Deloitte.

SIEM Implementation Approach Discussion

April 2012

Audit . Tax . Consulting . Financial Advisory.

Agenda

- ❑ What are we trying to solve?
- ❑ Summary Observations from the Security Assessments related to Logging & Monitoring
- ❑ Problem Statement
- ❑ Solution – Conceptual Level
- ❑ Insourcing versus Outsourcing
- ❑ Vendors
- ❑ Implementation Considerations

What are we trying to solve?

Summary Observations from the Security Assessments related to Logging & Monitoring

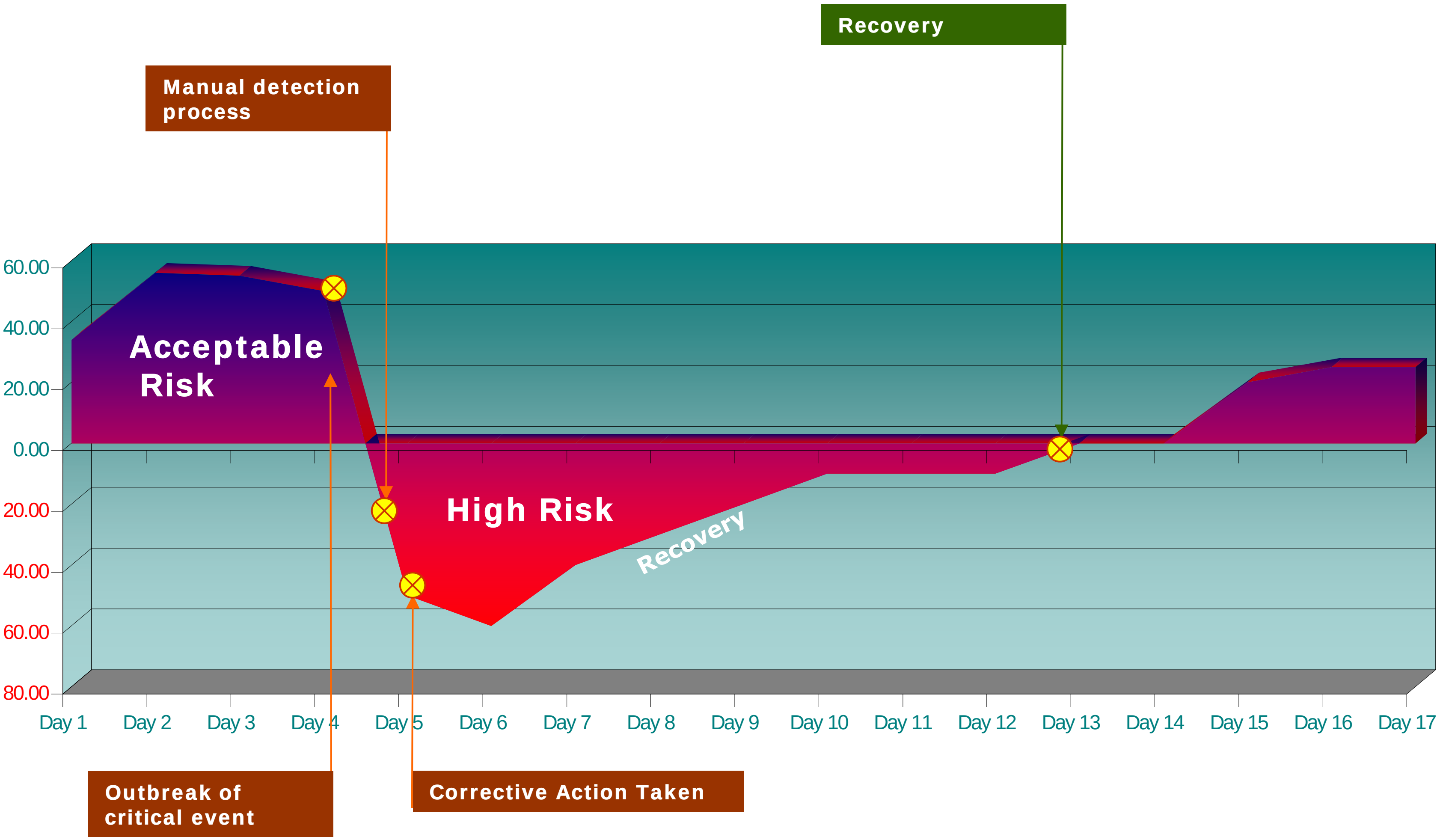
- Inconsistent logging of security events (servers, databases, network devices, security devices, etc.)
- No logging standard
- Monitoring of logs ranged from non-existent to limited
- Correlation capability of security events was mostly non-existent (for identifying threats timely)
- Log retention was not consistent
- Limited monitoring for sensitive data leakage via network
- Limited monitoring for change in system configurations (security related)

Problem Statement

- Institutions may not detect security incidents (e.g., unauthorized access to sensitive repositories, changes in security configurations to critical systems, sensitive data leakage, etc.) on a timely basis (or at all).

- While this can be applied broadly, the focus of the observations was related to infrastructure (network, operating systems, and databases) – perimeter devices, security devices, as well as select internal servers.

Typical Scenario



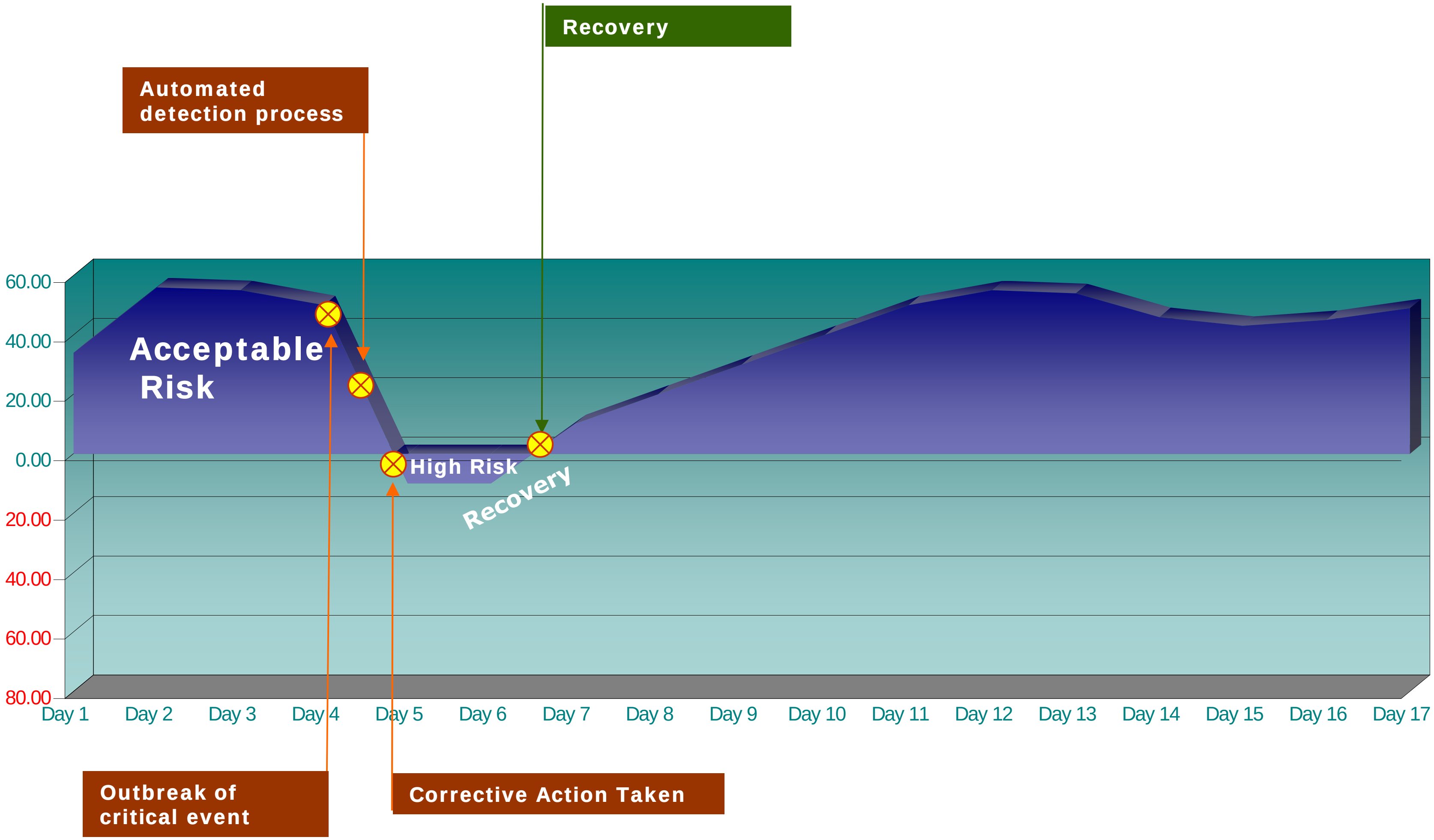
Recovery

Manual detection process

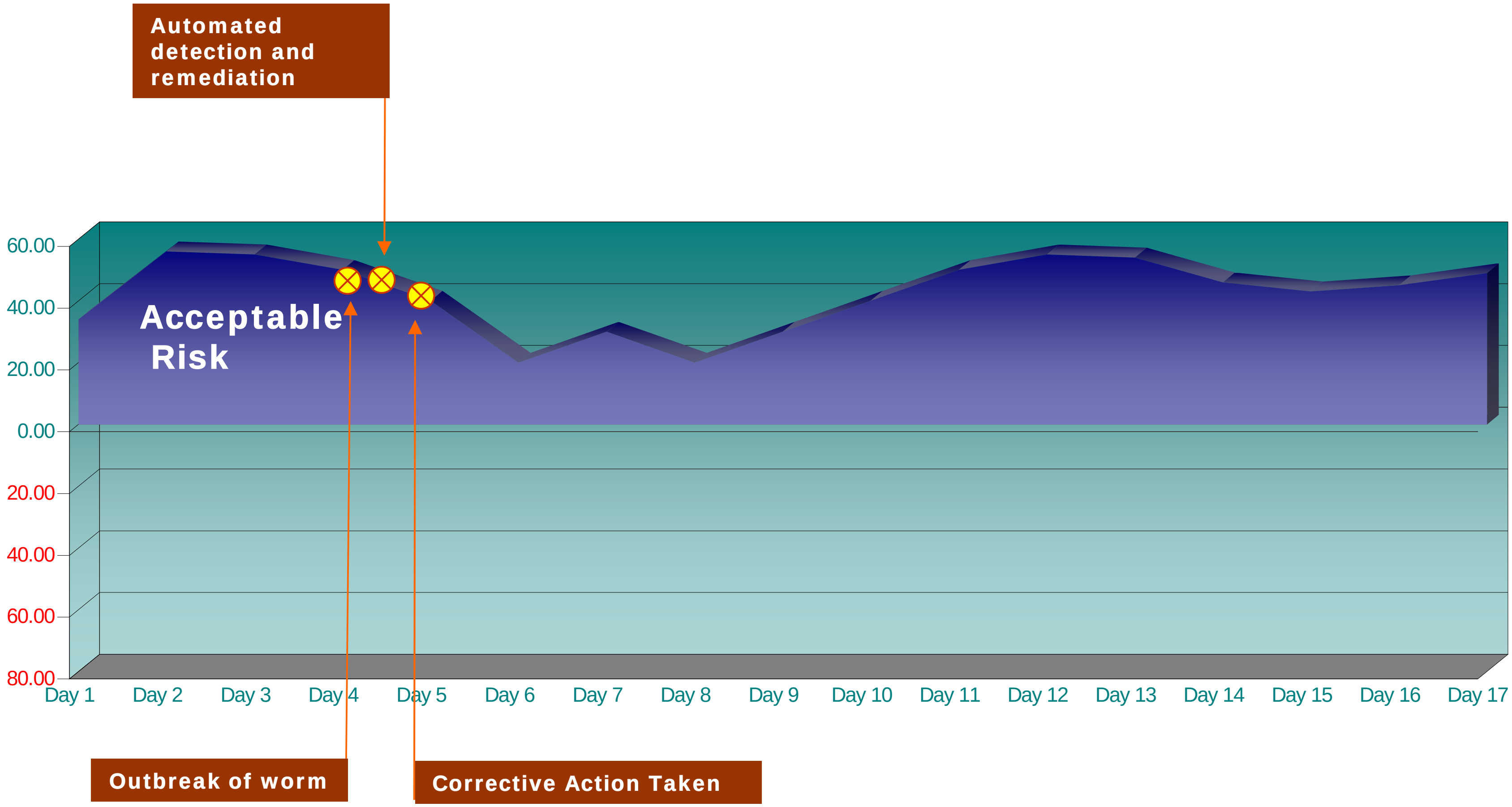
Outbreak of critical event

Corrective Action Taken

Organizations With SEIM



Organizations With SEIM and Active Threat Management/Effective Incident Escalation



Automated detection and remediation

Outbreak of worm

Corrective Action Taken

SEIM Addressing of Organizational Challenges

Challenges addressed by LMR	Risk Containment	Operational Cost	Compliance
Lack of visibility from external threats (Intrusion Detection)	●●●●●	●○○○○	●●●●●
Lack of visibility from internal threats (Extrusion Detection)	●●●●●	●○○○○	●●●●●
Limited visibility of misappropriation and mis-use	●●●●●	●○○○○	●●●●●
Inability to effectively enforce and monitor security controls	●●●●●	●●●●●	●●●●●
High loss of revenue due to virus and worm outbreaks	●●●●●	●●●●●	●●●○○
Disabling or limitation of audit controls due to information overload	●●●●○	●●●○○	●●●●○
Inability to correlate events from disparate sources	●●●●○	●●●●○	●●●●○
High operational cost to monitor security events	●○○○○	●●●●●	●○○○○
High exposure window due to the time to react	●●●●●	●●●●○	●●●●○
Too much technology making monitoring (operationally) cost prohibitive	●●●●○	●●●●○	●●●●○
Inability to effectively demonstrate security compliance	●○○○○	●●●●●	●●●●○

Conceptual Solution

Solution – Conceptual Level

- Develop a Logging & Monitoring Strategy
  - Develop logging standard aligned with regulatory and business needs
  - Align / provision logging on devices based on logging standard (careful on DB!)
  - Perform analysis on requirements, options (in-house versus MSSP, SOC approach), and sustainment considerations for implementing log management and monitoring processes
  - Procure tool (and/or services) and resources for managing and monitoring logs (SIEM, DLP - network, FIM)
  - Design Use Cases for monitoring
  - Implementation strategy (phases, tuning, etc.)

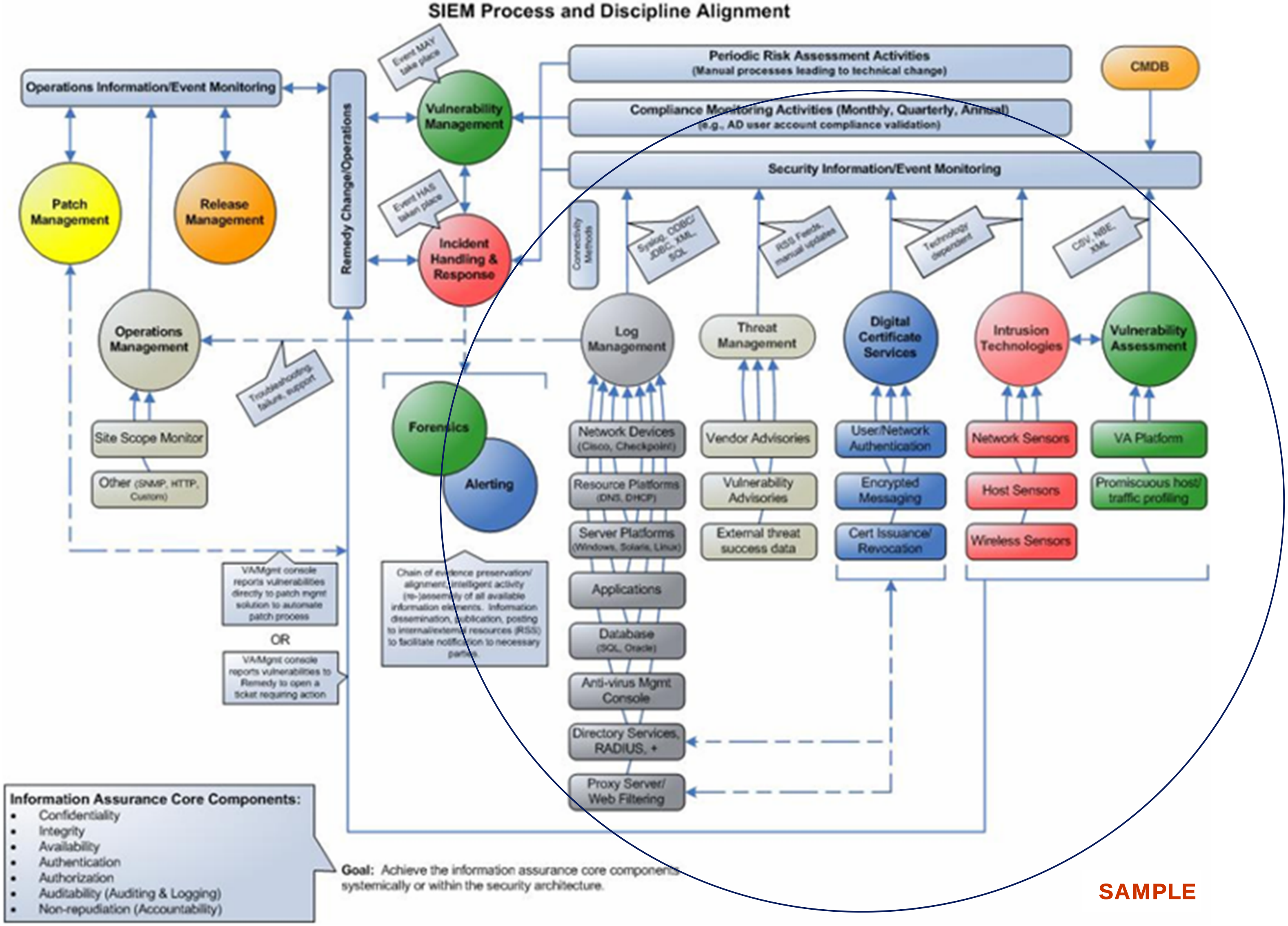
Microsoft
werPoint Presentat

Detective Controls (Sample for illustration purposes)

Higher business value

	Infrastructure Threats	Outbreak Threats	Mis-use of privilege	Insider Threat	Data Leakage	Advanced Persistent Threats	Industry Channel Threats	Fraud and Misappropriation
Business Applications								
Web Application Gateway								
APT feed								
CTI feed								
Cyber-beacon feed								
DLP					Emerging Threats – High Business Impact			
Vulnerability data								
Identity Management								
Database / DAM etc.								
File and Print								
Authentication Servers (Radius, TACACS+, AD etc.)								
IDS / IPS / WAF / NAC								
Content Management (AV, Malware Detection, URL etc.)								
Network Behavioral Analysis				Current Threats – Structured Controls				
FW / VPN								
OS logs								
Core Switches								
Distribution Switches								
Access Level Switches		Infrastructure Threats – Good Controls Typically Exist						

SEIM as Part of an Organizational Security Architecture (Typical)


SIEM Process and Discipline Alignment
Periodic Risk Assessment Activities
(Manual processes leading to technical change)
CMDB
Compliance Monitoring Activities (Monthly, Quarterly, Annual)
(e.g., AD user account compliance validation)
Security Information/Event Monitoring
Operations Information/Event Monitoring
Remedy Change/Operations
Event MAY take place
Vulnerability Management
Event HAS taken place
Incident Handling & Response
Patch Management
Release Management
Operations Management
Troubleshooting, failure, support
Site Scope Monitor
Other (SNMP, HTTP, Custom)
Connectivity Methods
Syslog, ODBC/ JDBC, XML, SQL
RSS Feeds, manual updates
Technology dependent
CSV, NBE, XML
Log Management
Threat Management
Digital Certificate Services
Intrusion Technologies
Vulnerability Assessment
Forensics
Alerting
Network Devices (Cisco, Checkpoint)
Resource Platforms (DNS, DHCP)
Server Platforms (Windows, Solaris, Linux)
Applications
Database (SQL, Oracle)
Anti-virus Mgmt Console
Directory Services, RADIUS, +
Proxy Server/ Web Filtering
Vendor Advisories
Vulnerability Advisories
External threat success data
User/Network Authentication
Encrypted Messaging
Cert Issuance/ Revocation
Network Sensors
Host Sensors
Wireless Sensors
VA Platform
Promiscuous host/ traffic profiling
OR

VA/Mgmt console reports vulnerabilities directly to patch mgmt solution to automate patch process

OR

VA/Mgmt console reports vulnerabilities to Remedy to open a ticket requiring action

Chain of evidence preservation/ alignment, intelligent activity (re-)assembly of all available information elements. Information dissemination, publication, posting to internal/external resources (RSS) to facilitate notification to necessary parties.

Information Assurance Core Components:

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Auditability (Auditing & Logging)
- Non-repudiation (Accountability)

Goal: Achieve the information assurance core components systemically or within the security architecture.

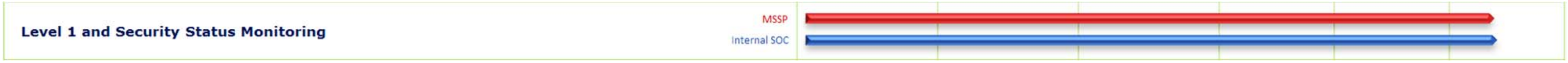
SAMPLE

Insourcing versus Outsourcing

Comparison of an in versus outsourced solution

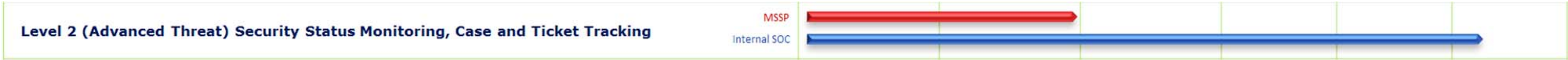
Level 1 and Security Status Monitoring

MSSP’s can often provide repeatable and highly effective services for level 1 (traditional) security threats. This includes traditional security monitoring of common threats that are faced by other organizations.



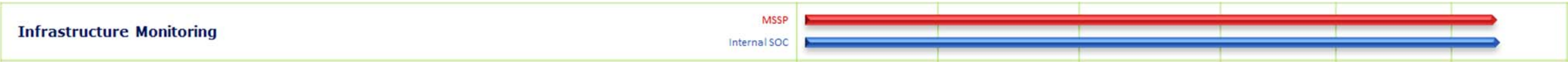
Level 2 (Advanced Threat)

The MSSP is generally dependent on the organization for advanced threat monitoring (e.g., emerging threats that are not defined in the SLA), coordination with internal application owners, case and ticket tracking, etc. Most MSSP operate under a model of monitor, detect, escalate and handoff. MSSP’s define a maximum number of complementary use cases that will be integrated into the SOC, per year. Additional use cases may affect the financial impact of operating the SOC over time.



Infrastructure Monitoring

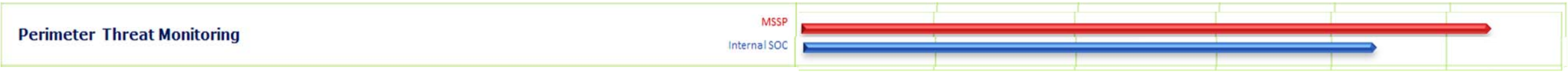
MSSP’s can monitor against organization’s defined use cases for Infrastructure Monitoring. However the logic around the dynamic nature of the infrastructure requires specific (client specific) familiarity and assimilation into the fabric of the organization. For example, new initiatives that results in increased firewall activity. A process workflow can be created to notify MSSP’s of these activities, but usually there is a threshold of how often these notifications occurs and typically do not include smaller changes.



Comparison of an in versus outsourced solution

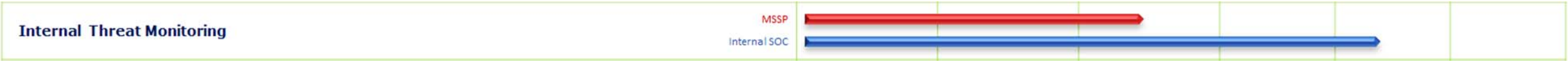
Perimeter Threat Monitoring

MSSP's generally have repeatable and optimized processes around perimeter threat monitoring. Given the fact that MSSP's work with other like organizations, MSSP's can distinguish between a general Internet threat and a more focused organizational specific threat.



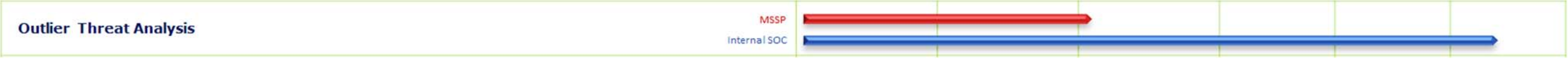
Internal Threat Monitoring

Internal (Insider) Threat Monitoring requires detailed understanding of the Lines of Business, expected behavior and a good appreciation for the organization's specific operational and business model, including the tendency for "expected behavior" to change over time.



Outlier Threat Analysis

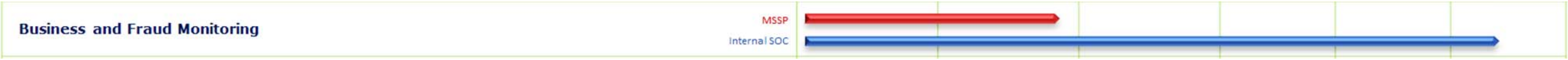
Similar to Internal Threat Monitoring, Outlier Threat Analysis is the evaluation of threats against an organization's baseline. However the baseline at client may change based on various factors and therefore an internal SOC is better geared to evaluate against outlier and statistical models.



Comparison of an in versus outsourced solution

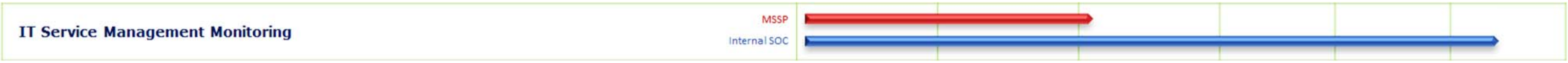
Business and Fraud Monitoring

Most MSSP have good capability on traditional security monitoring, but have limited capability against client focused business and fraud monitoring. The reason being that MSSP's are designed and operate on a scalable platform to service a large subset of clients. However Business and Fraud patterns differ from organization by organization.



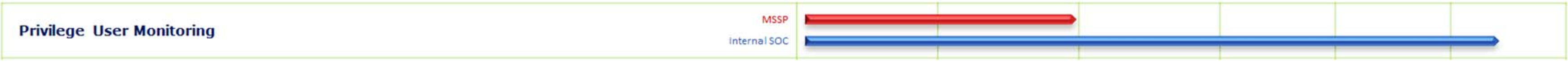
IT Service Management Security Monitoring

A key part of security monitoring is reconciling security events against ITIL based services. For example, comparing configuration changes against approved changes (or releases). Most MSSP's support the export of cases (or incidents) into a ticketing system, but usually do not have the ability to receive changes to CI's (Configuration Item's) related to an approved change, especially from the diverse ticketing processes. An insource SOC can build a process to either receive information on approved changes, automate CI's on assets related to a change or be able to interface with the change initiator to validate change approval.



Privilege User Monitoring

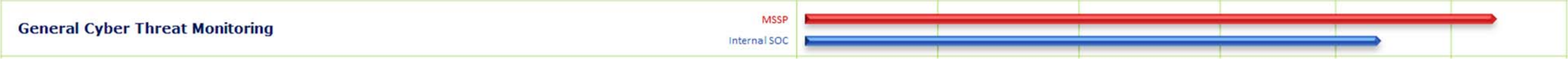
Similar to IT Service Management Monitoring, MSSP's can monitor based on client use cases, but are unable to fully reconcile use of privilege out of role (or duty). An internal SOC can build Identity Provisioning input into the SOC to evaluate security events against role, segregation of duty and other factors.



Comparison of an in versus outsourced solution

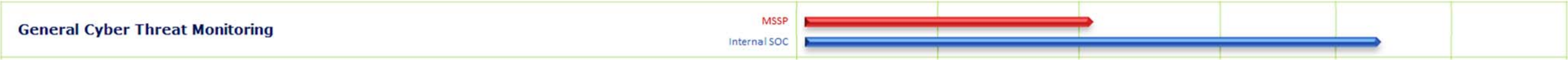
General Cyber Threat Monitoring

MSSP's have threat vectors for general cyber threats, should they have other like monitored organizations. Therefore they theoretically can provide repeatable capability against general cyber threats.



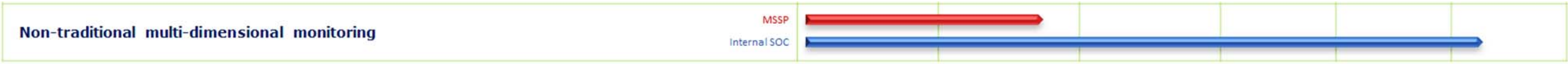
Brand Protection and Cyber Beacon Monitoring

Most of the threats nowadays originate or can be depicted through an organizations "Cyber Beacon" . Cyber Beacon is how an Organization is viewed in cyber space, including data points from a Web 2.0 perspective. Most innovative organizations are starting to pre-empt threats by obtaining advanced knowledge from Cyber Threat Intelligence from these sources. This includes how the brand or association with the brand is used and the threats posed by Spammer, Phishers, etc. Unless provided as a supplementary service (not part of the core offering) most MSSP's do not have the ability to perform brand and cyber beacon monitoring. However this can be built within the people, process and technology of an insourced SOC.



Non-traditional multi-dimensional threat monitoring

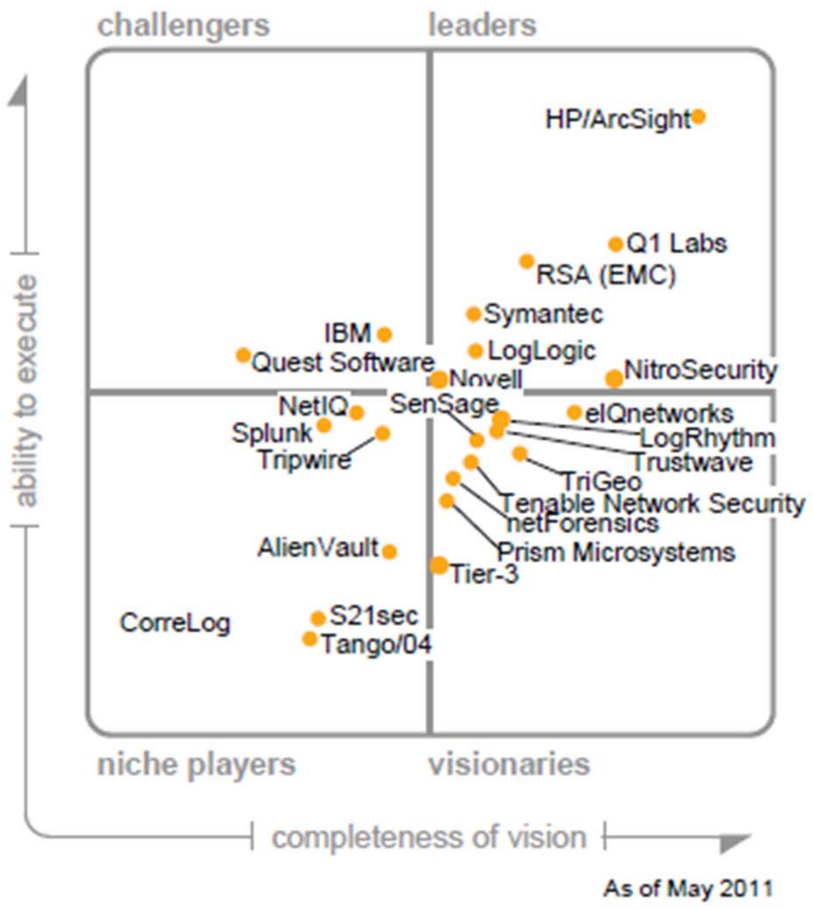
As organizations expand the foot print of Security Status monitoring, the organization may consider non-traditional security monitoring. For example Physical Security and the like. Most MSSP's that monitor for logical threats are usually not tooled (people, process and technology) to address these non-traditional devices.



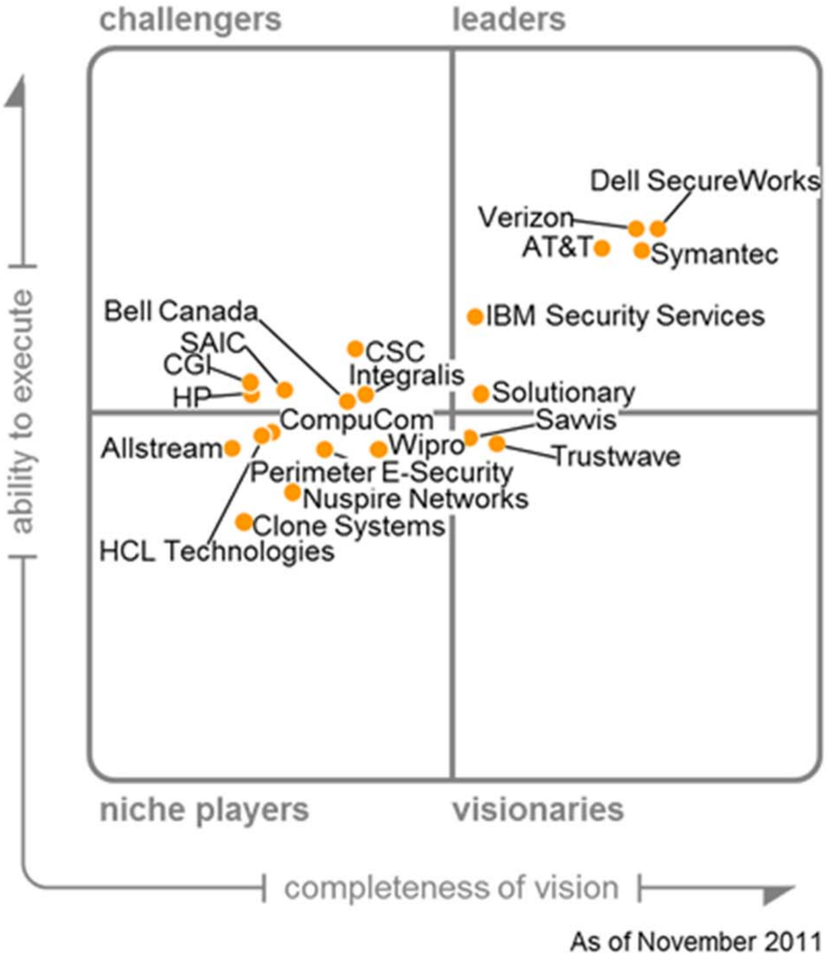
Vendors

SIEM and MSSP Vendors

Magic Quadrant for Security Information and Event Management



Source: Gartner (May 2011)

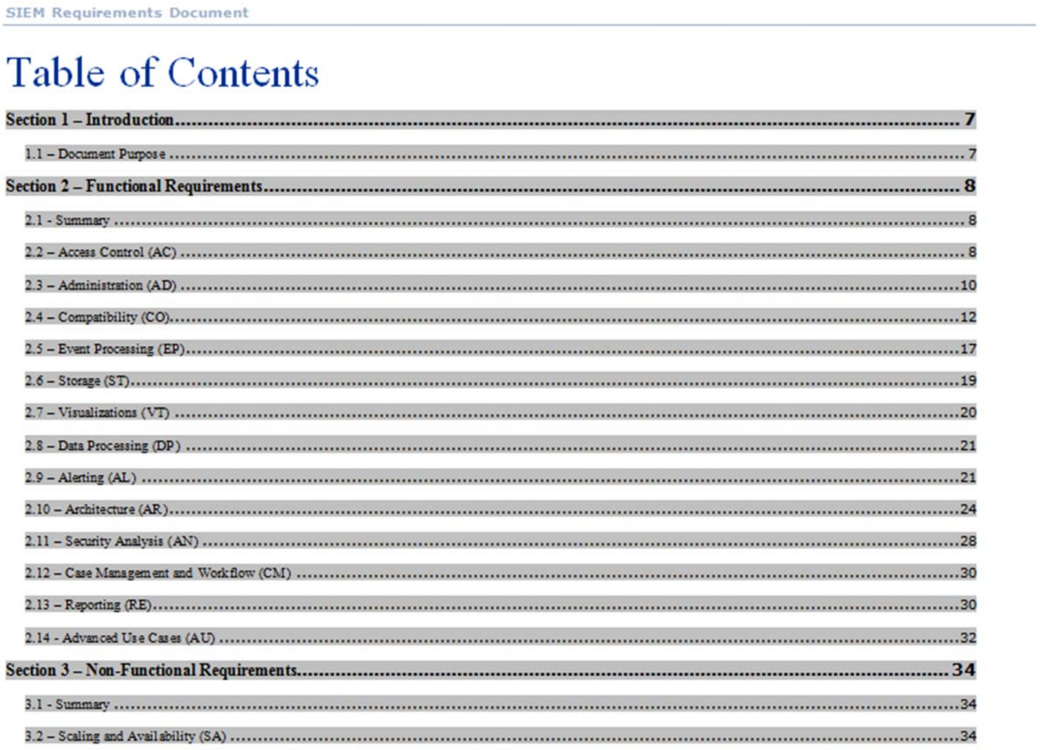


(From "Managed Security Services Providers," North America 2011)

Implementation Considerations

Implementation Considerations

- Decide on Sourcing Strategy (in-house versus MSSP)
- Identify what data sources will you need to monitor in order to detect potential security incidents => may lead to identification of additional tools needs (e.g., network DLP, FIM, etc.) – SIEM on its own does not provide any value!
- Regardless of what any of the vendors say, implementing a logging and monitoring solution properly will require take some time
- Device Inventory is Key
- Develop specific technical and functional requirements for the solution
- Develop Architecture and Sizing (EPS rates and Log Capacity) – will impact cost



SIEM Requirements Document

Table of Contents

Implementation Considerations (cont.)

- Logging Standard Developed
- Device Identification and Integration - Exact devices to be integrated have been identified? (This can be a pain and can impact project schedule if not nailed down early) - Data classification in place?
- Develop Configuration Guides for Device Integration and consistency
- Types of devices – databases will add complexities; some devices may require custom connector development
- Change Management Process (can impact device integration)
- Cyber Threat Intelligence (CTI) Feed consideration
- May require additional products – syslog server
- Number and Type of Use Cases for SIEM (outside of out-of-box rules) – these should be developed in conjunction with the phased strategy
- Tuning will be key! (Level 1, 2 and 3)

Lesson's Learned

- **Requirements analysis:** Define the requirements, control objectives, compliance requirements and problem definition;
- **Determine appropriate control levels:** Ensure that the rollout plan is mapped to control objectives;
- **Optimize and prioritize:** The key factor of a successful SEIM deployment is the appropriate selection and prioritization of log sources;
- **Threat landscape matrix:** Define a threat inventory based on the risk and control requirement profile of the client. This will be used for architecture development;
- **Set expectation:** Ensure that management and technical staff understand the key realities of the architecture;
- **Define enterprise infrastructure requirements:** This can include data store requirements, retention, network bandwidth requirements etc. It is important to involve key stakeholders;
- **Solution analysis:** Review and map compliance/risk requirements against solutions;
- **Customized for unique requirements:** SEIM solutions offer base capability however require customization to meet organizational risk and compliance goals;
- **Process development:** Define the people and processes required to support the architecture.

In Deloitte's experience, SEM/SEIM projects usually fail due to weaknesses in processes, people and vision

Questions?