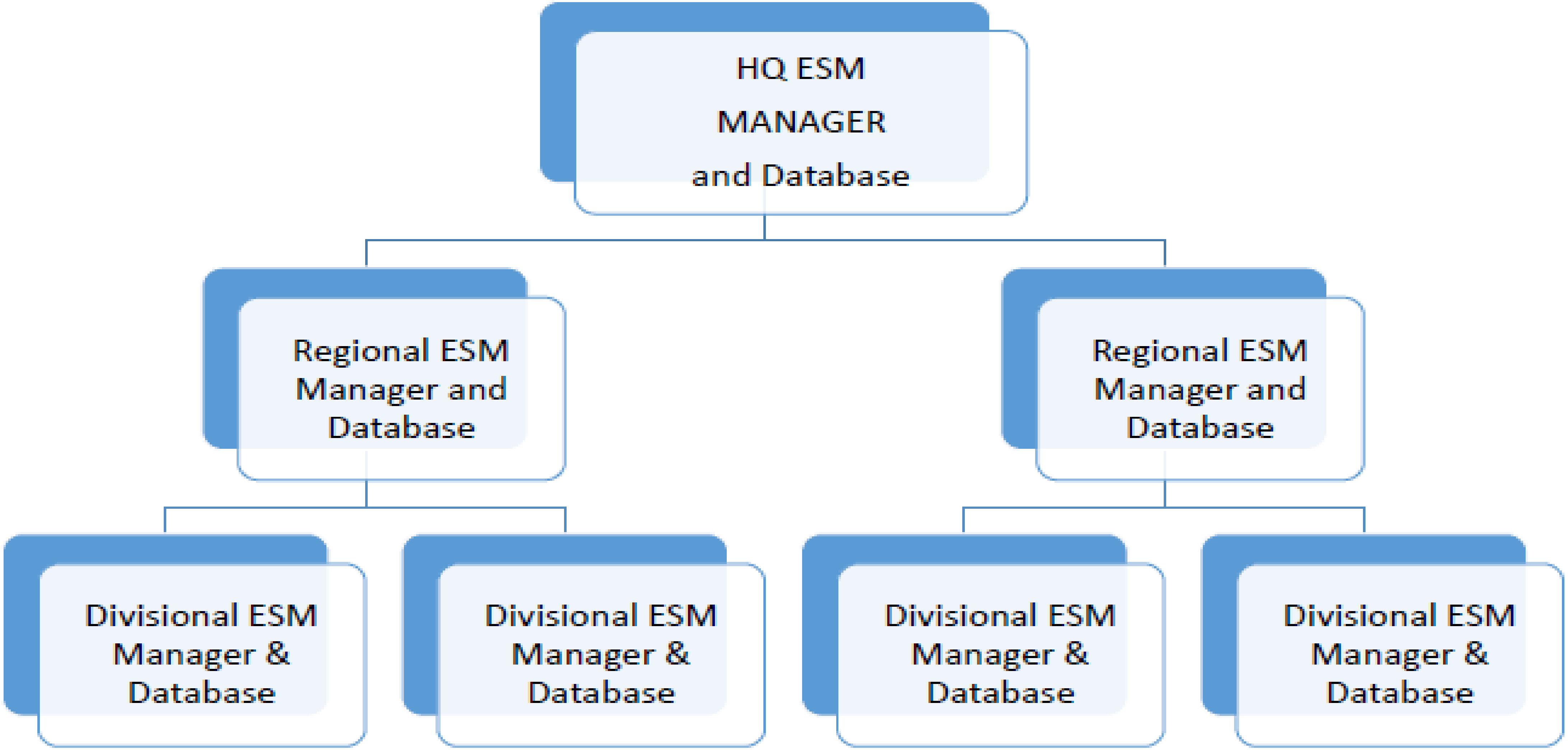
ESM AS A CENTRE OF PHYSICAL & LOGICAL SECURITY

ESM AS A DATA CENTER

- Collaborate and integrate the physical & logical security together
  - Aggregate digital solutions and IP based Protocols. Eg : deploy digital surveillance camera with IP, video surveillance and badge reader information with VPNs

- Become a requirement for incident prevention, detection and management.

EXAMPLE - ESM IMPLEMENTATION



HQ ESM MANAGER and Database

Regional ESM Manager and Database

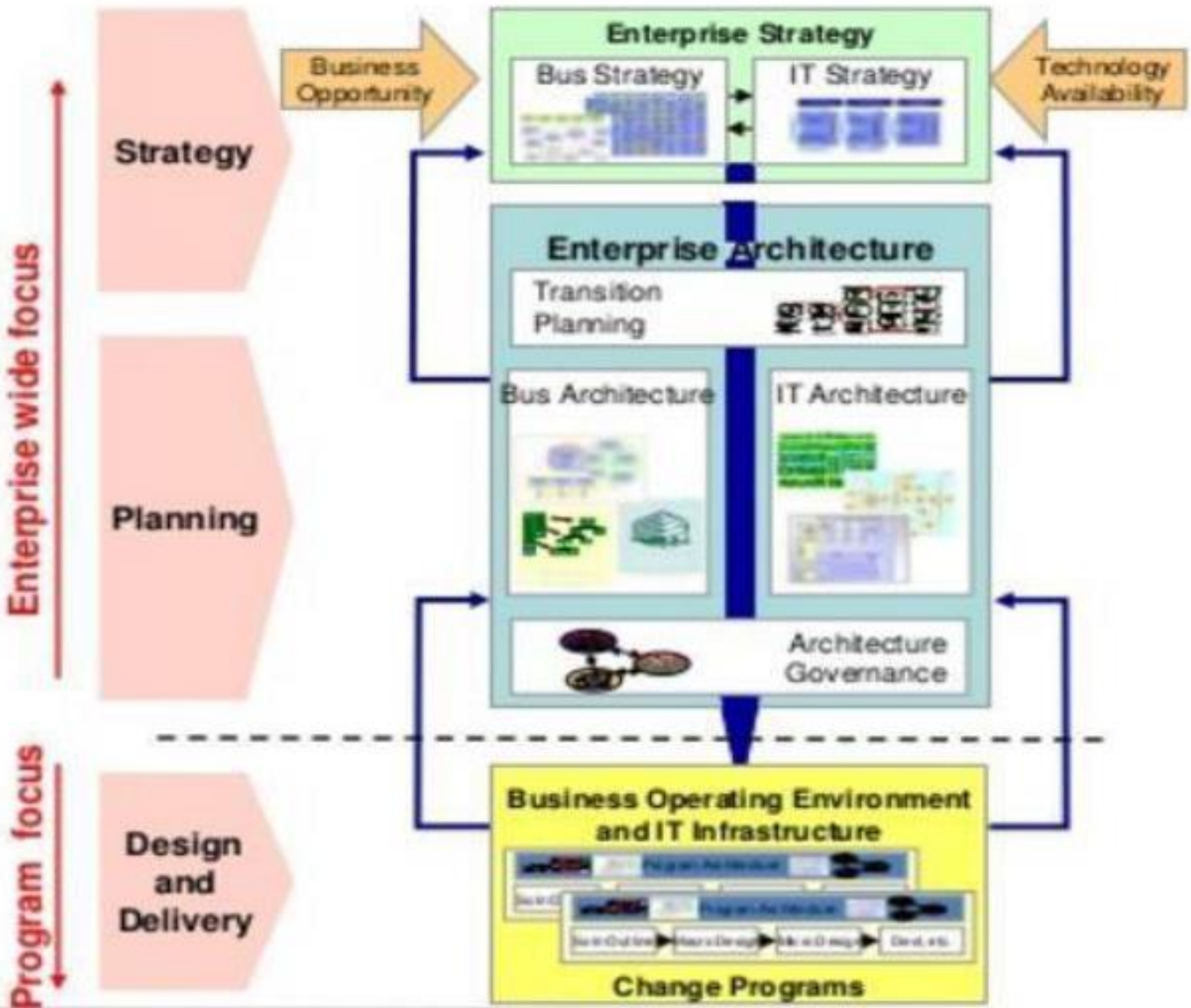
Regional ESM Manager and Database

Divisional ESM Manager & Database

Divisional ESM Manager & Database

Divisional ESM Manager & Database

Divisional ESM Manager & Database



"Do the Right Things"

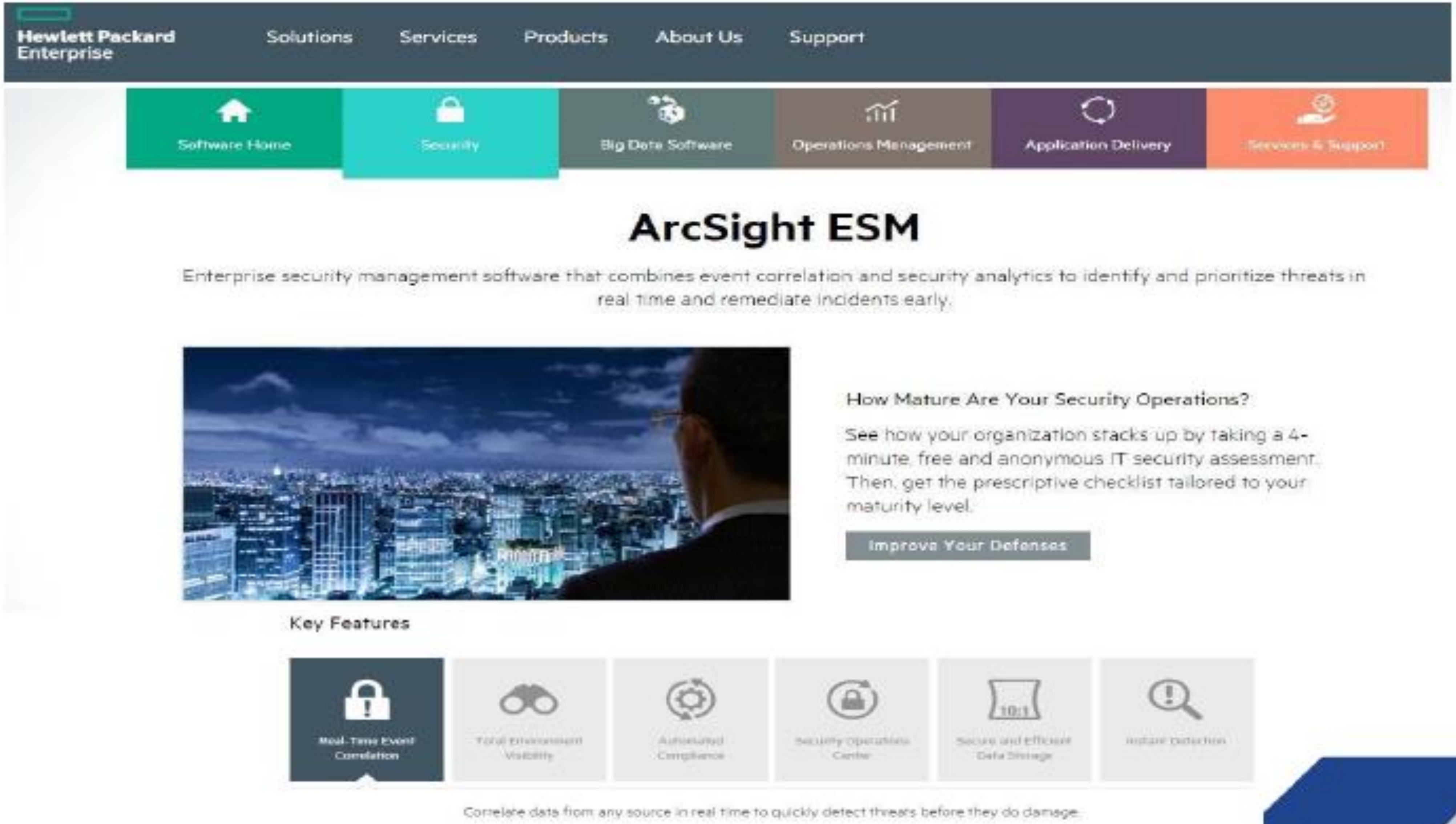
Strategy
= *"the city's purpose & goals"*

Enterprise Architecture
= *"the city plan"*

"Do the Right Things Right"

System Design
= *"the buildings"*

Example – ESM – HP Product



ArcSight ESM

Enterprise security management software that combines event correlation and security analytics to identify and prioritize threats in real time and remediate incidents early.

How Mature Are Your Security Operations?

See how your organization stacks up by taking a 4-minute, free and anonymous IT security assessment. Then, get the prescriptive checklist tailored to your maturity level.

Key Features

Real-Time Event Correlation
Total Environment Visibility
Automated Compliance
Security Operations Center
10:1
Secure and Efficient Data Storage
Instant Detection

Correlate data from any source in real time to quickly detect threats before they do damage.

ESM SERVICES

ESM SERVICES

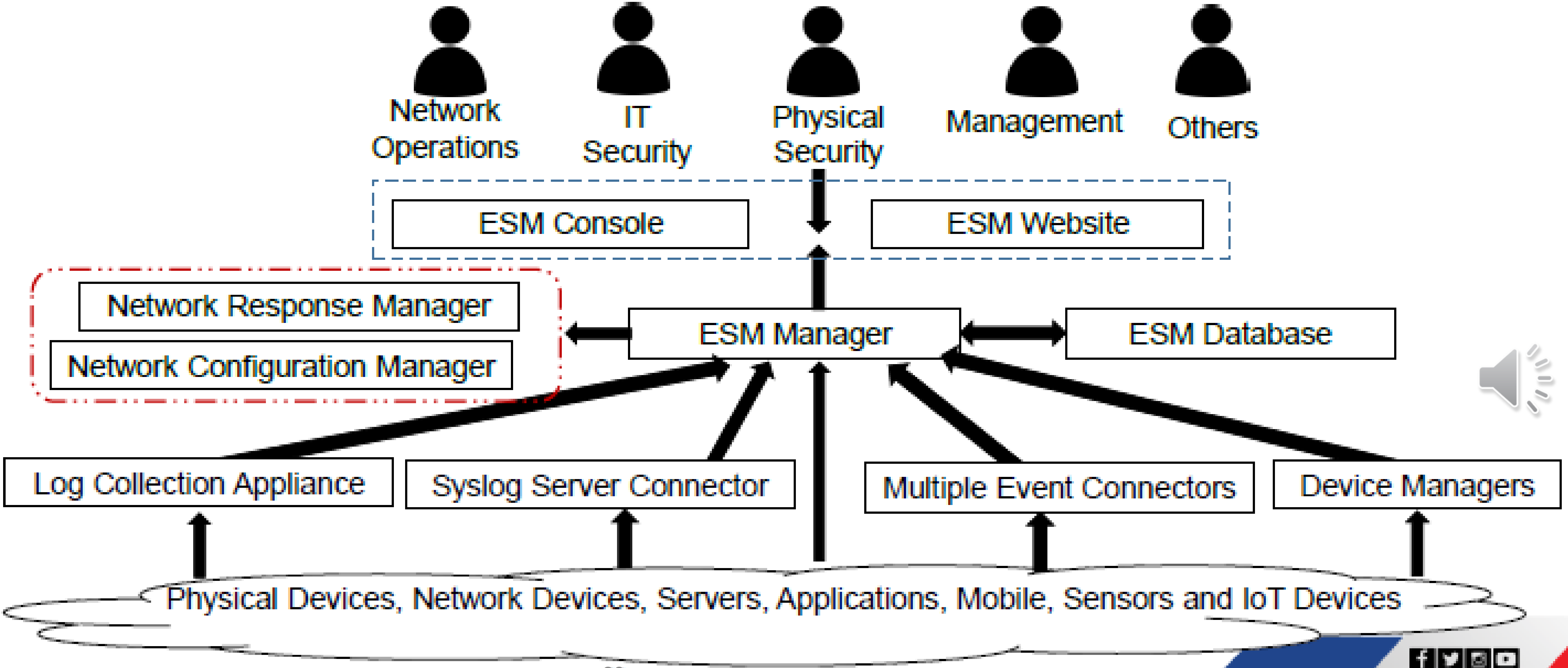
- User Administration
- Single Sign On (SSO)
- Reporting Capabilities
- Vulnerability Assessment
- Asset Vulnerability
- Alert Management Log Management
- Behavioural Monitoring
- Network Monitoring
- Security Monitoring

SECURITY MONITORING

- The security monitoring in ESM provides a complete documentation of investigation and audit trail for forensics process.
- Two basic types of security monitoring:
  - **Common Access Cards**
    - Access control with a single card
    - Include photo ID, descriptive information
    - Scanning CAC reader by door to enter building, swipe CAC connect to PC, use CAC to encrypt information & access website
  - **In House Physical Security**
    - Monitoring fire alarms, burglar alarms, facility access and video surveillance

ESM DEPLOYMENT STRATEGY

ESM DEPLOYMENT STRATEGY



ESM DEPLOYMENT STRATEGY

- CIO manages ESM frameworks to reduce risks in the enterprise and foster security culture in long term planning. Strategy steps of ESM deployment are:
- **Patch Management**
- The patch is extra programming codes to overcome the vulnerability in software development. The purpose is to scanning and updating the patch for mitigation in every phases of security cycle.
- **Threat Modelling**
- Identify Threat, Survey, Data Validation (e.g. SQL Injection), use STRIDE Threat Model
- **Risk Management**
- Risk management helps organization to reduce risk and prevent the company from being a victim. Also, adopt intelligence based security solution in threat information sources.

ESM DEPLOYMENT STRATEGY

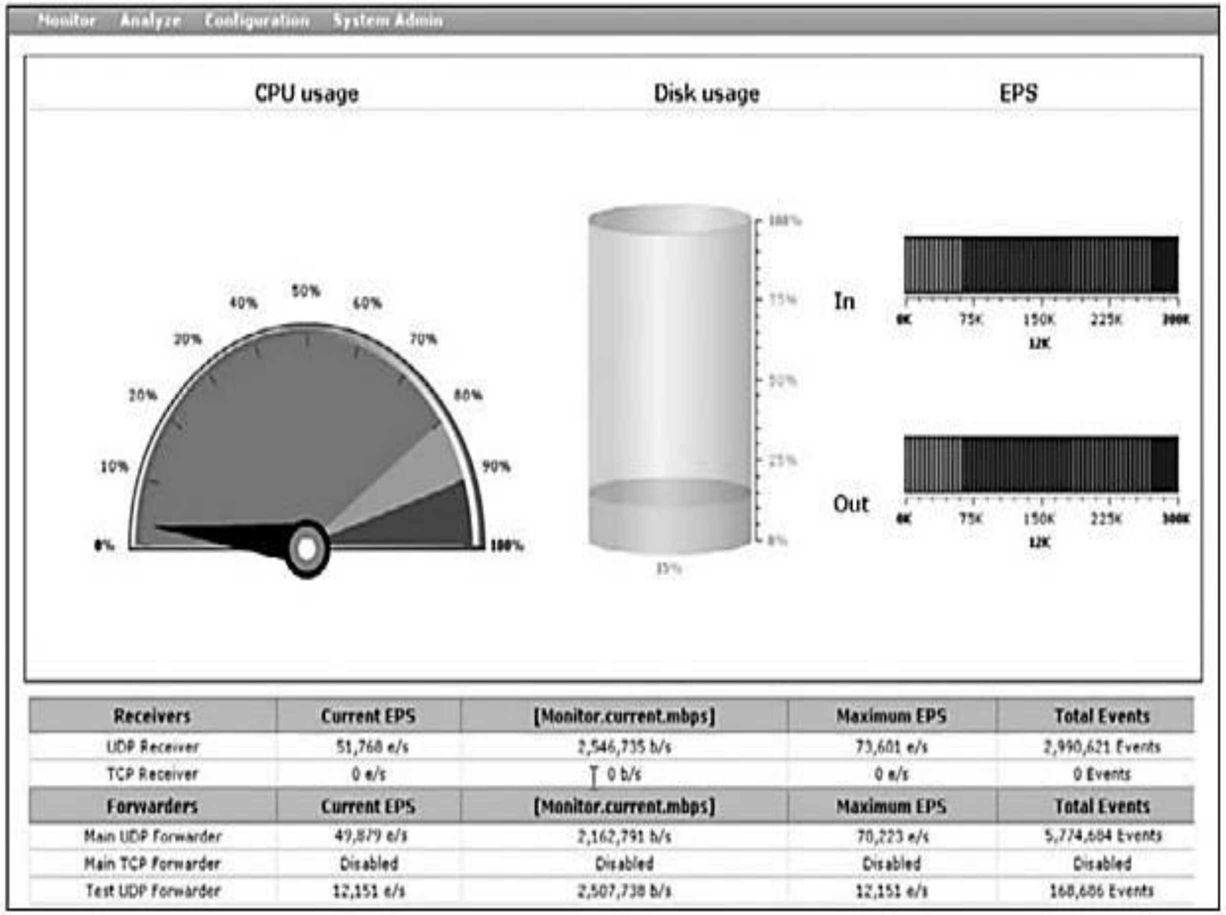
- **Architecture Principles**
- Implement multiple control to prevent damage in the company. The architecture provides a risk mitigation for specific threats. The principles in ESM are:
- Security Resilient security defense using software based tool (e.g. server)
- Segregation (different VLAN, Trunk and VPN)
- Regulator Compliance and Efficiency Industry best practices followed to the standard or procedure compliance such as Incident Audit or Incident Response
- **Bring your own device (BYOD) and mobile device mgmt. (MDM)**
- Employee who bring devices and smart phone into the enterprise need to inform to the higher level of management. A standard procedure for BYOD and MDM need to properly manage for enterprise safety.

LOG COLLECTION APPLIANCE

- **<u>Physical, Network and Mobile Devices</u>**
- ESM system captures logs from various devices for data processing.
- **<u>Log Collection Appliance</u>**
- Data about log is collected at different phase, level and resources.

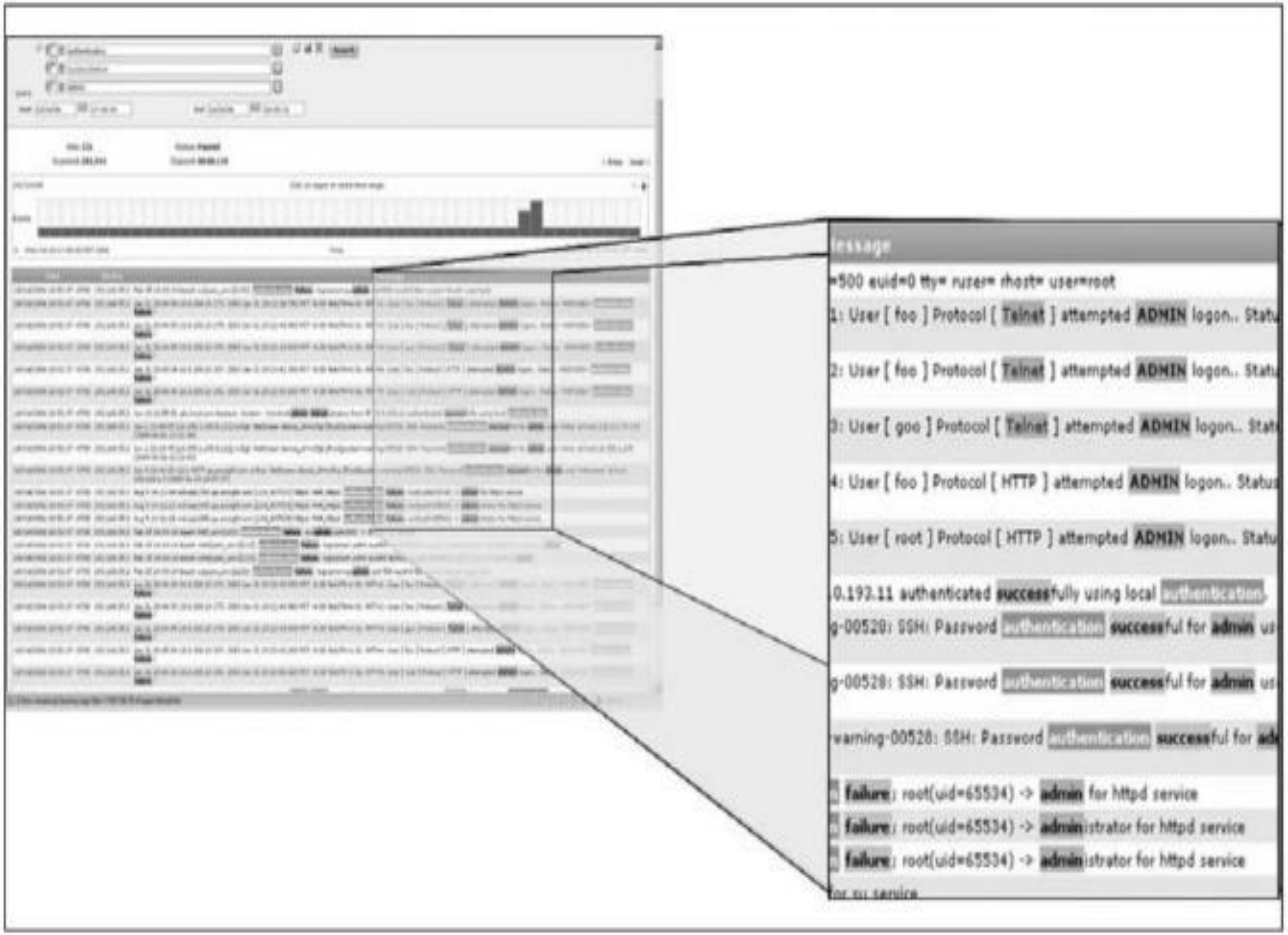
Focus on system status view where Statistics regarding CPU usage, disk usage, and number of logs/events per second being received and transported to ESM Manager. Its provides a fast and easy way to understand what is happening with in the appliance.

System StatusView
(Source: ArcSight Logger v1.0)



Receivers	Current EPS	[Monitor.current.mbps]	Maximum EPS	Total Events
UDP Receiver	51,768 e/s	2,546,735 b/s	73,601 e/s	2,990,621 Events
TCP Receiver	0 e/s	0 b/s	0 e/s	0 Events
Forwarders	**Current EPS**	**[Monitor.current.mbps]**	**Maximum EPS**	**Total Events**
Main UDP Forwarder	49,879 e/s	2,162,791 b/s	70,223 e/s	5,774,684 Events
Main TCP Forwarder	Disabled	Disabled	Disabled	Disabled
Test UDP Forwarder	12,151 e/s	2,507,738 b/s	12,151 e/s	168,686 Events

LOG COLLECTION APPLIANCE



```
lessage
=500 euid=0 tty= ruser= rhost= user=root
1: User [ foo ] Protocol [ Telnet ] attempted ADMIN logon.. Statu
2: User [ foo ] Protocol [ Telnet ] attempted ADMIN logon.. Statu
3: User [ goo ] Protocol [ Telnet ] attempted ADMIN logon.. Stat
4: User [ foo ] Protocol [ HTTP ] attempted ADMIN logon.. Status
5: User [ root ] Protocol [ HTTP ] attempted ADMIN logon.. Statu
.0.193.11 authenticated successfully using local authentication.
g-00528: SSH: Password authentication successful for admin us
g-00528: SSH: Password authentication successful for admin us
warning-00528: SSH: Password authentication successful for ad
 failure: root(uid=65534) -> admin for httpd service
 failure: root(uid=65534) -> administrator for httpd service
 failure: root(uid=65534) -> administrator for httpd service
for su service
```

Analysis View (Source:ArcSight Logger v1.0)

Focus on analysis view displays the logs flowing on certain criteria such as time, protocols, source IPs, destination IPs and other key variable. Eg: Image show Telnet access for admin account (failures and successes) where information and passwords are transmitted in clear text.

SYSLOG SERVER CONNECTOR

- Syslog Server collects syslog messages from number of devices.
- The server is called as connector, which it pre processes the syslog and submit to the ESM.
- Example of syslog server connector is :
  - SNMP (wired)
  - OPSEC (wired)
  - MRTG (wired)
  - PRTG (wired)
  - Wireshark (wireless)

SYSLOG SERVER CONNECTOR

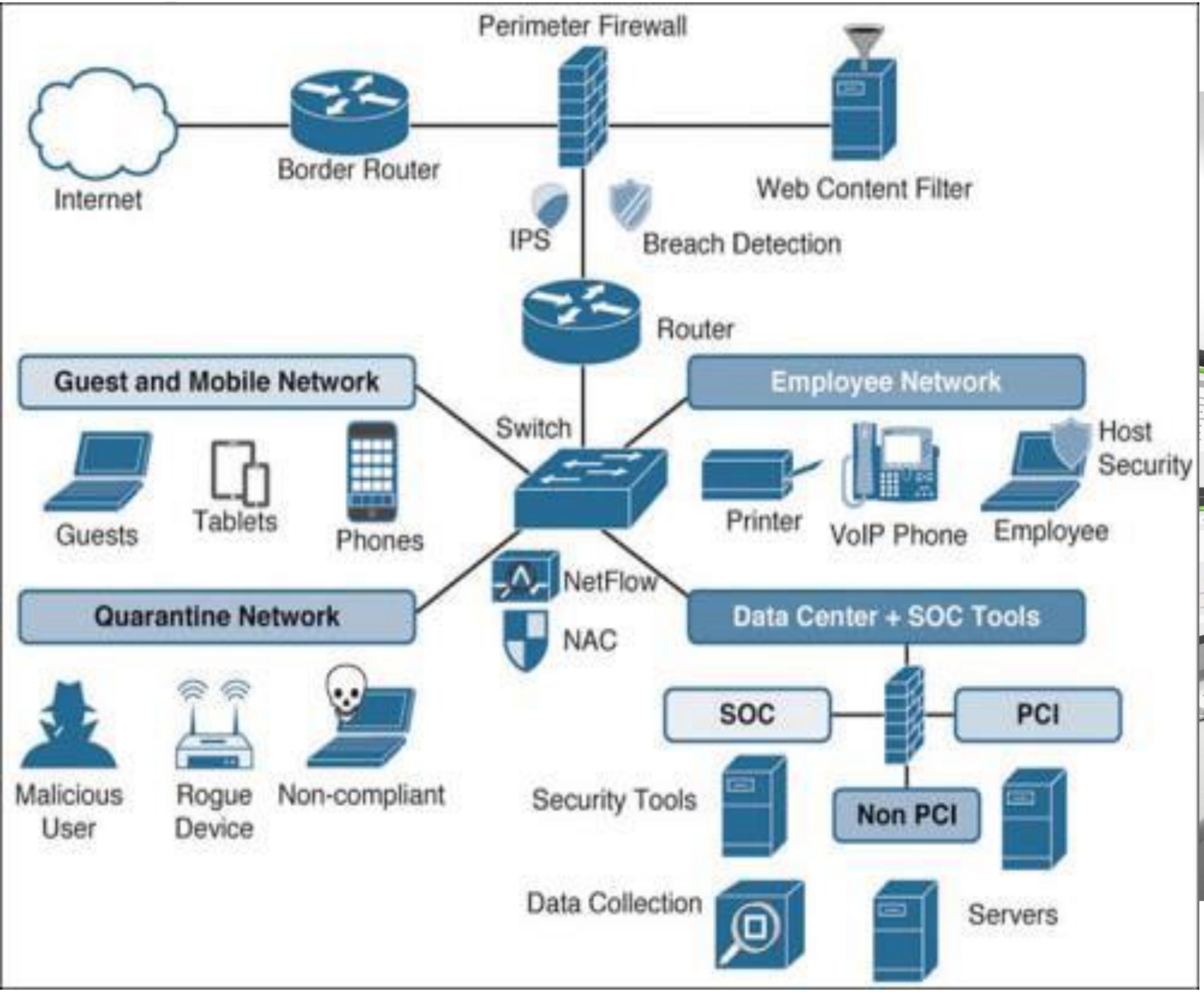
- Move multiple events into the ESM to be analyze.
- Using existing server to deploy a number of connectors receive, pre-process and relay logs to ESM manager.

- Server built with multiple connectors installed.

DEVICE MANAGER

- Deploy log connectors to any natural aggregation points
- Commonly firewall managers, IDS managers, access control databases
- Collect all the mission critical logs while at the same time reducing the number of point devices

CONVERGENCE OF NETWORK OPERATIONS CENTRE (NOC) & SECURITY OPERATIONS CENTRE (SOC)

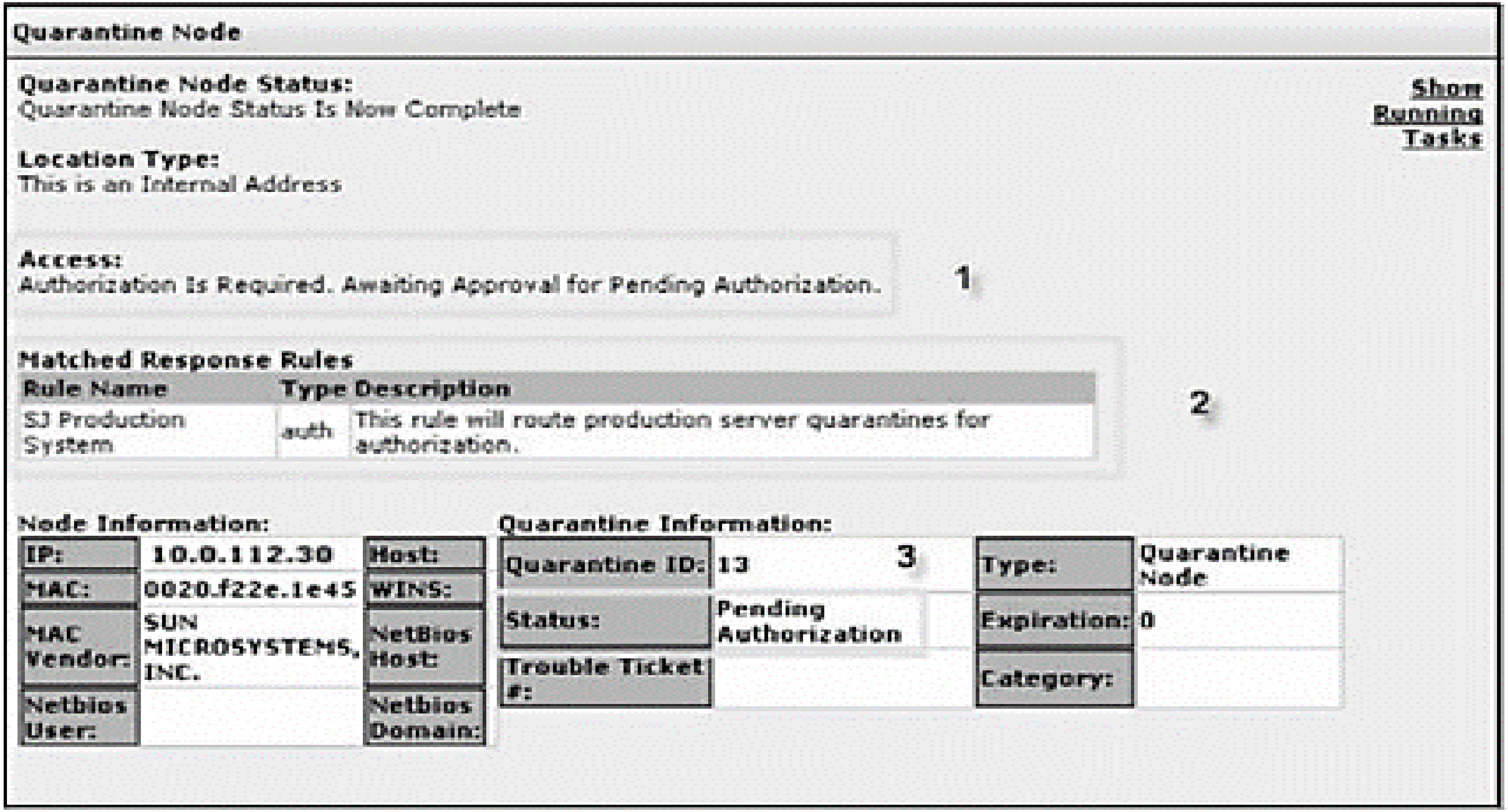

Perimeter Firewall
Internet
Border Router
Web Content Filter
IPS
Breach Detection
Router
Guest and Mobile Network
Switch
Employee Network
Guests
Tablets
Phones
Printer
VoIP Phone
Host Security
Employee
NetFlow
NAC
Quarantine Network
Data Center + SOC Tools
SOC
PCI
Malicious User
Rogue Device
Non-compliant
Security Tools
Non PCI
Data Collection
Servers

Intrusion Alert!

- IT Mission has change NOCs and SOCs more focused on business impact than hardware and software impact
- NOCs and SOCs need to collaborate effectively to handle the risk in term of analysis, workflow and response
- Important concept in convergence is separation of duties and checks and balances
- Convergence is powerful concept but if without good process , it creates inverse situation and slow down operations and reduce security
- Two main criteria need to be considered are:

a) people & process and b) technology.

Example: Incident Response using ArcSight NRM v2.0



Quarantine Node

Show Running Tasks

Quarantine Node Status:
Quarantine Node Status Is Now Complete

Location Type:
This is an Internal Address

Access:
Authorization Is Required. Awaiting Approval for Pending Authorization.

Matched Response Rules

Rule Name	Type	Description
SJ Production System	auth	This rule will route production server quarantines for authorization.

Node Information:

IP:	10.0.112.30	Host:	
MAC:	0020.f22e.1e45	WINS:	
MAC Vendor:	SUN MICROSYSTEMS, INC.	NetBios Host:	
Netbios User:		Netbios Domain:	

Quarantine Information:

Quarantine ID:	13	Type:	Quarantine Node
Status:	Pending Authorization	Expiration:	0
Trouble Ticket #:		Category:	

Thank You

MyUTeM

www.utem.edu.my