The Business Case for Security Information and Management Systems

Engr. Prof. Dr. Athar Mahboob, TI
Professor and Dean
Faculty of Engineering & Applied Sciences
DHA Suffa University
Karachi, Pakistan
Email:athar.mahboob@dsu.edu.pk

8th International InfoSec Conference, Karachi
December 10, 2013

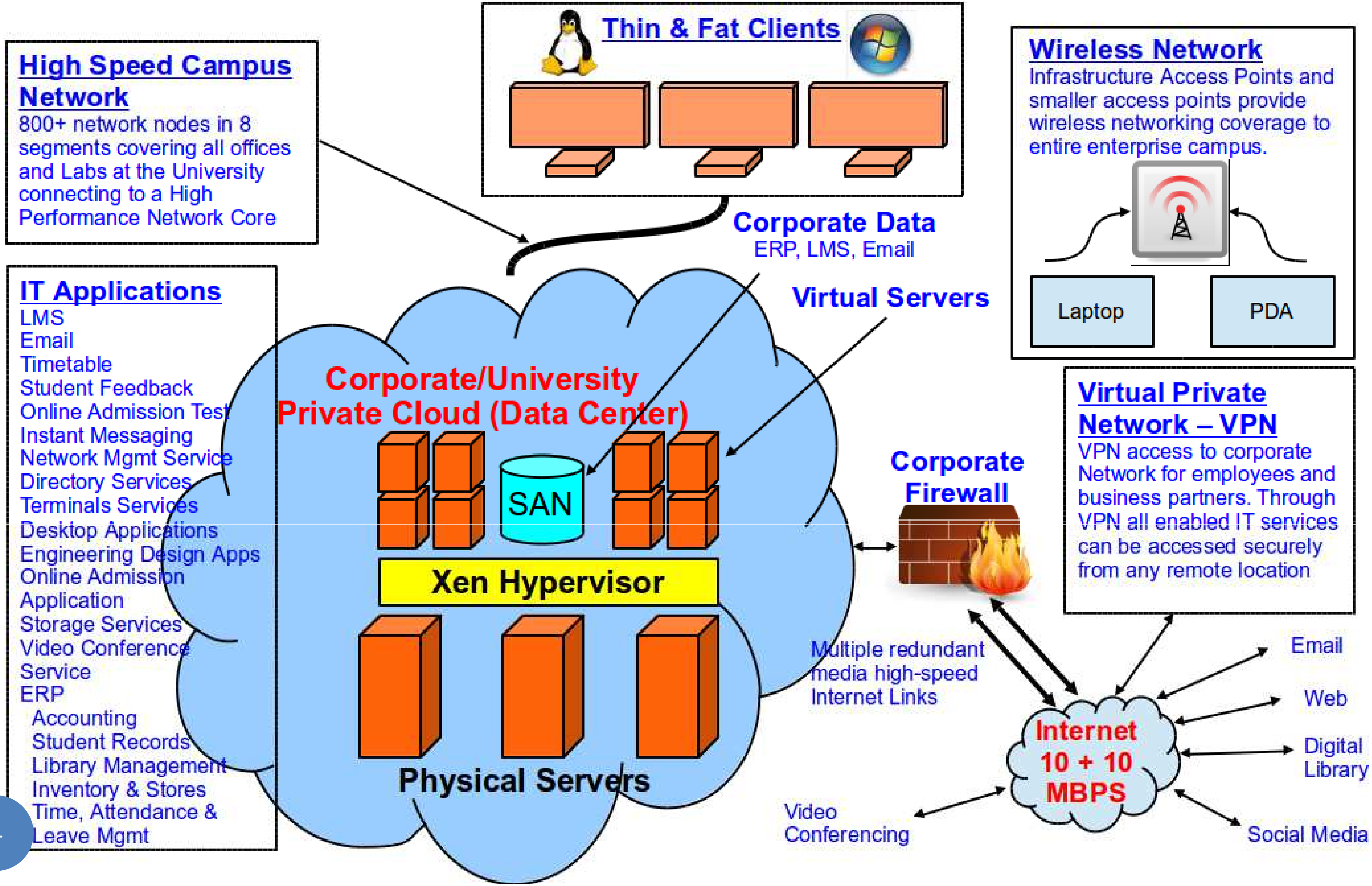
Presentation Objective

- Introduction to Security Information and Event Management
- Understand the business case for a SIEM solution
- Understand the technical architecture of a SIEM solution
- Get familiar with an economical and open source SIEM solution – OSSIM

Dr. Athar Mahboob, TI

- Professor, Dean & Director IT, DHA Suffa University, Karachi 2012-2013
- PhD (Information Security & Cryptology), NUST, Pakistan, 2005
- MS & BS (Electrical Engineering), Florida State University, USA, 1995/1992
- Awarded Tamgha-e-Imtiaz (TI) by the President, Islamic Republic of Pakistan on account of valuable contributions to Engineering and Science & Technology Education in the country, 2012
- 25+ years of Teaching, Research, Industrial and Management Experience, 1988-2013
- President Ibn Khaldun Systems: successfully managed more than 50 industrial projects 2005-2012
- Former Head of Computer Science Department, PNEC-NUST, Karachi, 2011-2012
- Former Head of Computer Engineering Department, Sir Syed University of Engineering & Technology (SSUET), Karachi, 1996-2001
- Former Head of Linux Task Force for promotion of Linux and open source software, Ministry of Science & Technology (MoST), Government of Pakistan, 2001-2002
- HEC Approved PhD Supervisor
- Published a book on Cyber Security which is being used as a Textbook in advance universities of USA and Europe, 2011
- Invented: Bitwizard Secure Communication Device for VoIP Phones
- Trained large number of students and professionals in Linux, Cryptography, Information Security and Internet Technologies, 1996-2013
- Published more than 30 research papers in referred international journals and international conferences, 1998-2013

Typical Private Cloud



High Speed Campus Network

800+ network nodes in 8 segments covering all offices and Labs at the University connecting to a High Performance Network Core

Thin & Fat Clients

Wireless Network

Infrastructure Access Points and smaller access points provide wireless networking coverage to entire enterprise campus.

Corporate Data

ERP, LMS, Email

Virtual Servers

IT Applications

LMS
Email
Timetable
Student Feedback
Online Admission Test
Instant Messaging
Network Mgmt Service
Directory Services
Terminals Services
Desktop Applications
Engineering Design Apps
Online Admission Application
Storage Services
Video Conference Service
ERP
- Accounting
- Student Records
- Library Management
- Inventory & Stores
- Time, Attendance & Leave Mgmt

Corporate/University Private Cloud (Data Center)

Corporate Firewall

Virtual Private Network – VPN

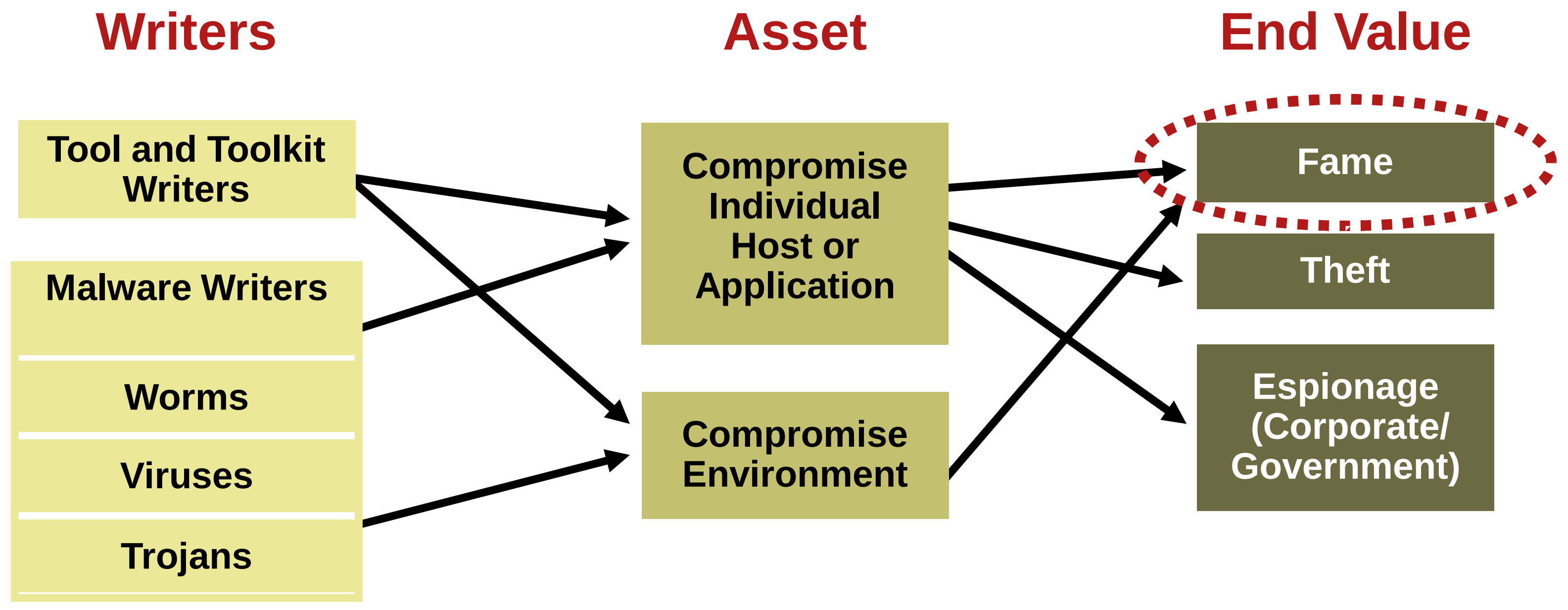
VPN access to corporate Network for employees and business partners. Through VPN all enabled IT services can be accessed securely from any remote location

Multiple redundant media high-speed Internet Links

Information Security

- Information is stored on servers, client machines and hand held devices
- Information needs to be protected and secured from eavesdropping and from damage caused by hackers, viruses and worms
- End to end secure transmission protocols, data encryption techniques and several layers of authentication provide the much needed information security

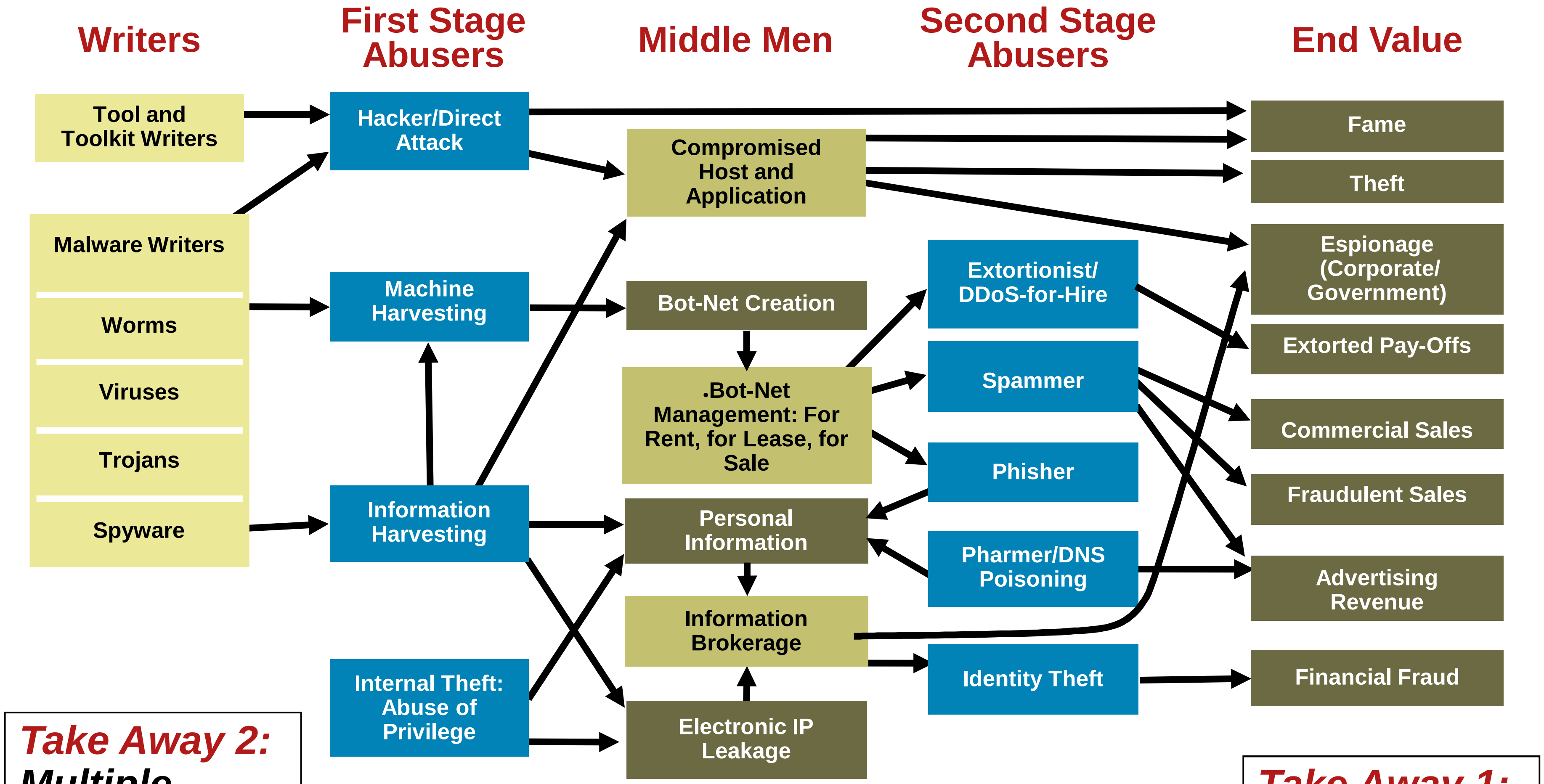
Threat Economy: Historic Attacker Motivations



Take Away: Fame was by far the dominant motivator

From: Security Information Management (SIM) Technology Brief, Ken Kaminski, Cisco Systems, Security Architect – Northeast US, CISSP, GCIA

Threat Economy: Today



Writers

First Stage Abusers

Middle Men

Second Stage Abusers

End Value

Tool and Toolkit Writers

Malware Writers

Worms

Viruses

Trojans

Spyware

Hacker/Direct Attack

Machine Harvesting

Information Harvesting

Internal Theft: Abuse of Privilege

Compromised Host and Application

Bot-Net Creation

.Bot-Net Management: For Rent, for Lease, for Sale

Personal Information

Information Brokerage

Electronic IP Leakage

Extortionist/ DDoS-for-Hire

Spammer

Phisher

Pharmer/DNS Poisoning

Identity Theft

Fame

Theft

Espionage (Corporate/ Government)

Extorted Pay-Offs

Commercial Sales

Fraudulent Sales

Advertising Revenue

Financial Fraud

***Take Away 2:* Multiple methods to achieve goal**

***Take Away 3:* Sustainable economy, resilient to shocks**

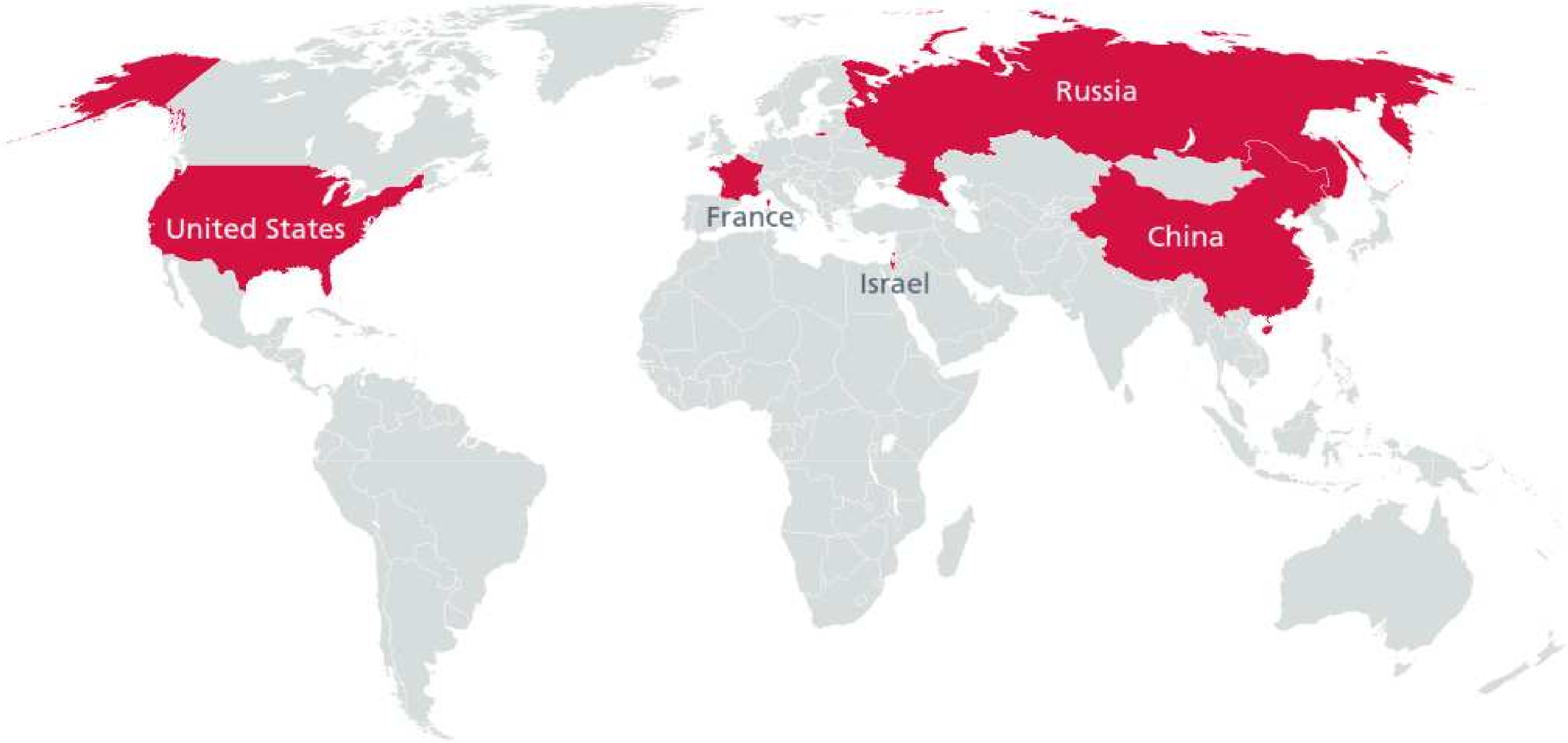
***Take Away 1:* For-Profit end values**

From: Security Information Management (SIM) Technology Brief, Ken Kaminski, Cisco Systems, Security Architect – Northeast US, CISSP, GCIA

All is fair in love and war !!!

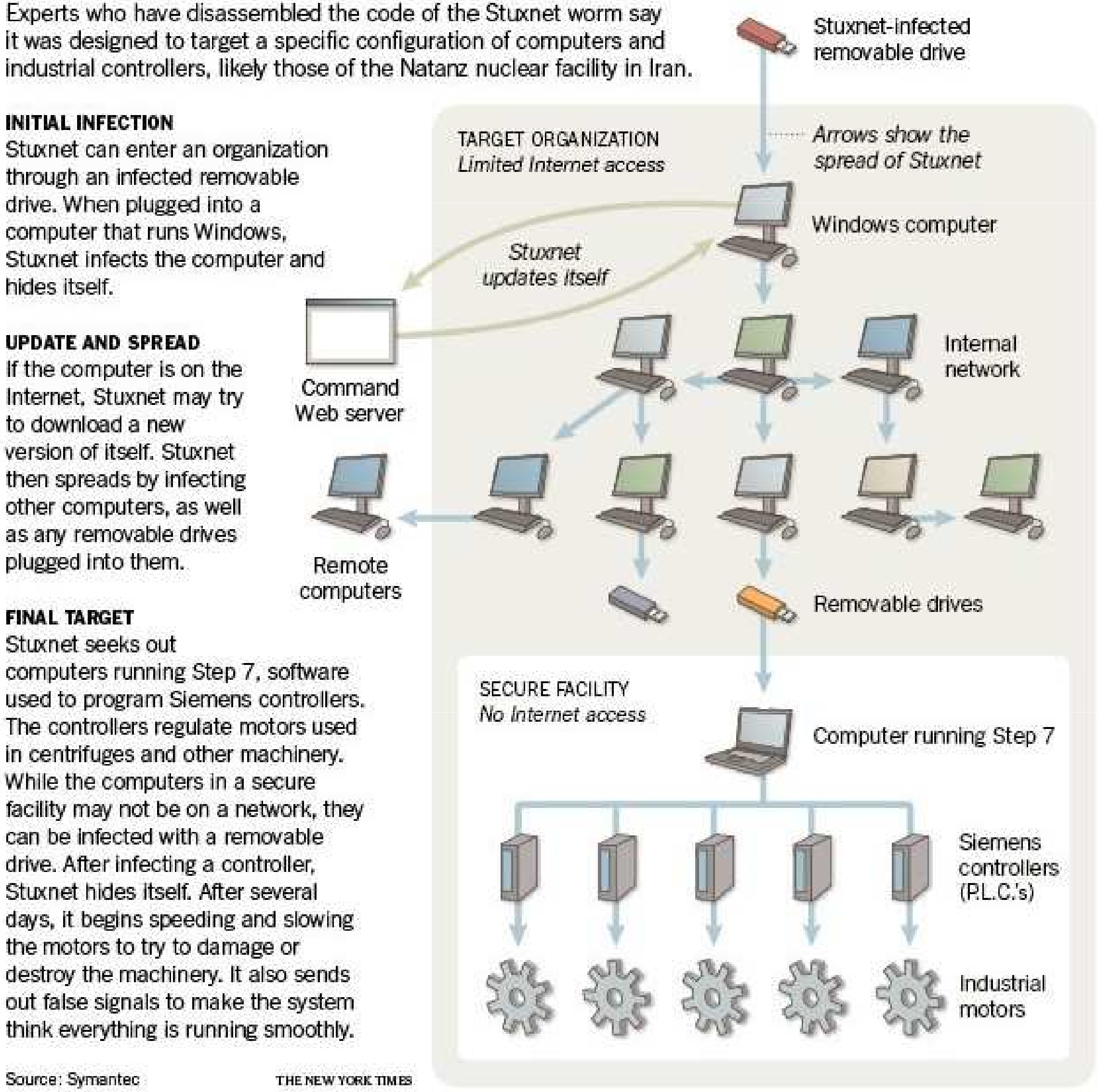
<u>STATE ACTORS ARE PART OF THE THREAT ECONOMY TOO</u>
<u>PUBLIC-PRIVATE PARTNERSHIP :-)</u>

Countries Developing Advanced Offensive Cyber Capabilities



Advanced Persistent Threat - APT

- The attack techniques started from self replicating code evolved into Advanced Persistent Threat
  - Use 0-day
  - Be stealthy
  - Target users
  - Target indirectly
  - Exploit multi-attack vectors
  - Use “state-of-the-art” technique
  - **Be Persistent**
- Hacking is no more about fun
  - Corporate Espionage
  - State Secrets
  - Cyber “Sabotage”



Experts who have disassembled the code of the Stuxnet worm say it was designed to target a specific configuration of computers and industrial controllers, likely those of the Natanz nuclear facility in Iran.

INITIAL INFECTION
Stuxnet can enter an organization through an infected removable drive. When plugged into a computer that runs Windows, Stuxnet infects the computer and hides itself.

UPDATE AND SPREAD
If the computer is on the Internet, Stuxnet may try to download a new version of itself. Stuxnet then spreads by infecting other computers, as well as any removable drives plugged into them.

FINAL TARGET
Stuxnet seeks out computers running Step 7, software used to program Siemens controllers. The controllers regulate motors used in centrifuges and other machinery. While the computers in a secure facility may not be on a network, they can be infected with a removable drive. After infecting a controller, Stuxnet hides itself. After several days, it begins speeding and slowing the motors to try to damage or destroy the machinery. It also sends out false signals to make the system think everything is running smoothly.

Source: Symantec

THE NEW YORK TIMES

APT - Example

- June, 2010 – **StuxNet Worm**
- **Target:** Natanz Nuclear Facility
- **Motivation:** Cyber Sabotage?

Drivers for Information Security Management

- Regulatory Compliance
  - HIPAA, SOX, FISMA, GLBA, FDA, PCI, Basel II, OSHA and ISO 27002
- Information security breaches are costly
  - Need to respond timely to security events
- Information systems environment is heterogeneous, multi-vendor, and complex
- Advance Persistent Threats

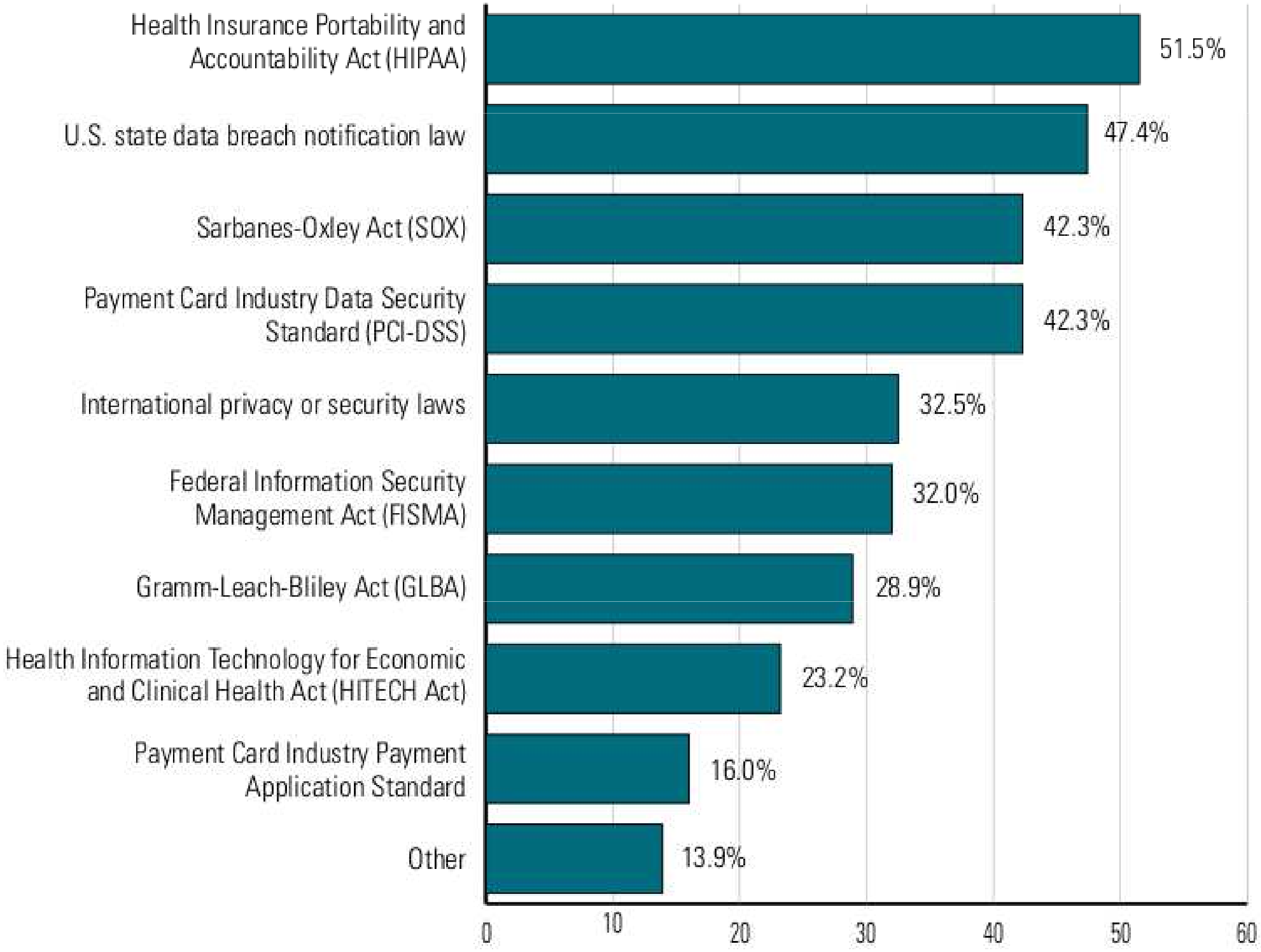
compliance - a state or acts of accordance with established standards, specifications, regulations, or laws. Compliance more often connotes a very specific following of the provided model and is usually the term used for the adherence to government regulations and laws

http://searchcio.techtarget.com/sDefinition/0,,sid182_gci947386,00.html

HIPAA: Health Insurance Portability and Accountability Act
SOX: Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX
FISMA: The Federal Information Security Management Act of 2002
FDA: The Food and Drug Administration
PCI Data Security Standard (PCI DSS): The Payment Card Industry (PCI) and Validation Regulations
Basel II: The New Accord: International Convergence of Capital Measurement and Capital Standards
GLBA: Gramm-Leach-Bliley Act, also known as the Gramm-Leach-Bliley Financial Services Modernization Act
ISO/IEC 27002 (formerly 17799) is an information security standard published and most recently revised in June 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
OSHA: The United States Occupational Safety and Health Administration

Which Laws and Industry Regulations Apply to Your Organization?

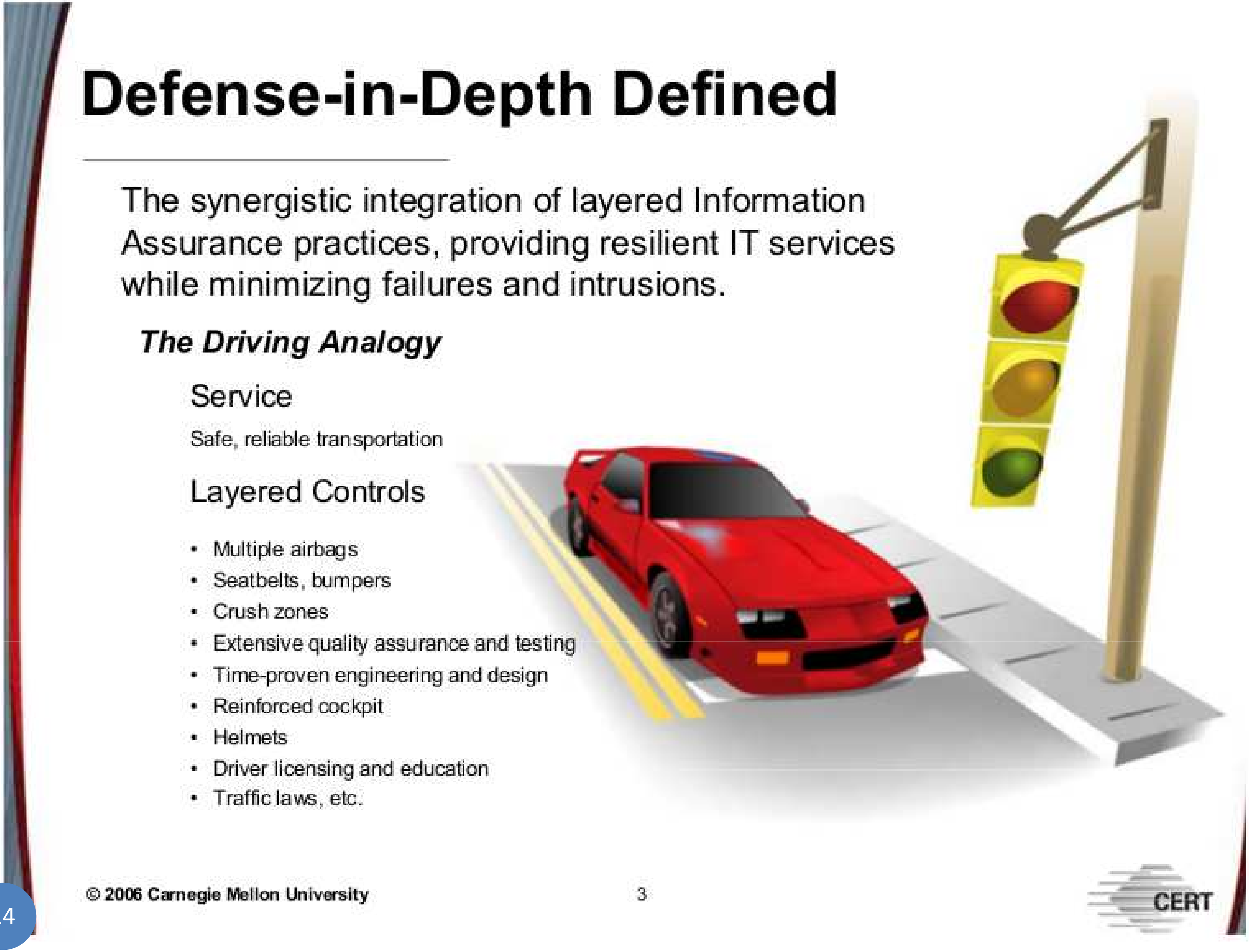
By Percent of Respondents



Security Infrastructure for Defense in Depth Deployed by Typical Enterprise

- Firewalls
- Intrusion Detection Systems/Intrusion Preventions Systems
- Deep-packet Inspection
- Antivirus
- Anti-malware
- Security Event Logs
- Access Control Systems
- Strong Password
- Multi-factor Authentication
- Public Key Infrastructure
- Network Security Protocols (IPSec, TLS, PPTP, etc.)
- Application level gateways
- VPN gateways

Defense in depth is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical for the duration of the system's life cycle. (Wikipedia)



Defense-in-Depth Defined

The synergistic integration of layered Information Assurance practices, providing resilient IT services while minimizing failures and intrusions.

The Driving Analogy

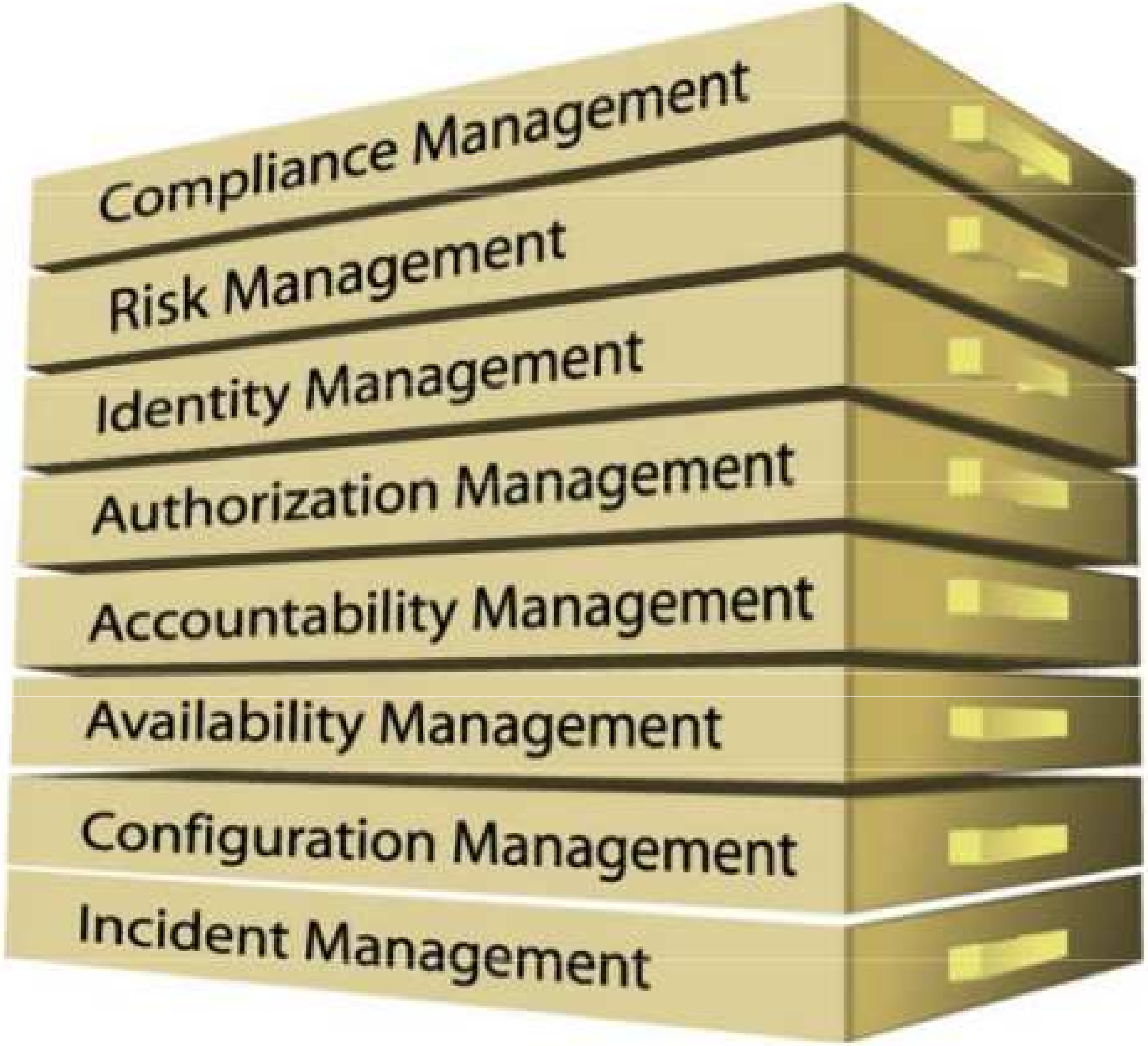
Service

Safe, reliable transportation

Layered Controls

- Multiple airbags
- Seatbelts, bumpers
- Crush zones
- Extensive quality assurance and testing
- Time-proven engineering and design
- Reinforced cockpit
- Helmets
- Driver licensing and education
- Traffic laws, etc.

Defense-in-Depth Components



Compliance Management

Risk Management

Identity Management

Authorization Management

Accountability Management

Availability Management

Configuration Management

Incident Management

Security Event Logs

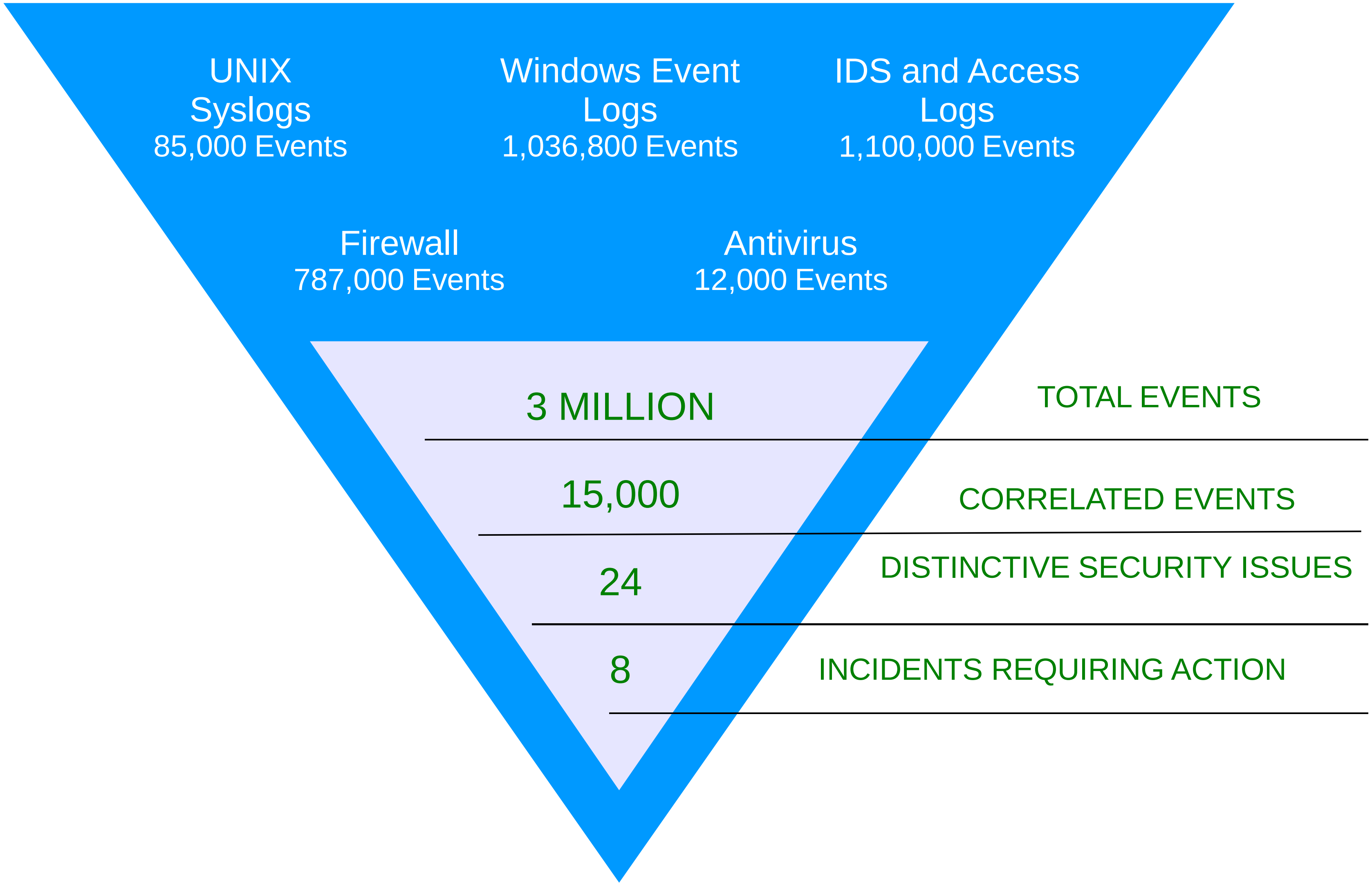
- **What Security Event Logs?**
- Audit Logs
- Transaction Logs
- Intrusion Logs
- Connection Logs
- System Performance Records
- User Activity Logs
- Misc. alerts and other messages

- **From Where?**
- Firewalls/Intrusion Prevention
- Routers/switches
- Intrusion Detection
- Servers, Desktops, Mainframes
- Business Applications
- Databases
- Anti-virus
- VPNs

The Challenge of Managing Security Information

- “Millions and Millions” of events
    - Firewalls, IDS, IPS, Anti-Virus, Databases, Operating Systems, Content filters
    - Information overload
- Lack of standards
- Difficult correlation
    - Making sense of event sequences that appear unrelated
    - False positives and validation issues
    - Heterogeneous IT environment

Inverted Pyramid of Event Significance



UNIX Syslogs
85,000 Events

Windows Event Logs
1,036,800 Events

IDS and Access Logs
1,100,000 Events

Firewall
787,000 Events

Antivirus
12,000 Events

3 MILLION — TOTAL EVENTS

15,000 — CORRELATED EVENTS

24 — DISTINCTIVE SECURITY ISSUES

8 — INCIDENTS REQUIRING ACTION

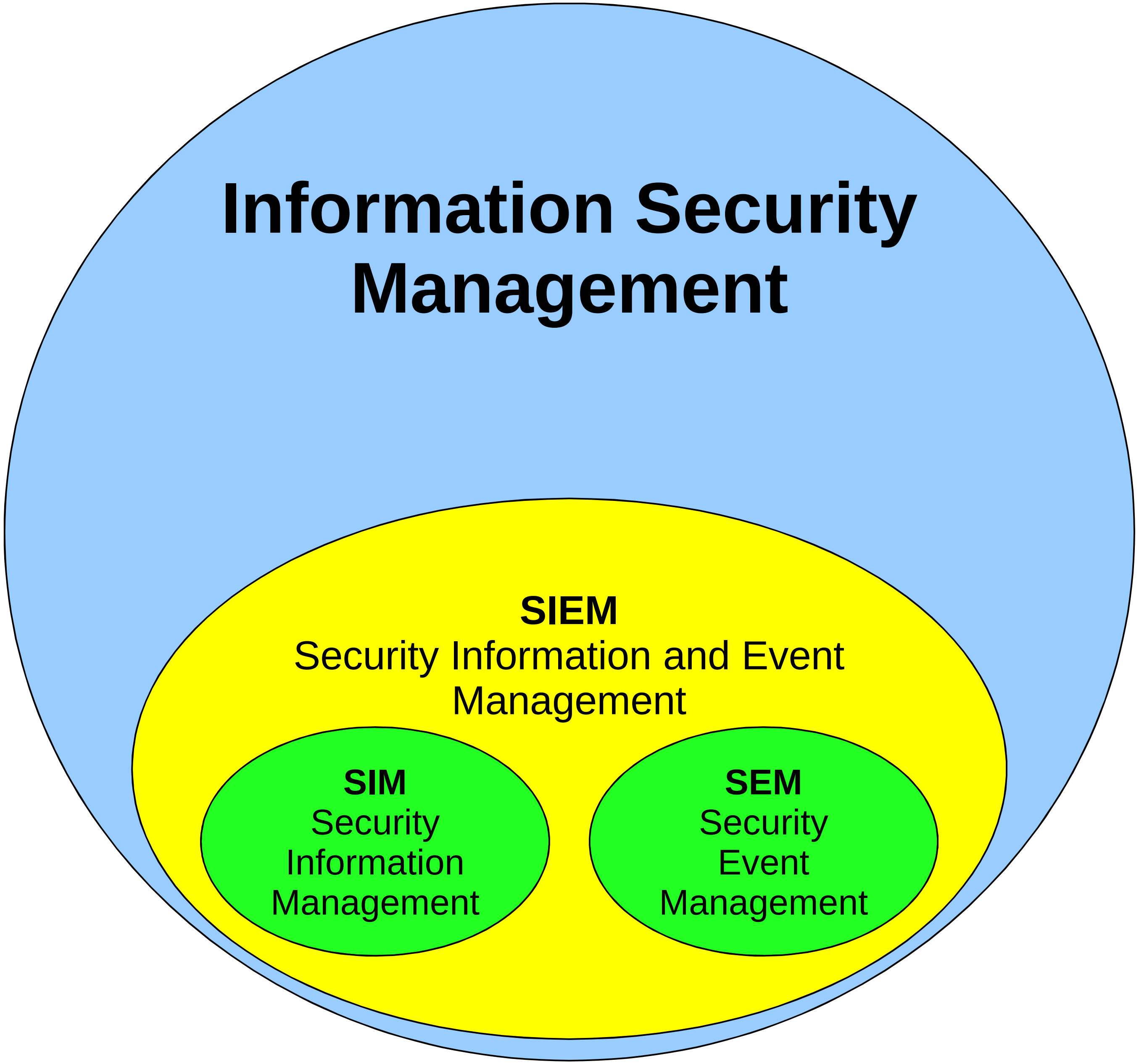
Beginnings of SIEM are in Log Management

- Log management: what to log and where to?
- Automation in collection of logs in a central place – e.g. syslog-ng: centralization of logs
- Tools for log searching and analysis: finding significant log events
- Still a dependence on expert human for analysis
  - Typical human expert cannot process more than a 1000 events a day
- Conclusion - automate more

SIEM

- "A SIEM or SIM is a computerized tool used on enterprise data networks to centralize the storage and interpretation of logs, or events, generated by other software [or hardware] running on the network"
- A new concept (About 10 Years old)
- A natural evolution of log management
- A SIEM enables organizations to achieve round-the-clock 'pro-active' security and compliance.

SIEM versus ISM



Information Security Management
SIEM
Security Information and Event Management
SIM
Security Information Management
SEM
Security Event Management

Technical Drivers of Security Information & Event Management Systems (SIEM)

React Faster!

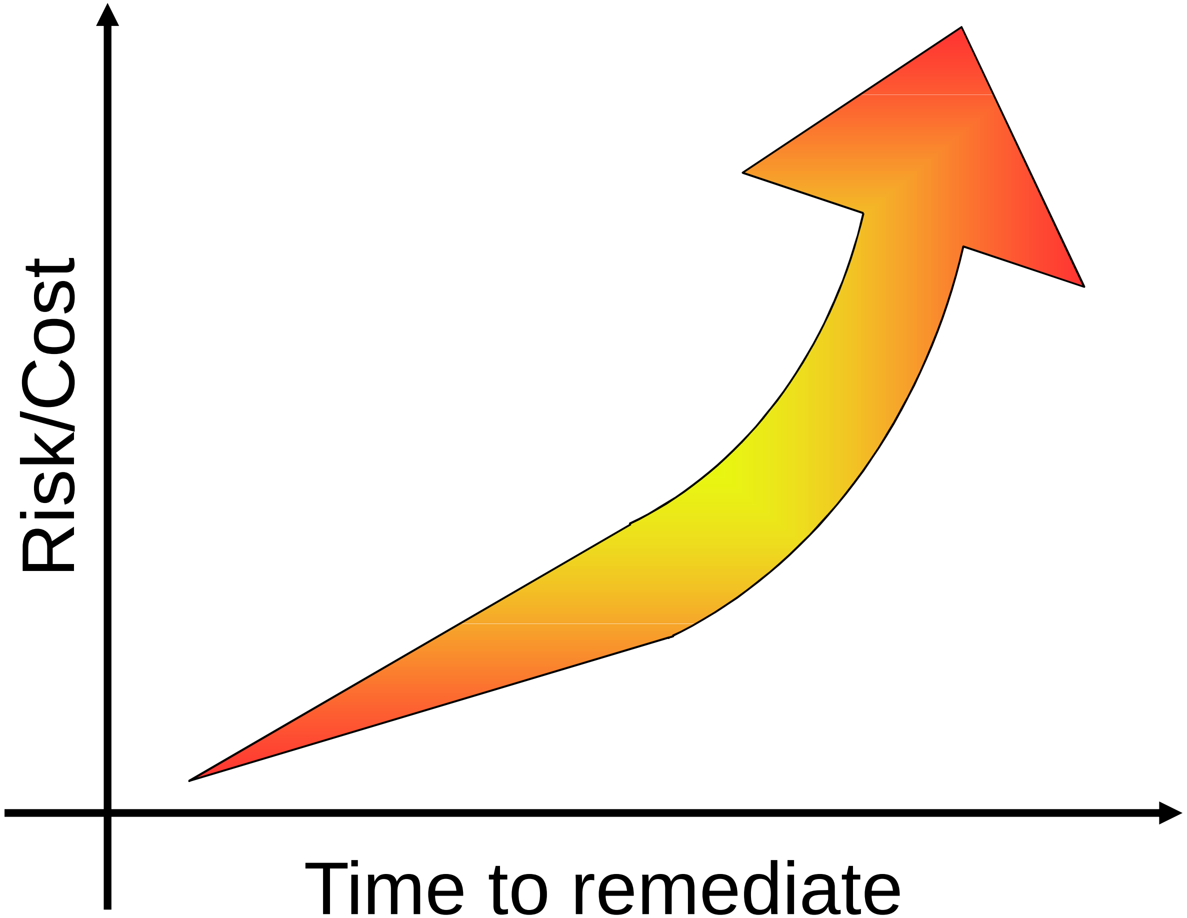
- Too much data, but not enough information
- High Signal To Noise Ratio
- No “situational awareness”
- Too many tools to isolate root cause

Improve Efficiency

- Compliance requirements
- Nothing gets shut down
- Cost center reality

Reduce risk and cost

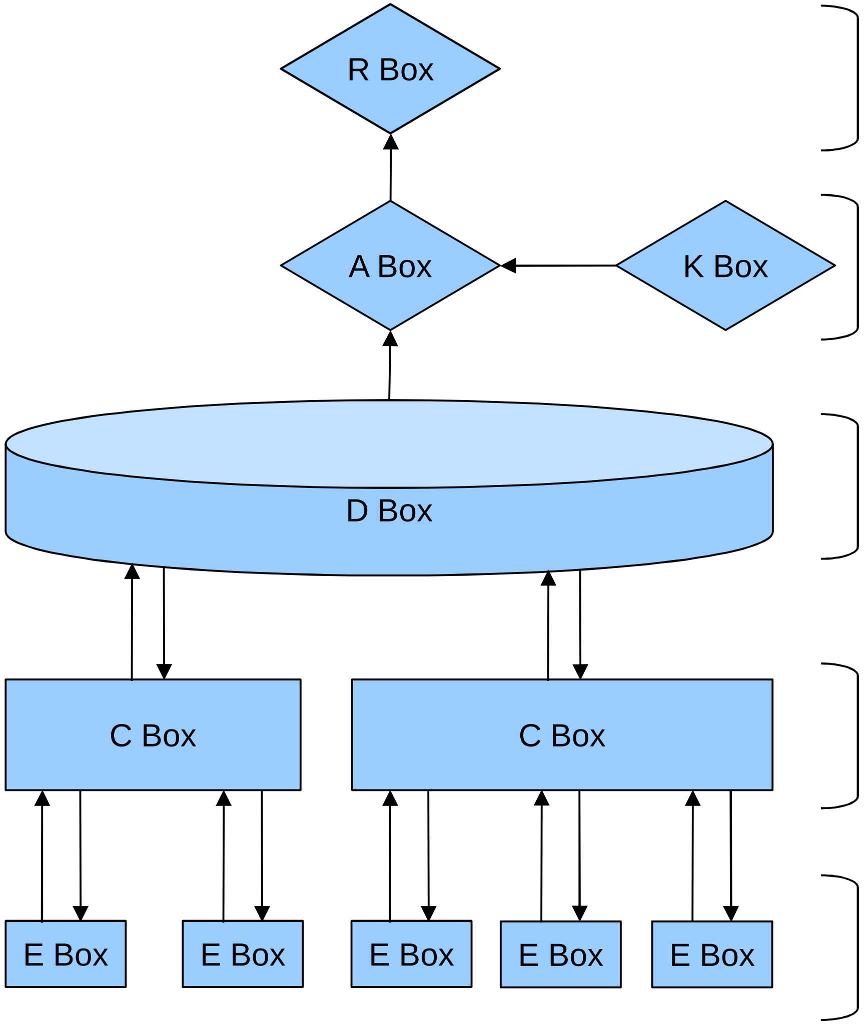
Reduce risk and cost by dramatically reducing the time it takes to effectively respond



Business Objectives of SIEM

- Increase overall security posture of an organization
- Turn chaos into order
- Aggregate log file data from disparate sources
- Create holistic security views for compliance reporting
- Identify and track causal relationships in the network in near real-time
- Build a historical forensic foundation

Generic SIEM Architecture



R Box
Reaction and reporting

A Box + **K Box**
Incident Analysis — Knowledge base

D Box
Formatted messages database

C Boxes
Collection boxes

E Boxes
Event generators: sensors & pollers

Collect
Inputs from target sources
Agent and agentless methods

Aggregate
Bring all the information to a central point

Normalize
Translate disparate syntax into a standardized one

Correlate
If A and B then C

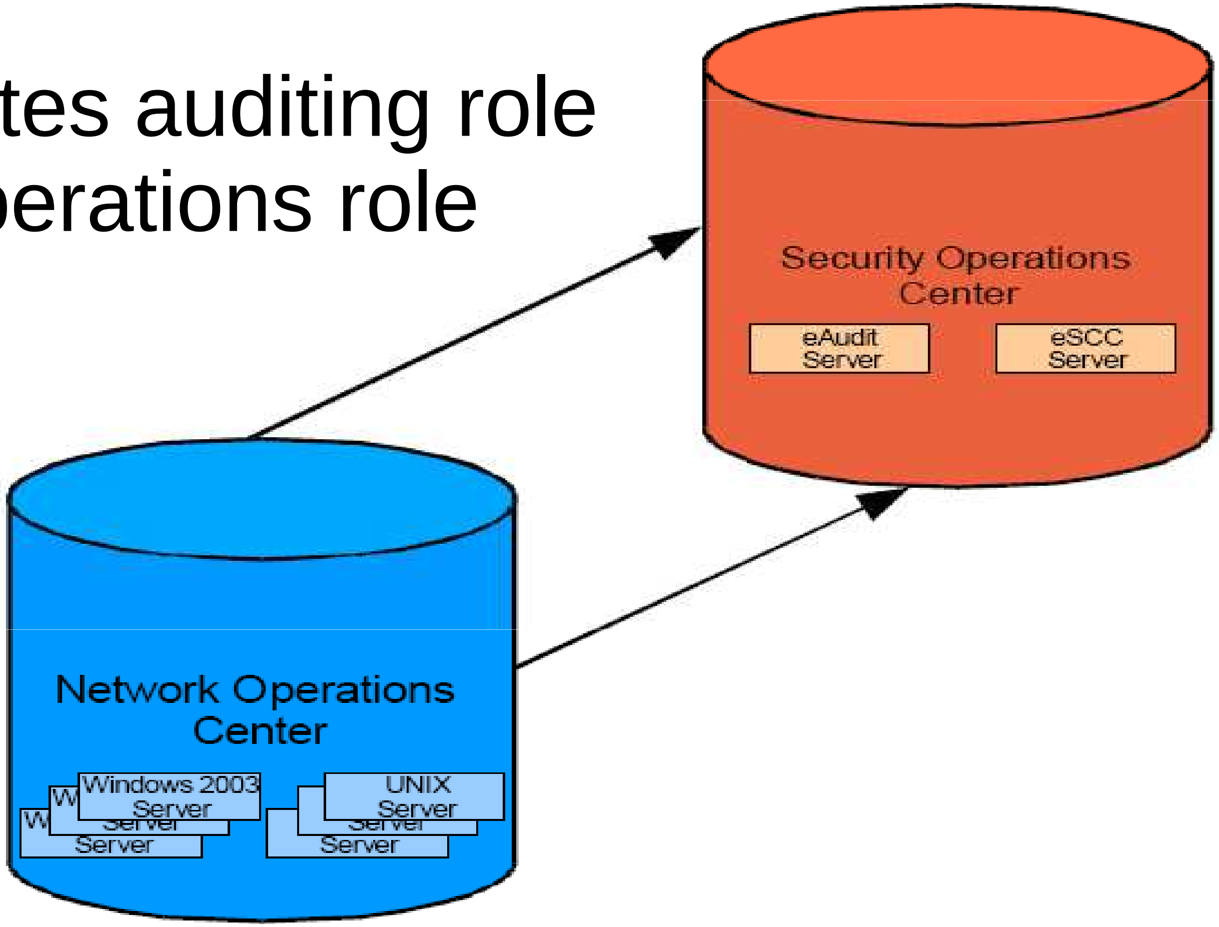
Report
State of health
Policy conformance

Archive

NOC vs SOC

IT AUDITING

Separates auditing role from operations role



IT OPERATIONS

State-of-the-art Cyber Security Operations Center, a comprehensive cyber threat detection and response center that focuses on protecting Northrop Grumman and its customers’ networks and data worldwide. (Northrop Grumman)

http://www.armybase.us/2009/07/northrop-grumman-opens-cyber-security-operations-center/

SOC BENEFITS

Reactive		Proactive	Predictive
SOC	Incident Response, Notification, Tracking, Analysis, Containment, Eradication, and Remediation	Network Vulnerability Scanning: Network, Systems	Strategic Analysis
	Incident Detection Systems (IDS)	Vulnerability Handling	Threat Management & Correlation System
	Computer Forensics & Malware Analysis	Third-Party Pen. Testing (3rd Party)	
		Email Filtering & Blocking	
		DNS Sinkhole	
		Threat Tracking, Monitoring, & Mitigation	
		Patch/Asset Management	
Situational Awareness: Log Monitoring, Event Aggregation and Correlation (SIM)			
Flow/Network Behavior Monitoring			
Host Based Monitoring System (HBSS): Antivirus, Firewall, Anti-Malware, Application White listing			
Active Protection: Intrusion Prevention System (IPS)			
		Web & Application Scanning	
Incident Scope Analysis & Remote Forensics			
Content Monitoring/Data Loss Prevention			
		Red Team/Blue Team	

Linux and Open Source

- Business model is based on services alone:
    - Implementation
    - Customizations
    - Training
    - Documentation
    - Support
- A fair and consumer friendly business model for software because:
    - Software is ***incrementally developed***
    - Software is ***infinitely replicable***

Clearing Misconceptions About Open Source

- Open source is free software !
- Software is free, *people are not* !
- Free as in “freedom” not necessarily as in “free beer”
- Open source is a viable business model
- Open source is a better software engineering methodology

“Given enough eye-balls, all bugs are shallow”

Linus' Law

Why Open Source for SIEM?

- Commercial products have a high cost of entry barrier
- User can become confused with the:
    - Marketing terms
    - Feature bloat
- Open source SIEM has matured – can compete head-on with commercial offerings
- Open Source SIEM can even be used as a learning tool – requirements analysis tool for a commercial SIEM specifications

Open Source Security Information Management - OSSIM

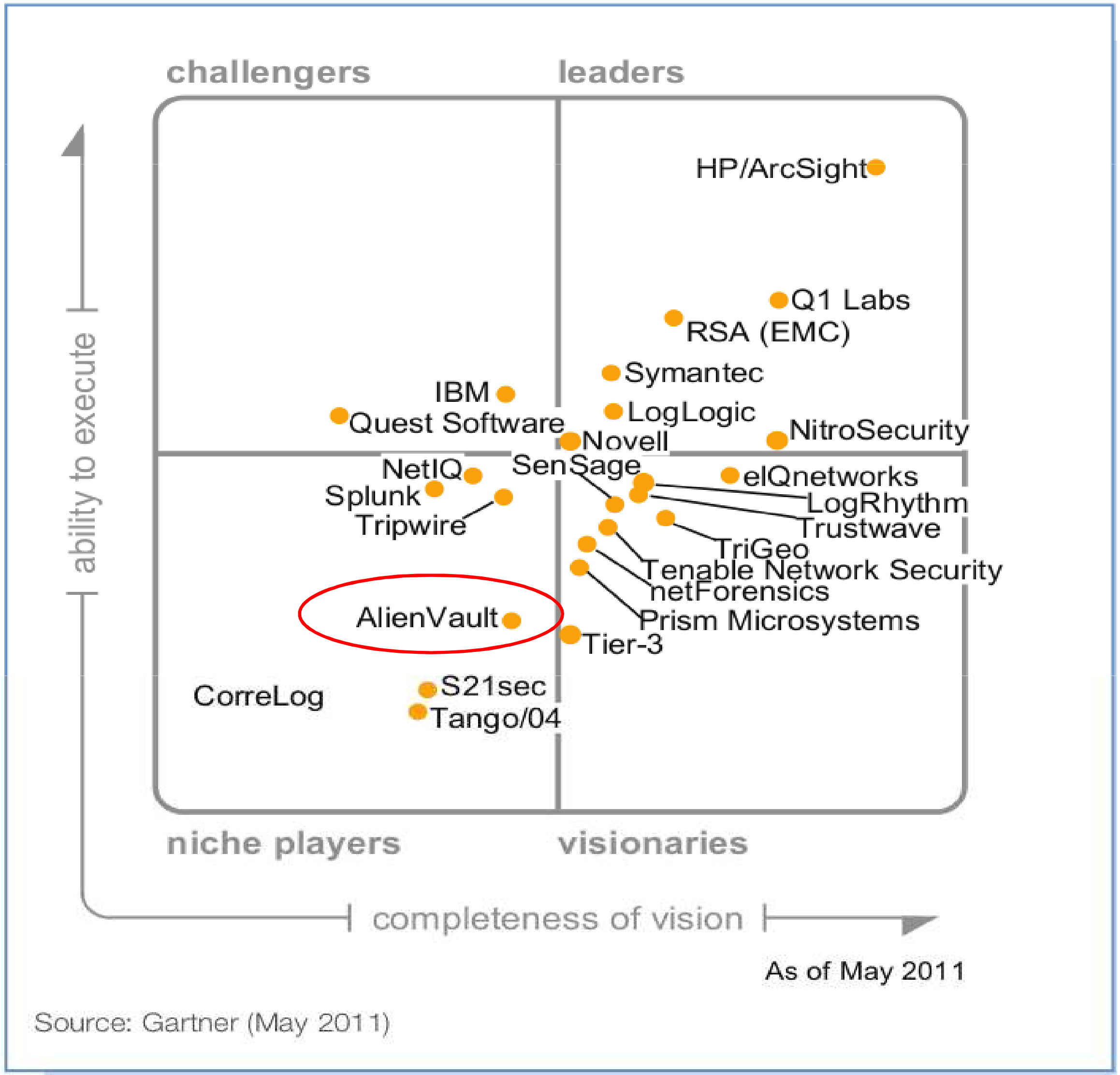
- Made of best of breed open source security tools: snort, ntop, nmap, nagios
- Full installer – plug & play
- Integrated Graphical Management Console
- Includes Reporting Engine (JasperReports) with pre-designed reports
- Commercially supported - AlienVault
- Implemented in local companies

OSSIM - Integrated Tools

- Snort
- Ntop
- Fprobe
- NFDump
- NFSen
- OCS
- Nagios

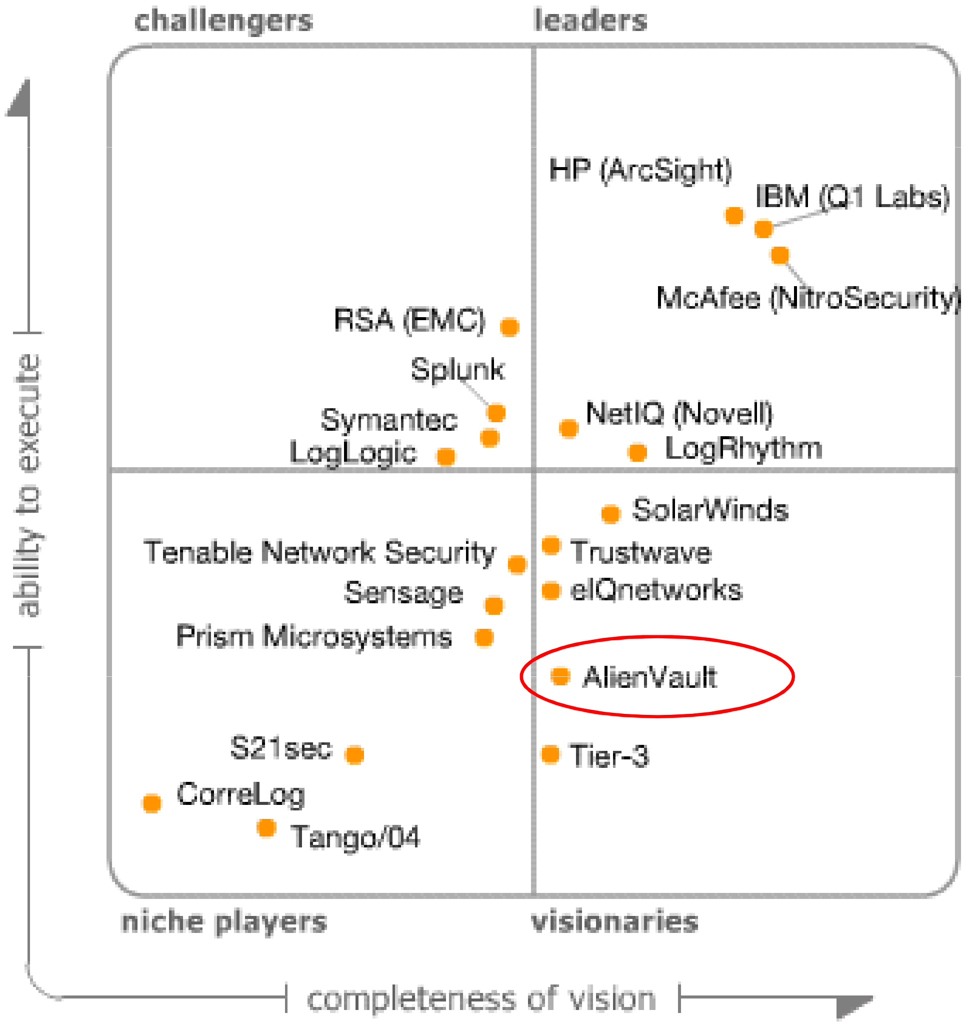
- OpenVAS
- Nikto
- OSVDB
- OSSEC
- KISMET
- NMAP
- P0f
- ArpWatch

Magic Quadrant for Security Information and Event Management - 2011



Source: Gartner (May 2011)

Magic Quadrant for Security Information and Event Management - 2012



Source: Gartner (May 2012)

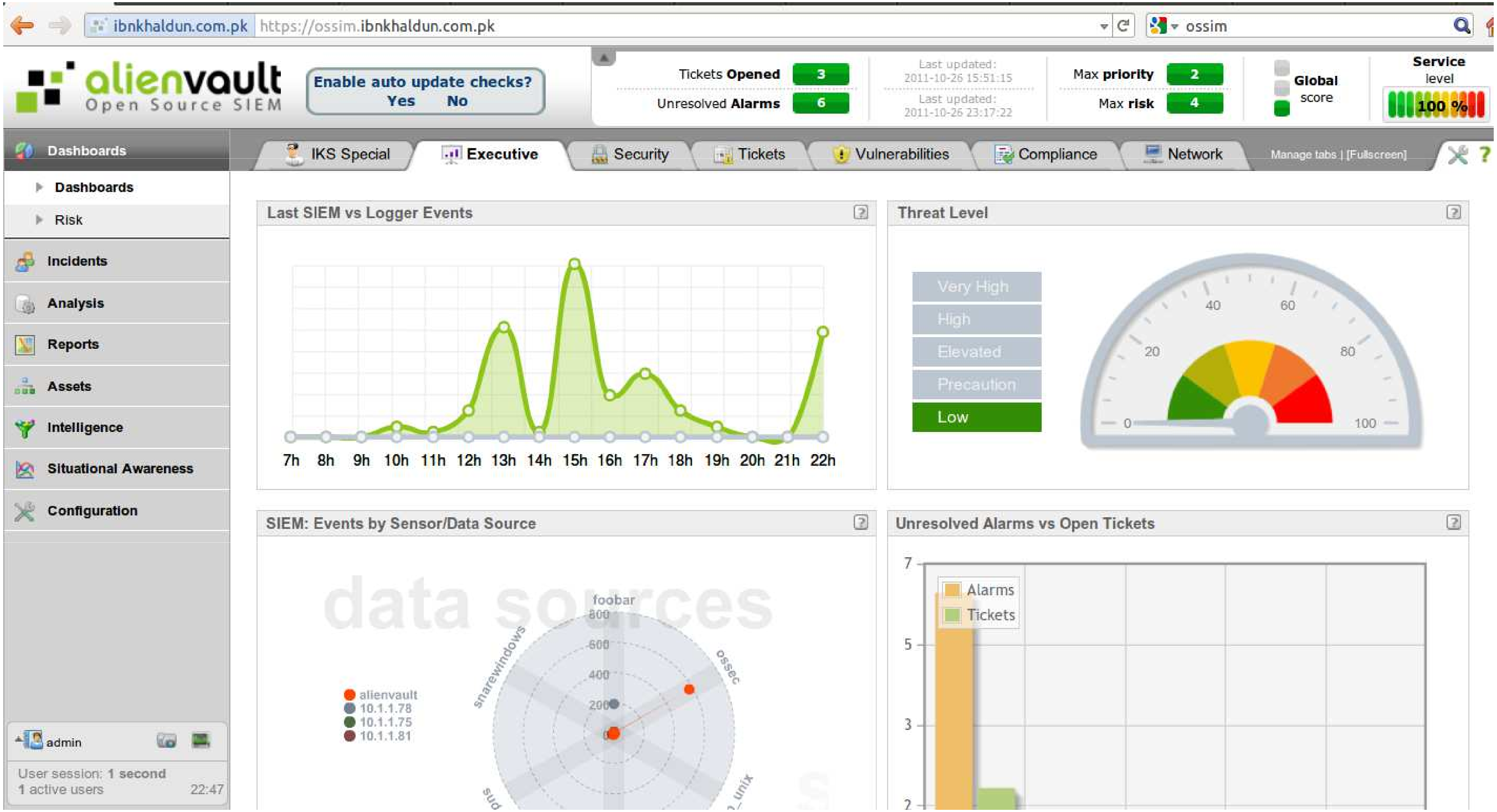
As of May 2012

OSSIM / AlienVault moving up the ladder

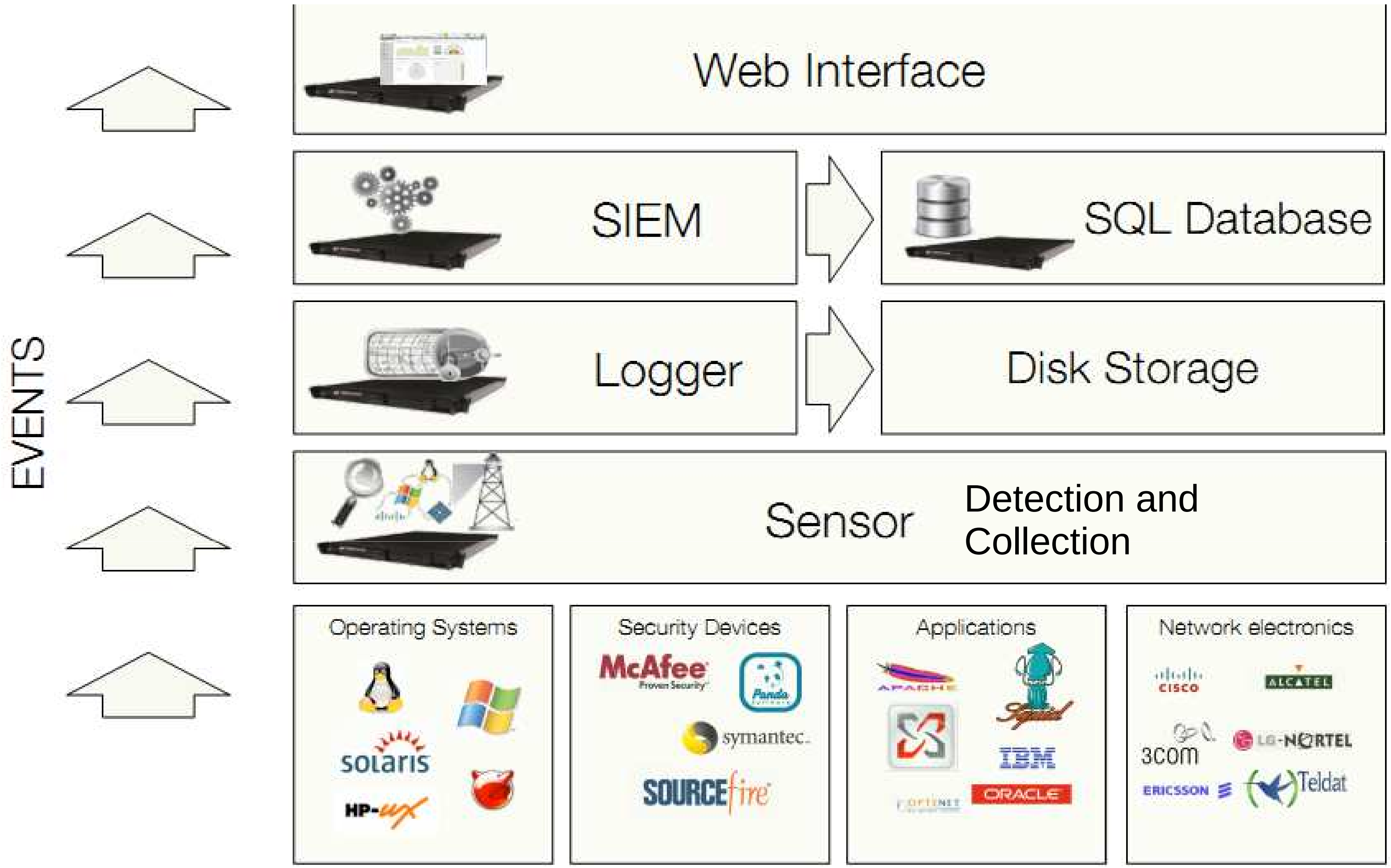
OSSIM Pros

- Extendable
- Stable – getting more mature with time
- Low cost
- Works with native tools and mechanisms
    - Easier to integrate
    - Less overhead
- Wide range of tools combined into one solution
- Based on Debian Linux (well known stable platform)

OSSIM Web Interface



OSSIM Concepts



EVENTS

Web Interface

SIEM

SQL Database

Logger

Disk Storage

Sensor

Detection and Collection

Operating Systems

Security Devices

Applications

Network electronics

Sensors: Data Sources

- **Data Source**
  - Any application or device that generates events within the network that is being monitored

External Data Sources

- □ Network Devices: Routers, Switches, Wireless AP...
- □ Servers: Domain Controller, Email server, LDAP...
- □ Applications: Web Servers, Databases, Proxy...
- □ Operating Systems: Linux, Windows, Solaris...

Collectors

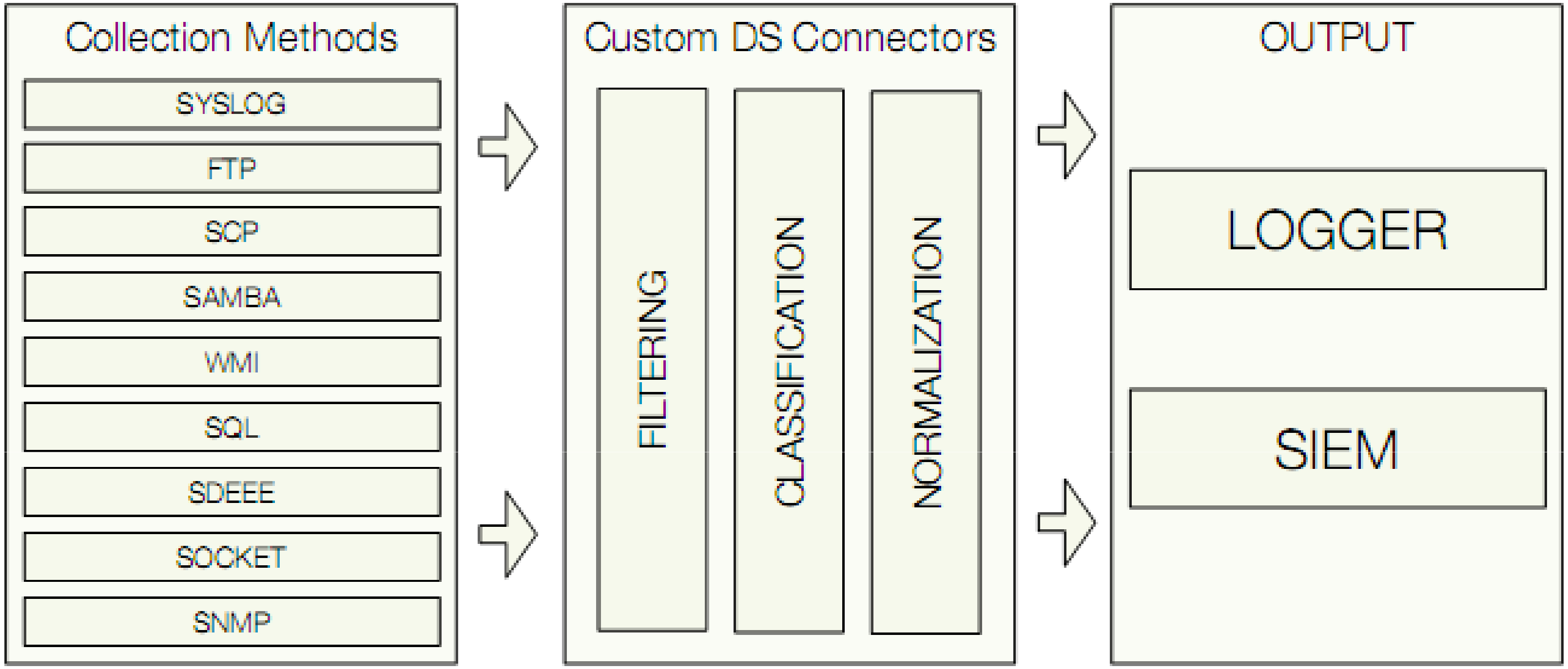
Internal Data Sources

- Collect information on the network level
- □ Intrusion Detection
- □ Vulnerability Detection
- □ Anomaly Detection
- □ Discovery, Learning & Network Profiling
- □ Inventory Systems

Detectors

Sensor: Collection

- The Sensor can aggregate events using multiple collection methods



Sensor: Detection

- Detection is done by setting the Sensors NIC into promiscuous mode to collect all the traffic on the monitored network
  - HUB
  - Port Mirroring/Spanning
  - Network Tap

OpenVAS
SNORT
KISMET
ntop
Nagios
OSSEC

Event

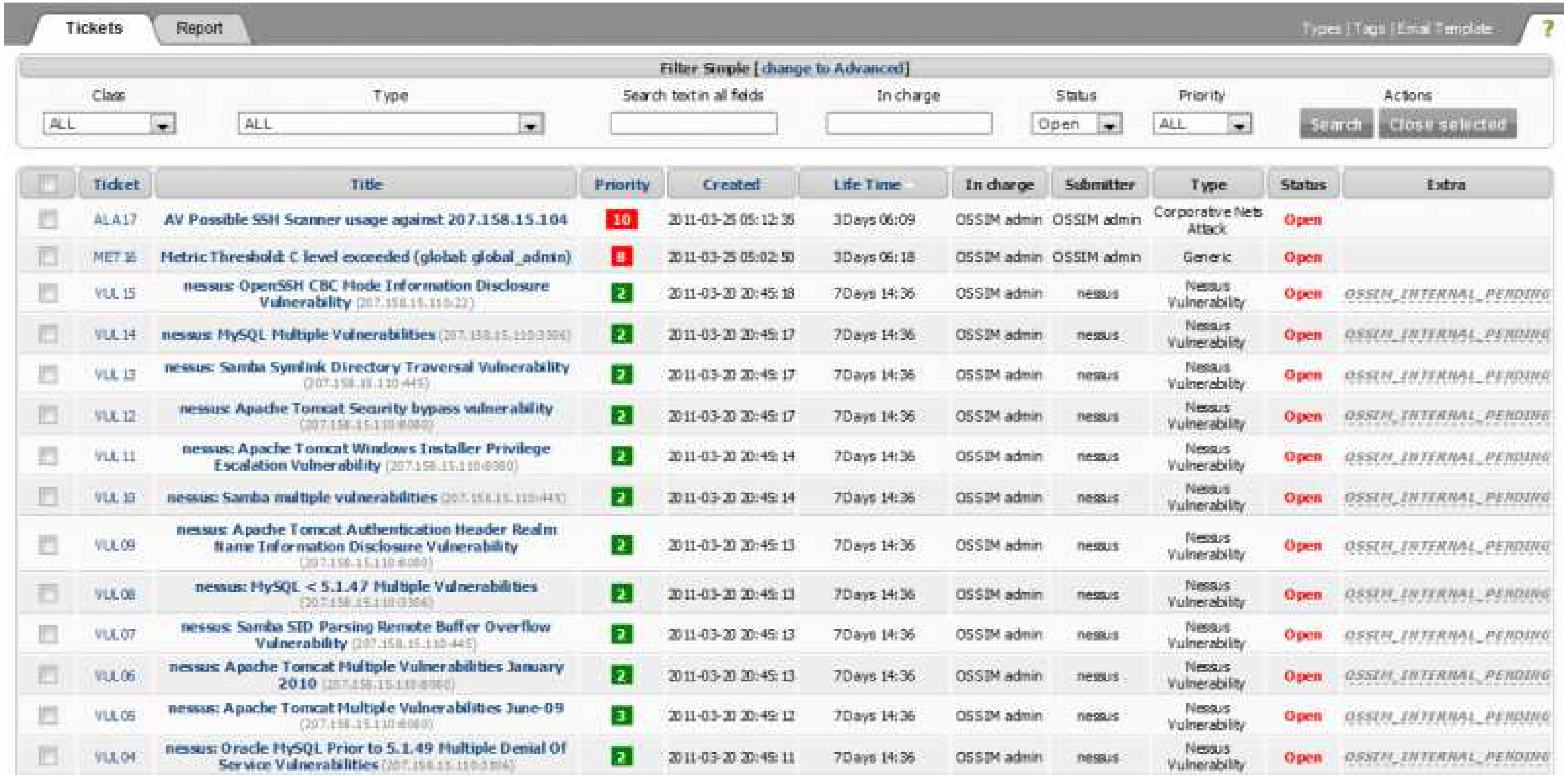
- Any log entry generated by any Data Source at application, system or network level will be called an event.

- For SIEM it is important to know:
  - When has the event been generated?
  - What is involved? (Systems, users, …)
  - Which application generated the event?
  - What’s the event type?

The SIEM

- The SIEM component provides the system with Security Intelligence and Data Mining capacities, featuring:
  - Real-time Event processing
  - Risk metrics
  - Risk assessment
  - Correlation
  - Policies Management
  - Active Response
  - Incident Management
  - Reporting

Security Event Management



Filter Simple [change to Advanced]

Class	Type	Search text in all fields	In charge	Status	Priority	Actions
ALL	ALL			Open	ALL	Search Close selected

☐	Ticket	Title	Priority	Created	Life Time	In charge	Submitter	Type	Status	Extra
☐	ALA17	AV Possible SSH Scanner usage against 207.158.15.104	10	2011-03-25 05:12:35	3Days 06:09	OSSIM admin	OSSIM admin	Corporative Nets Attack	Open	
☐	MET16	Metric Threshold: C level exceeded (global: global_admin)	8	2011-03-25 05:02:50	3Days 06:18	OSSIM admin	OSSIM admin	Generic	Open	
☐	VUL15	nessus: OpenSSH CBC Mode Information Disclosure Vulnerability (207.158.15.110:22)	2	2011-03-20 20:45:18	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL14	nessus: MySQL Multiple Vulnerabilities (207.158.15.110:3306)	2	2011-03-20 20:45:17	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL13	nessus: Samba Symlink Directory Traversal Vulnerability (207.158.15.110:445)	2	2011-03-20 20:45:17	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL12	nessus: Apache Tomcat Security bypass vulnerability (207.158.15.110:8080)	2	2011-03-20 20:45:17	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL11	nessus: Apache Tomcat Windows Installer Privilege Escalation Vulnerability (207.158.15.110:8080)	2	2011-03-20 20:45:14	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL10	nessus: Samba multiple vulnerabilities (207.158.15.110:445)	2	2011-03-20 20:45:14	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL09	nessus: Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability (207.158.15.110:8080)	2	2011-03-20 20:45:13	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL08	nessus: MySQL < 5.1.47 Multiple Vulnerabilities (207.158.15.110:3306)	2	2011-03-20 20:45:13	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL07	nessus: Samba SID Parsing Remote Buffer Overflow Vulnerability (207.158.15.110:445)	2	2011-03-20 20:45:13	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL06	nessus: Apache Tomcat Multiple Vulnerabilities January 2010 (207.158.15.110:8080)	2	2011-03-20 20:45:13	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL05	nessus: Apache Tomcat Multiple Vulnerabilities June-09 (207.158.15.110:8080)	3	2011-03-20 20:45:12	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING
☐	VUL04	nessus: Oracle MySQL Prior to 5.1.49 Multiple Denial Of Service Vulnerabilities (207.158.15.110:3306)	2	2011-03-20 20:45:11	7Days 14:36	OSSIM admin	nessus	Nessus Vulnerability	Open	OSSIM_INTERNAL_PENDING

Conclusions

- OSSIM provides SIEM capabilities to small and medium sized organizations
- OSSIM leverages best of breed open source tools and combines them into integrated SIEM to manage security events
- OSSIM can be setup quickly – time is money

Thank You !