

# Information security logging and monitoring

Nashville ISACA Chapter Training

November 3, 2009

Michael Sloan, CPA, CISA

Kyle Harvey, CISA, CIA, CIPP

 **ERNST & YOUNG**

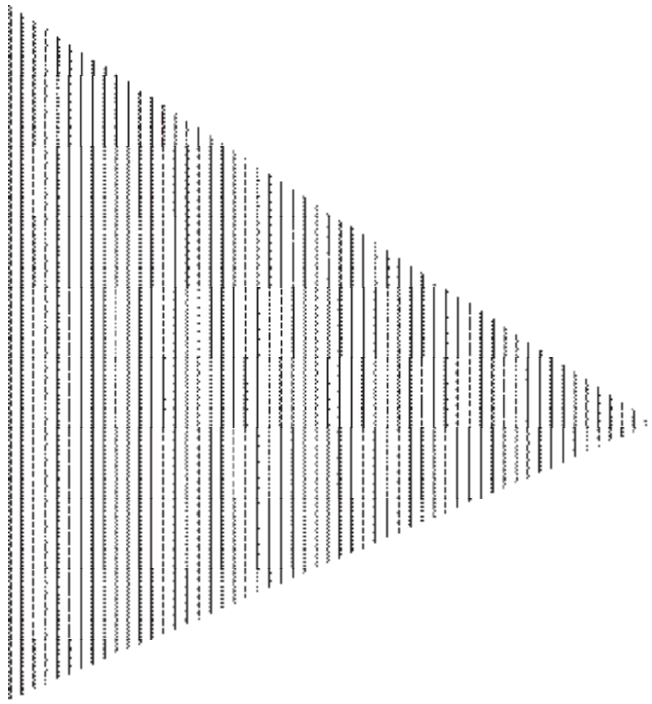
*Quality In Everything We Do*

---

# Agenda

---

- ▶ Overview
- ▶ Audit logging and monitoring overview
- ▶ Establishing a logging and monitoring vision
- ▶ Example leading practices
- ▶ Questions



# Audit logging and monitoring overview

---

# Logging and monitoring overview

---

- ▶ The purpose of security event logging and monitoring is to successfully capture relevant security events from devices and monitor activity to identify events requiring further investigation. Results from this program should trigger incident response processes.
  
- ▶ Organizations with successful security event monitoring and correlation capabilities usually have the following common goals:
  - ▶ Minimal time spent researching and categorizing security events
  - ▶ Minimal time spent researching location of security event
  - ▶ Minimal user disruption due to security events
  - ▶ Little/no impact to critical business functions as a result of a security incident
  - ▶ Minimal mean time to deploy countermeasures and mitigating controls due to increased information and accuracy of scope

---

# Benefits of logging and monitoring

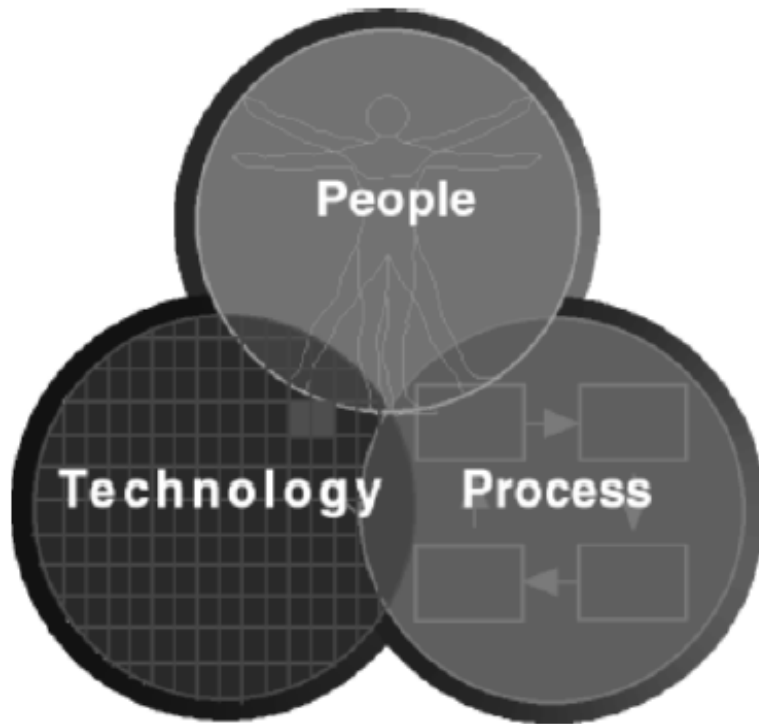
---

- ▶ Risk & regulatory compliance
  - Monitor policy and measure compliance - financial audit, SOX, PCI, HIPAA, etc.
  - Manage risk & priorities
  - Enhanced security - ability to effectively record important information security events and follow up on irregular activity
  
- ▶ Operational
  - Enhance security monitoring efficiency and reduce scope and duration of security incidents
  - Improved effectiveness for managing the security risk to the organization
  - Improved efficiency in evaluating and reporting on compliance to security policy and standards
  
- ▶ Financial
  - Focus security investment to protect most sensitive assets and critical processes
  - Enabling measurement and reporting of financial impacts of security incidents
  - Containing legal costs and corporate liabilities related to addressing security incidents

# Logging and monitoring building blocks

---

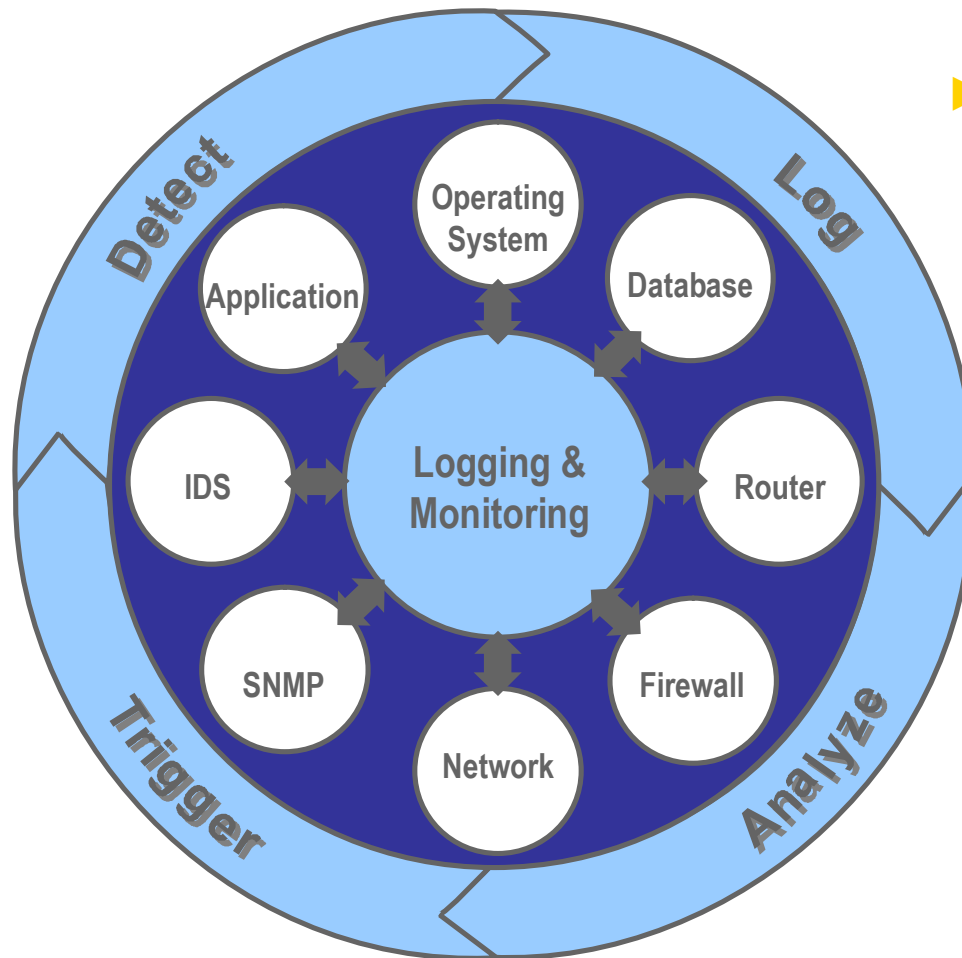
## Components



## Critical success factors

- ▶ **People**
  - ▶ Executive sponsorship
  - ▶ Defined roles and responsibilities
  - ▶ Appropriate skills and knowledge
- ▶ **Process**
  - ▶ Defined policies, procedures & Guidelines
  - ▶ Risk assessment drives scope
  - ▶ Effective incident response process
- ▶ **Technology**
  - ▶ Technology supports process
  - ▶ Technology is scalable to meet future objectives

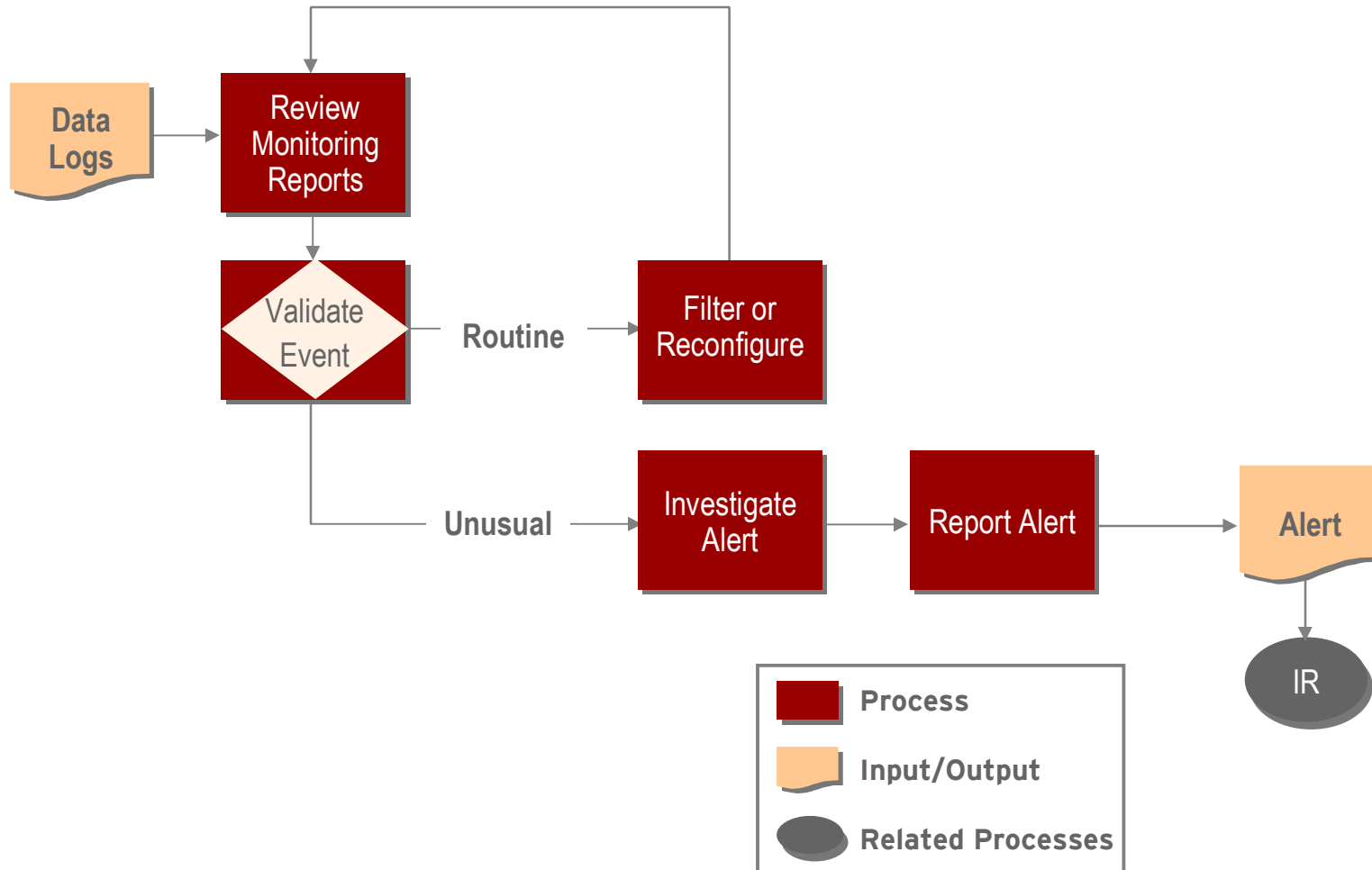
# Technology overview



## ▶ Example security event types

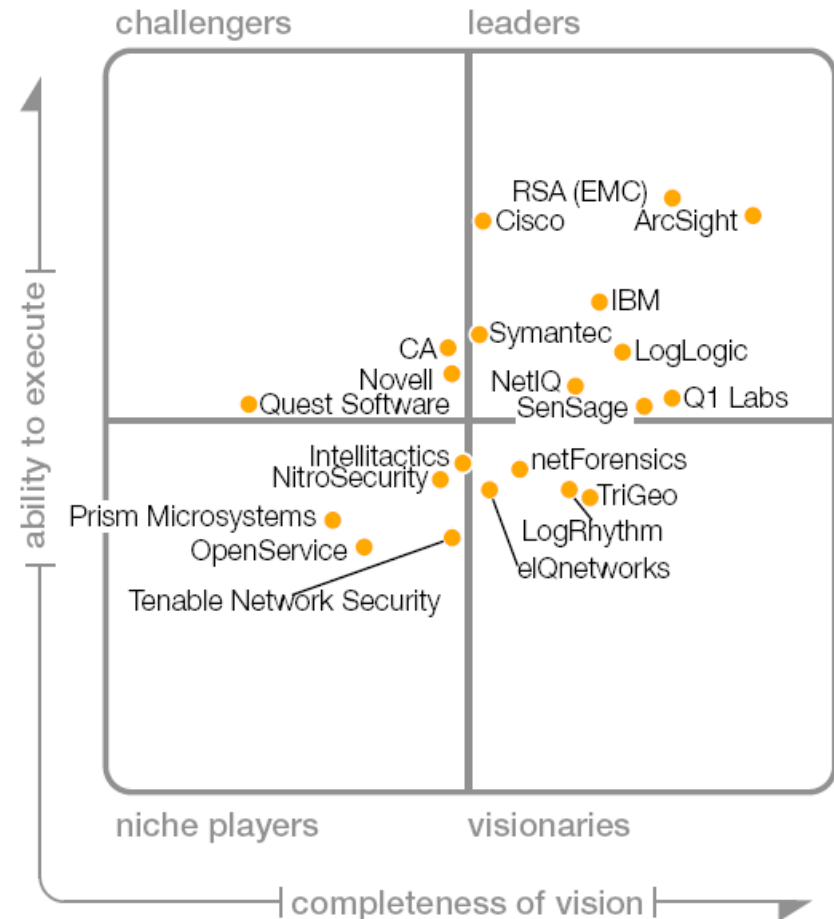
- ▶ Failed login attempts
- ▶ Failed access attempts
- ▶ Privileged user activity
- ▶ Security configuration changes
- ▶ Access to sensitive data
- ▶ Remote access
- ▶ IDS events

# Logging & monitoring - example process flow



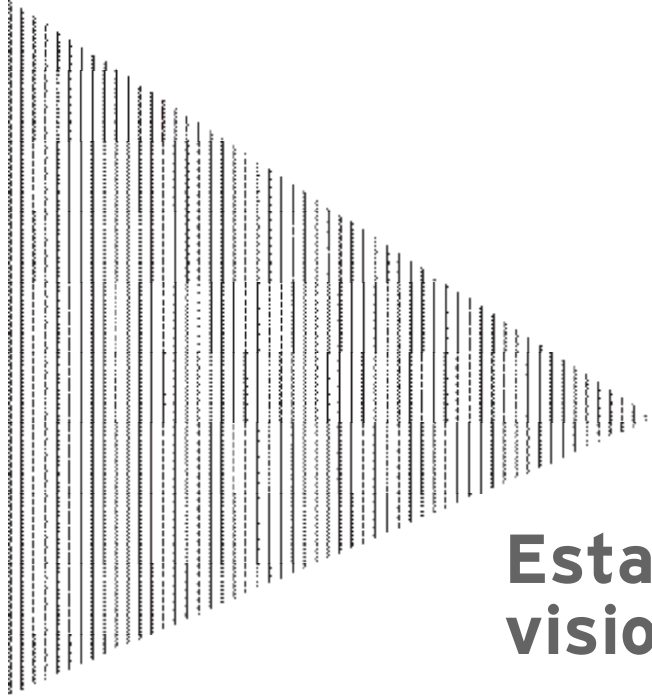
# Solution vendors

- ▶ Optimal solution in current market is one that combines the following:
  - ▶ Real-time collection and analysis of log data from host systems, security devices, and network devices
  - ▶ Supports long term storage and reporting
  - ▶ Will not require extensive customization
  - ▶ Easy to support and maintain
- ▶ While there are clear leaders in the SIEM market, different solutions may be optimal for different organizations' requirements



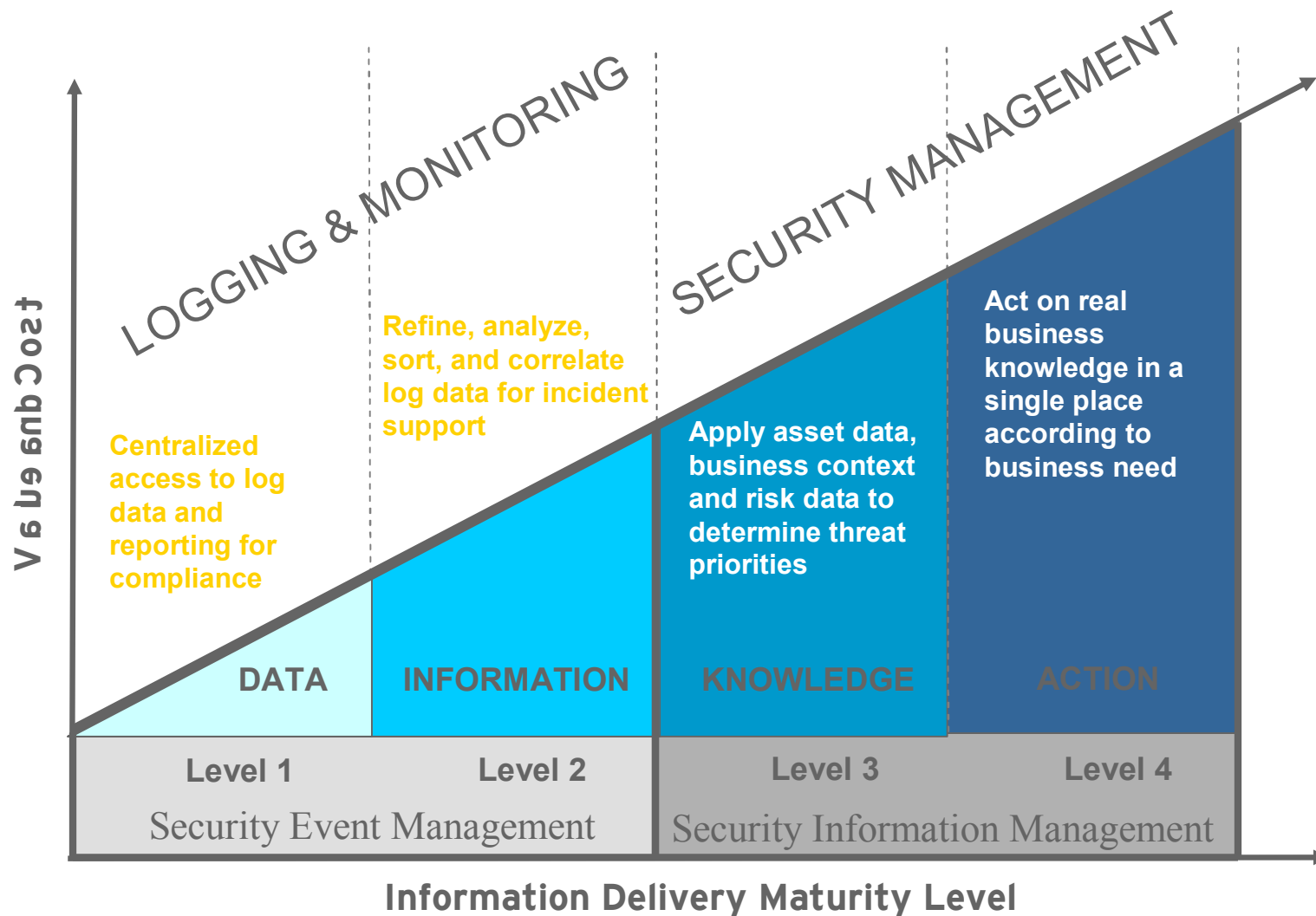
As of May 2009

Source: Gartner (May 2009)

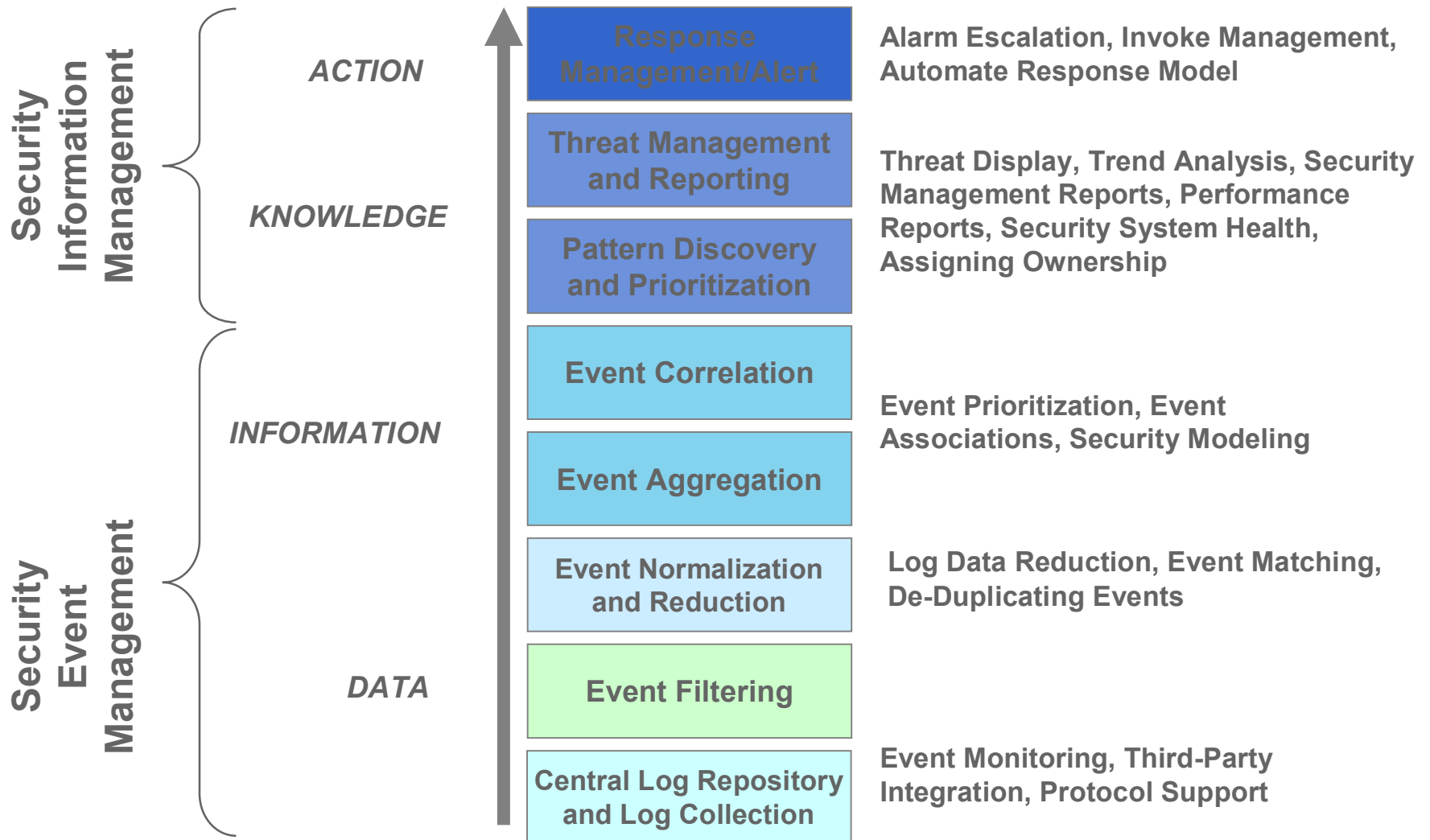


# Establishing a logging and monitoring vision

# Determining target maturity level



# Technology maturity model



---

# Systems scope

---

- ▶ What log sources are expected to be supported?
  - ▶ Network Devices (Firewalls, Routers, IDS, Gateway filters)
  - ▶ Operating Systems
  - ▶ Databases
  - ▶ Applications (Purchased/Developed)
  - ▶ Systems Management (patch management, asset management)
- ▶ Are there any planned implementations that should be supported?
- ▶ Which applications have the capability to perform logging?
- ▶ What types of reports do you envision being produced ?

---

# Organizational scope

---

- ▶ What is the organizational scope of this initiative?
  - ▶ Is this solution going to support the entire enterprise or will it be limited to specific operations?
  - ▶ What units/areas of the business do you expect to collect log data from?
  
- ▶ Do you anticipate a solution that supports multiple languages?
  
- ▶ Do you anticipate offering Logging and Monitoring as a service or closed system?
  - ▶ What services do you plan to offer with this solution?
  - ▶ What units/areas of the business do you expect to offer these services?

---

# Regulatory scope

---

- ▶ **HIPAA**
  - ▶ HIPAA Security Rule requires regular reviews of audit logs and access reports. Documentation of actions and activities need to be retained for at least six years.
  
- ▶ **Sarbanes-Oxley**
  - ▶ Although SOX applies primarily to financial and accounting practices, it also encompasses the information technology (IT) functions that support these practices. SOX can be supported by reviewing logs regularly to look for signs of security violations, including exploitation, as well as retaining logs and records of log reviews for future review by auditors.
  
- ▶ **Payment Card Industry Data Security Standard**
  - ▶ PCI DSS applies to organizations that “store, process or transmit cardholder data” for credit cards. One of the requirements of PCI DSS is to “track...all access to network resources and cardholder data”.

---

# Technology deployment options

---

- ▶ Architecture preferences
  - ▶ Appliance-based solution
  - ▶ Distributed software solution
  - ▶ Managed Hosted solution
  
- ▶ Data collection preferences
  - ▶ Agent-based or Agent less
  - ▶ Custom Log parsing flexibility
  
- ▶ Storage and capacity considerations
  - ▶ Local disk (lower cost)
  - ▶ Storage Area Network (higher scalability)
  
- ▶ Requirements for High Availability and Continuity of Service

---

# Technology integration

---

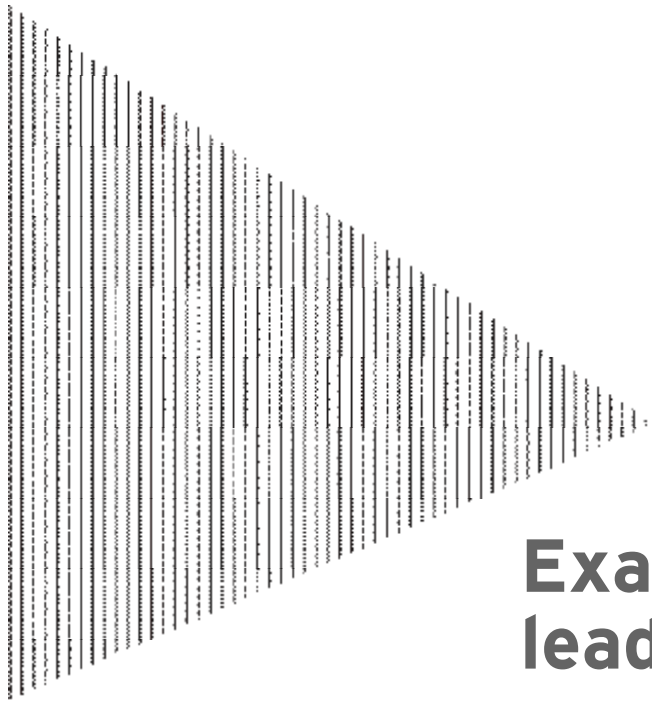
- ▶ Do you anticipate and/or desire integration with other technology solutions?
  - ▶ Help/Service Desk Management
  - ▶ Asset/Inventory Management
  - ▶ Configuration Vulnerability Management
  - ▶ Network Management
  - ▶ Identity and Access Management
  - ▶ Directory Services
- ▶ Are all log sources time synchronized using NTP and UTC?
- ▶ Does an existing Asset Management system that incorporates value and risk information for each asset exist?
- ▶ Do you anticipate integration with external threat data?
- ▶ Does a Configuration and/or Vulnerability Management solution exist?
- ▶ Does an Incident Response process exist?

---

# Operational support model

---

- ▶ How defined are event classifications and associated incident response process triggers? How integrated?
- ▶ How do you envision the operational model, workflow and process integration with other teams?
  - ▶ Log source integration and support
  - ▶ Log monitoring and response management
  - ▶ Report analysis and distribution
  - ▶ Solution support and management
- ▶ Who do you anticipate supporting and managing the solution?
  - ▶ System administration support
  - ▶ Storage administration support
  - ▶ Database administration support
  - ▶ Service development support



# Example logging and monitoring leading practices

---

## Example leading practices

---

- ▶ Spend time upfront for the following preparation activities:
  - ▶ Determine vision and strategy for logging and monitoring solution
  - ▶ Perform a risk assessment to determine which security events to log and which to log and monitor
  - ▶ Determine which log traffic you would like to capture, and from which devices
  - ▶ Risk assessment results should drive the enterprise-wide logging and monitoring governance framework.
  - ▶ Define formal logging and monitoring technical standards for all supported devices and technologies
  - ▶ Develop logging and monitoring use cases
  - ▶ Define formal policies and procedures which include specific action plans and review processes for detected events/exception reports
  - ▶ Integrate the logging and monitoring program with other processes (data classification, asset inventory, incident response, capacity planning, etc)

---

# Perform a logging and monitoring risk assessment

---

▶ Purpose:

- ▶ Identify and evaluate the types of security events that can be logged and monitored in order to determine those events that have the greatest potential for negatively impacting the organization.

▶ Approach:

- ▶ Leverage industry standards as a starting point, examples include:
  - ▶ ISO/IEC 27002:2005 Code of Practice for Information Security Management
  - ▶ NIST 800-92 "Guide to Security Log Management"
- ▶ Identify the relevant types of events that should be considered as part of the Logging and Monitoring program (technology agnostic).
- ▶ Establish categories of systems or risks levels that will be evaluated for each event type
- ▶ Evaluate the risk associated with each identified event type, considering the system category or relative risk of the affected information assets.

# Risk assessment example

- ▶ The event types as listed in Section 10.10.2 “Monitoring System Use” of ISO/IEC 27002:2005 are:
  - ▶ Authorized Access (To Key System Resources)
  - ▶ Privileged Operations
  - ▶ Unauthorized Access Attempts
  - ▶ System Alerts or Failures
  - ▶ Changes to System Security Settings and Controls
- ▶ For each event type defined above, consider the impact to critical systems and existing mitigating controls to determine the appropriate level of logging and monitoring for each system.

Unauthorized Access Event Type	High Risk	Moderate Risk	Low Risk
Failed Login Attempts	LM	LM	L
Failed Resource Access Attempts	L	L	N
Failed Attempts to Run Commands	LM	L	N

*Legend*

- LM** Log and Monitor
- L** Log Only
- N** No Action Recommended

---

# Turn risk assessment results into logging and monitoring framework

---

- ▶ Take high level event strategy determined during risk assessment and apply to each relevant security layer
  - ▶ Network
  - ▶ Operating system
  - ▶ Database
  - ▶ Application
- ▶ The combination of strategies for each layer should accomplish the high level objective specified in the risk assessment
- ▶ Define each event type by layer
- ▶ Create incident definitions for each event, which will link to response procedures or technical requirements for automated solution

---

# Develop use cases

---

- ▶ The day-to-day use of the logging and monitoring solution should be continually considered.
  - ▶ What process occurs when an event is detected?
  - ▶ At what point is an event escalated to an incident? What occurs at this point and who is involved?
  - ▶ When are business managers involved?
  - ▶ How do we demonstrate compliance with policies to an external auditor?
  
- ▶ Consider scenario-based use cases, such as:
  - ▶ Unauthorized activities by an internal user
  - ▶ Virus/worm infections
  - ▶ External attacker

---

# Risk assessment and framework creation feed policies and procedures

---

- ▶ Define logging and monitoring requirements
  - ▶ Event definitions and risk assessment process
  - ▶ Event logging, monitoring and response requirements
  - ▶ Log content requirements (e.g., date/time stamp, executor ID, location, etc)
  - ▶ Monitoring frequency
- ▶ Event assessment criteria
  - ▶ Incident definitions
- ▶ Incident management process (or reference to existing process)
- ▶ Log and incident report integrity, storage, and security
  - ▶ Log retention requirements
  - ▶ Access to log data and security requirements
  - ▶ Log integrity
  - ▶ Segregation of duties

# Policies drive technical standards

---

- ▶ Technical configuration standards must be developed to facilitate the configuration and log collection process for each supported technology.
- ▶ Translate the logging and monitoring policies and procedures into detailed technical standards for implementation.

## **2.4 LOG CONFIGURATION SPECIFICATIONS**

To log critical events, the AIX operating system must be configured appropriately. The following sections define the configurations that must be in place in order to support events defined in the **Logging and Monitoring Policy**.

<b>Event</b>	<b>Configuration Requirements</b>	<b>Log Collection</b>
Successful System Logins	Successful login activity is logged automatically by AIX.	Login information is stored in the <code>/var/adm/wtmp</code> file. The file can be read using the "who -s" command or the "last" command.

---

# Questions?

---