SIEM Maturity and SOC Optimization for the Portland ISSA SIEM Symposium

October 22, 2015

John Velisaris, IBM

JVelisaris@us.ibm.com

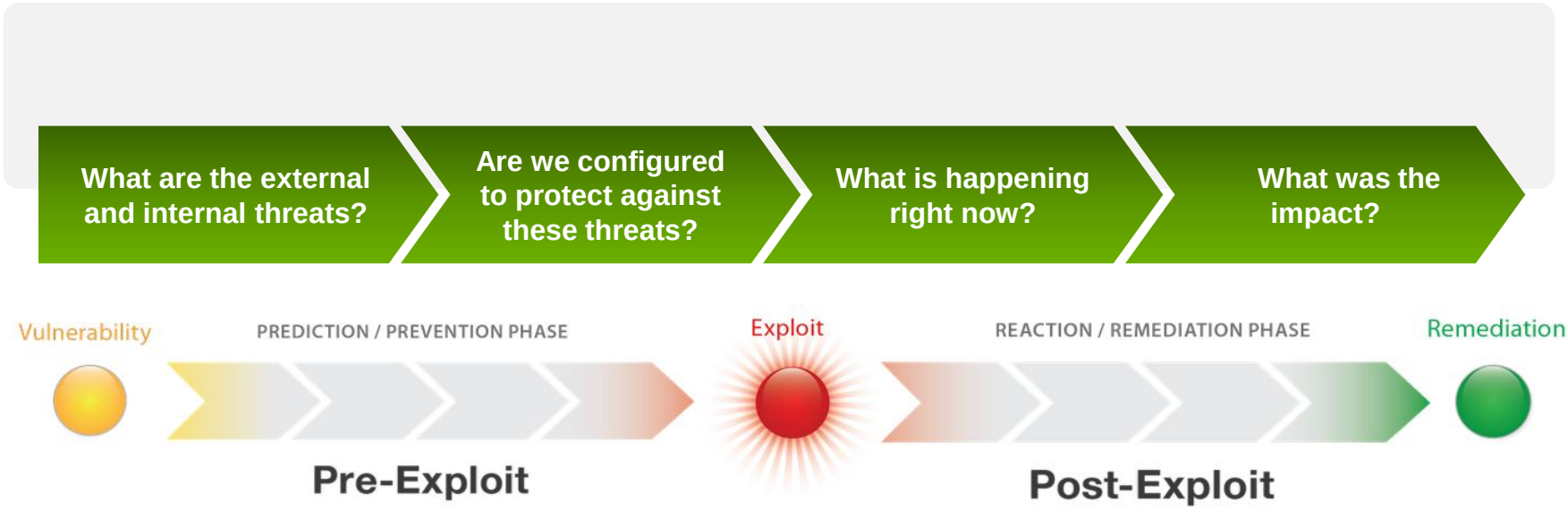
Speed of change is difficult to comprehend in an era of the industrialization of cyber security attacks

- Risk is Relative; Value of Security is different for each stakeholder
- Start gradually and build capabilities in phased implementation
- Measure and communicate the value of security capabilities
- Security intelligence is critical to prioritizing uses cases and data sources
- Migrate from low value to high value use cases gradually
- Dimensional data increases the resolution and value of all data
- Convergence of security, risk, fraud data and function
- Security Operations Centers are Transformational (Craftsman > Factory)
- Security is a program not a project, requires new capabilities every 90-120 days
- Leverage vertical vs. horizontal deployments when possible

The value of the SOC is directly related to the uses cases and rules that a client adopts and the data available

- Clients spend an avg. of $3-$10M dollars to buy and implement a SIEM
- Clients spend an avg. of $3M-$5M implementing a Security Operation Center
- Annual spending to operate a SOC average $3M-$10M per year
- 30-35% of annual SOC spend supports new data, use cases, rules, reporting
- Use cases and reporting evolve as new events and dimensional data are added
- Avg. cost of operationalizing a new case ranges from $20K-$50K
- Avg. time needed to identify, design, develop, test, implement and tune a new use case and its supporting SIEM rules are measured in weeks or months
- SOC and the security team must measure the value of use case portfolio
- Most clients start with low-value use cases that monitors infrastructure configuration and/or compliance controls because the data is easy to collect
- Security strategy should be to migrate to data that enables high value uses, reporting and analytics

Security Analytics Before and After the Exploit



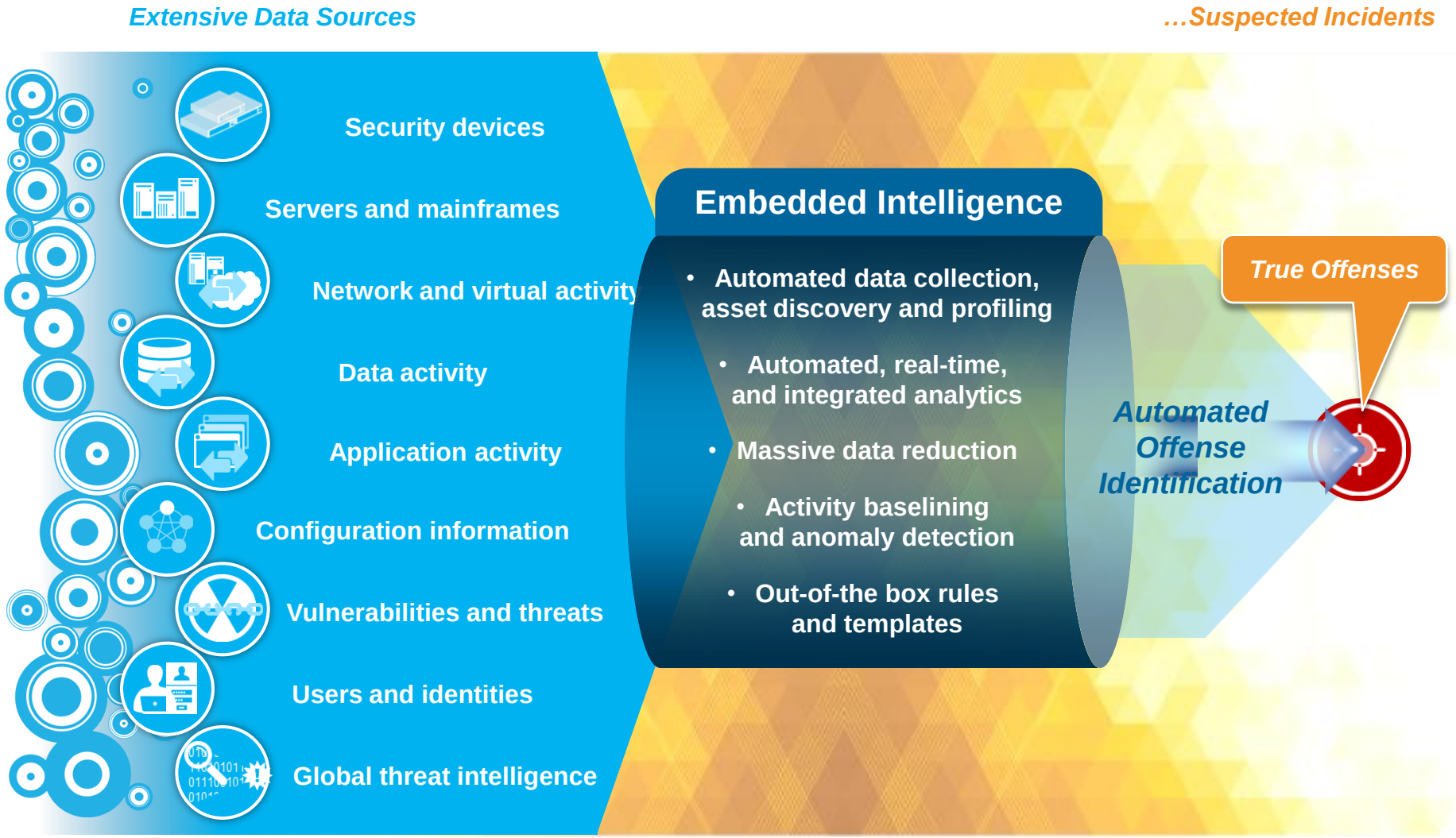
Pre-Exploit (Threats):

- Filtering Security Intelligence
- Build line of sight to emerging threats
- Alerts for high-priority threats

Post Exploit (Security Incidents):

- Enhanced Security Incident Reporting and Analysis
- Weekly reports by LOB, Function
- Alerts for key LOB. Functions

SIEM Technology Uses Analytics to Identify Threats



We are constrained to analyzing transaction behavior if referential data is missing

Contextual & Referential Data

- Core/Server/Access networks
- Non-routed networks
- Trusted/Untrusted networks

Network

- Function: web, mail, DNS
- OS: Windows, Linux

Assets

- Access and Entitlements
- Physical access
- Human factors; fraud, insider threat

User

Security Analyst

SIEM System

- Anonymous Proxy
- Botnet C&Cs
- Malware hosts

External

- Credentialed scan results

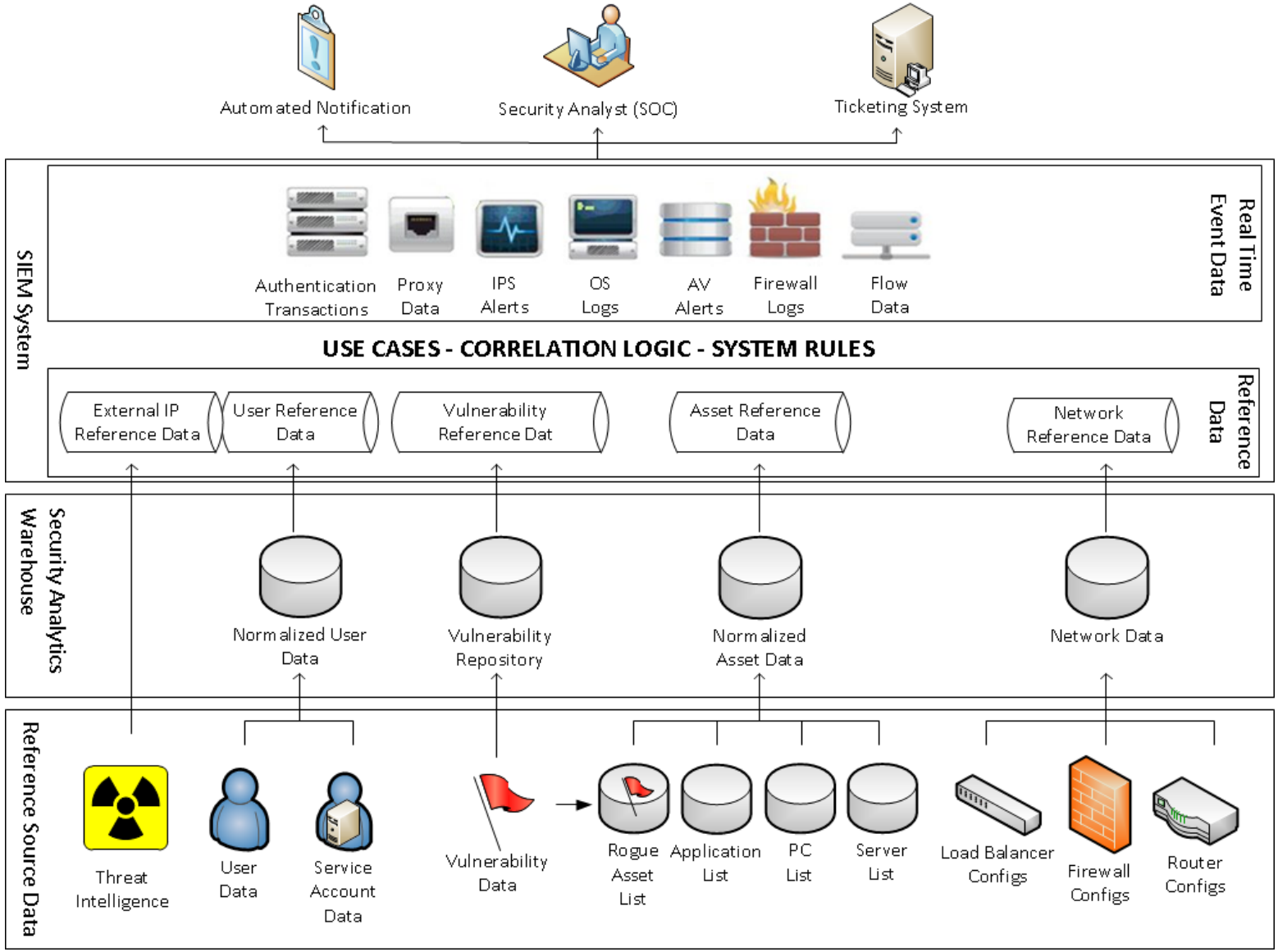
Vulner-ability

Real Time Event Data

- Network Activity
- Virtual Activity
- Config/Change Info
- Application Activity
- Servers & Hosts
- Security Systems
- User Activity

Situational Awareness

SIEM Functional Model



The SIEM Lifecycle Informs SIEM Design

SIEM **Governance** starts with the owner of a strategic plan laying out the company's **Strategy**, which is typically informed by stakeholders in security, IT, compliance, risk management and audit.

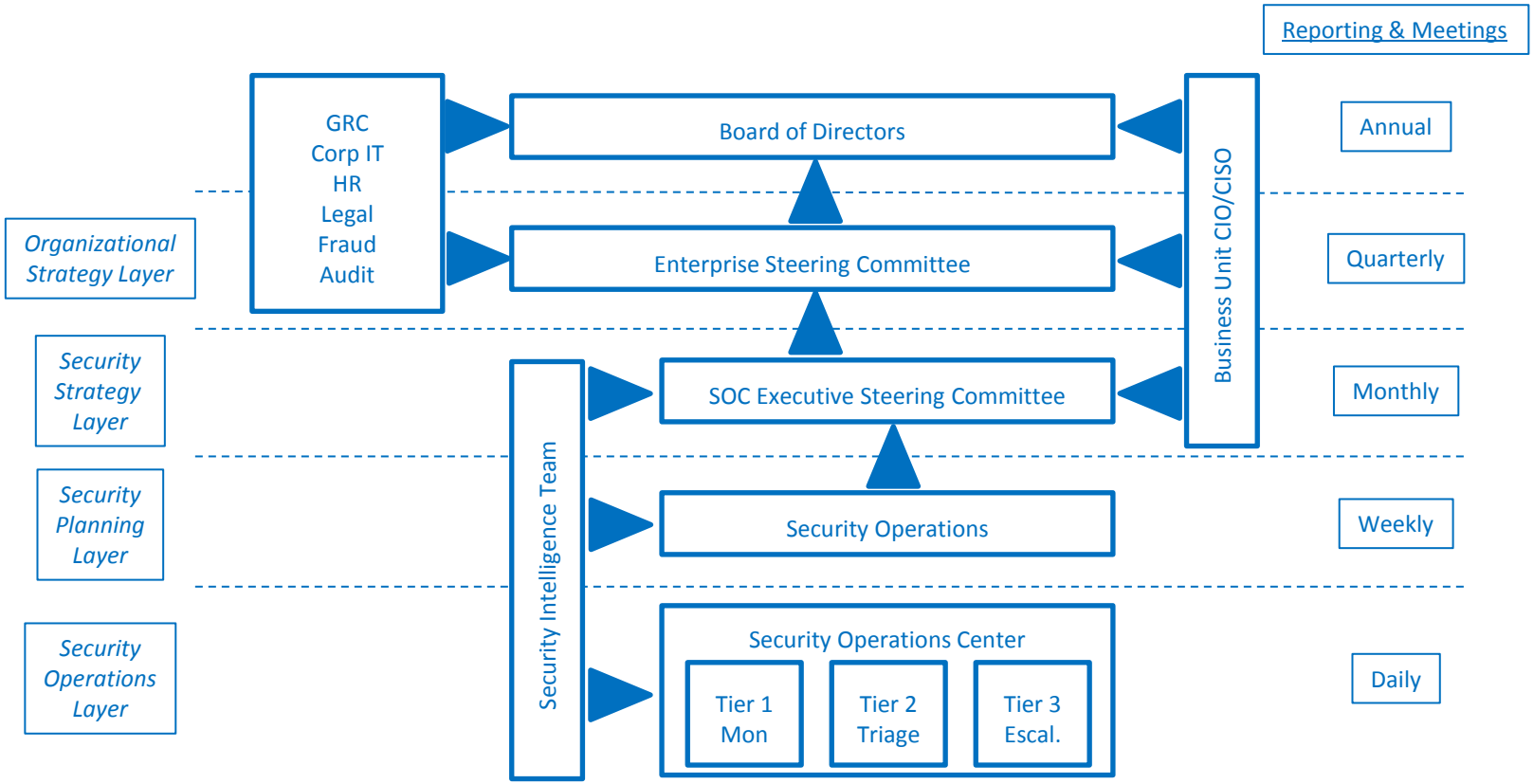
These stakeholders have **Requirements**, which need to be translated into **Use Cases.**

Once the Use Cases are identified, the required **Data & Log Sources** are interfaced with the SIEM system.

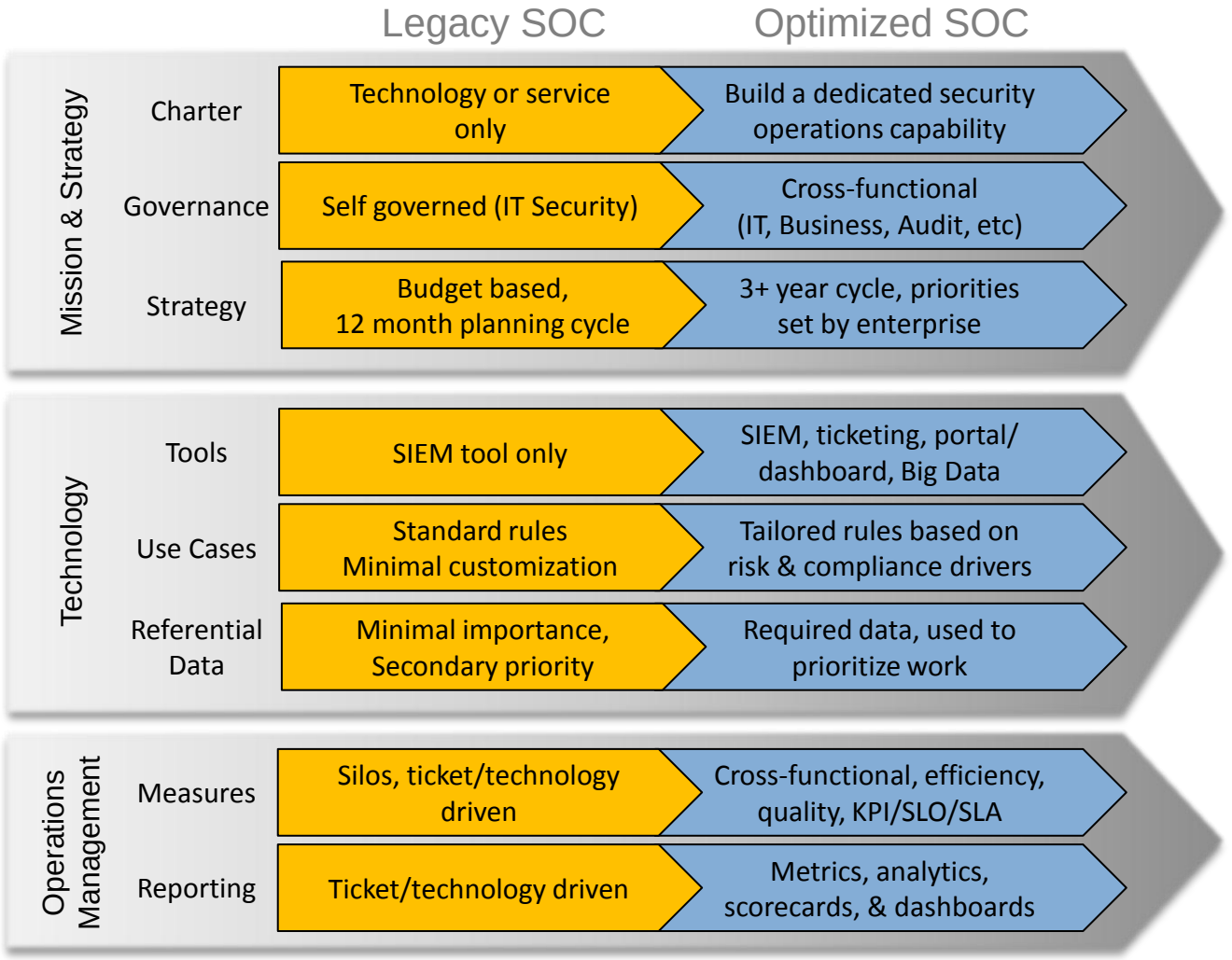
Use Cases typically require a contextual analysis of log data to be performed. The SIEM's **Correlation & Analytics** capabilities fulfill this role.

While **Monitoring** activities occur within the SIEM, system **Reporting** gives stakeholders data used to drive response activities or to refine the SIEM **Strategy** via approvals derived through the **Governance** process.

The governance model provides the leadership and decision making framework used to monitor and manage the project



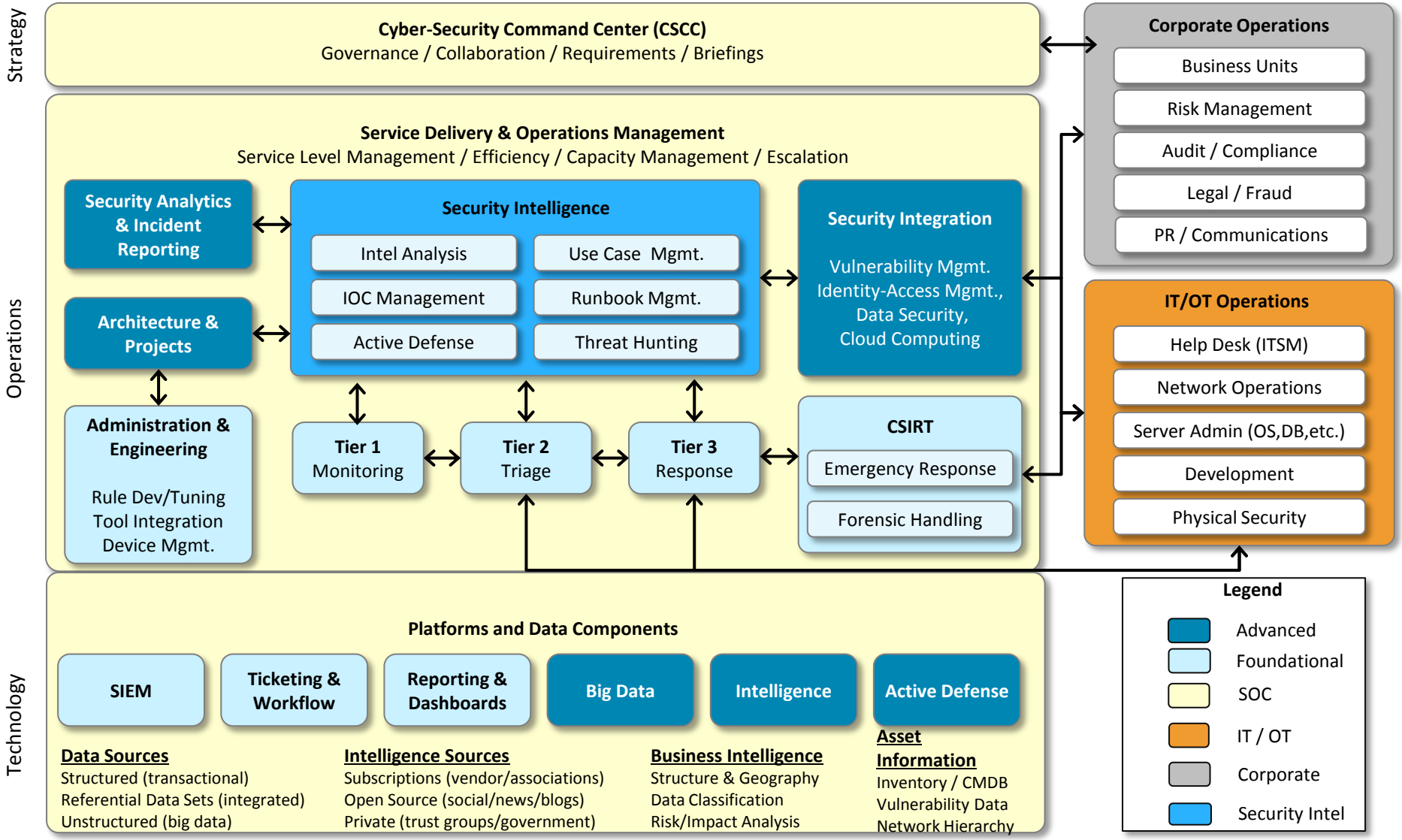
The changing requirements for enterprise security & risk management coupled with technology advancements have triggered a paradigm shift in the design and ongoing administration of a Security Operations Center ("SOC").



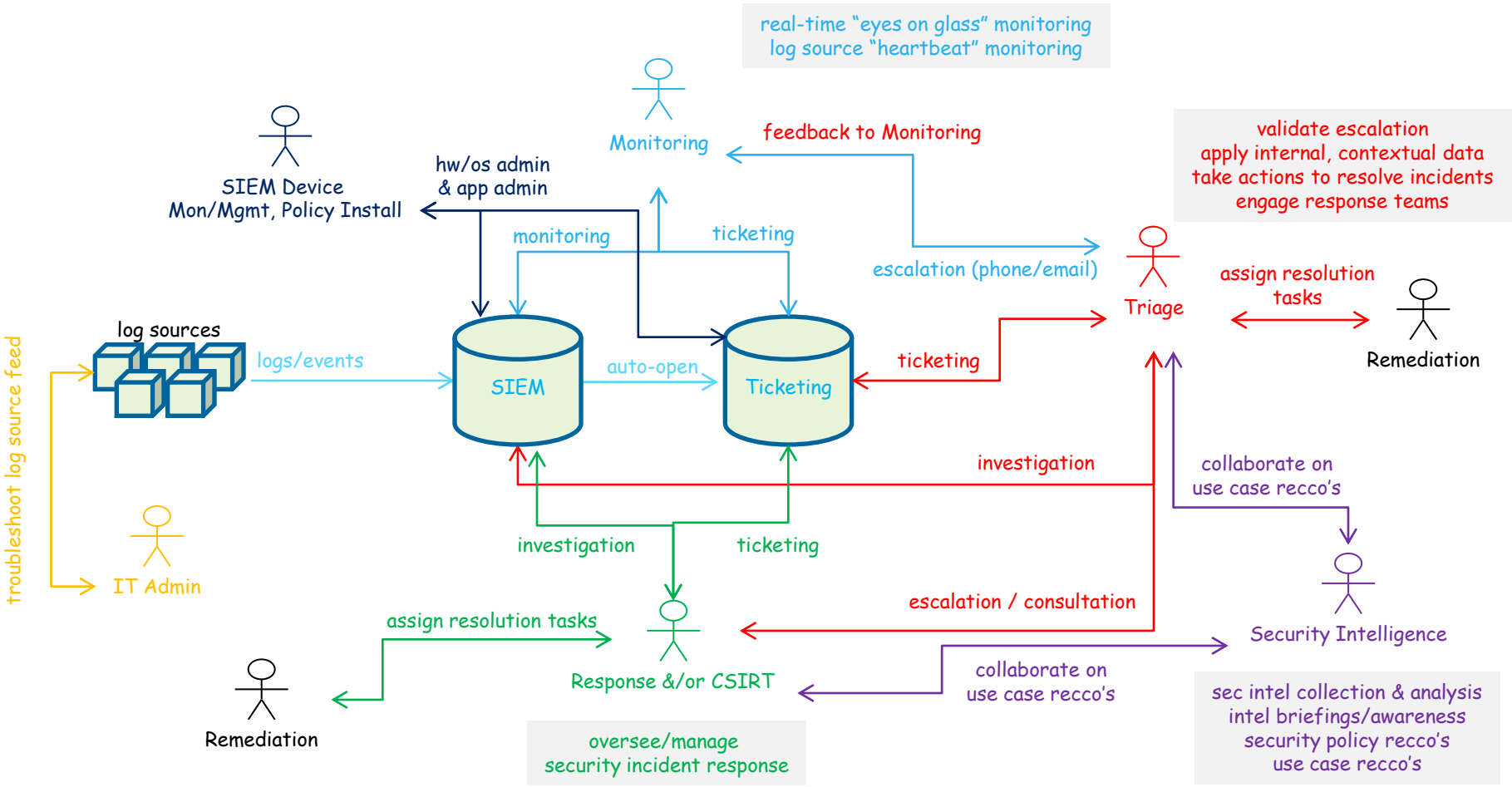
Detect & react to threats.

Proactive. Visible. Anticipate threats. Mitigate risks.

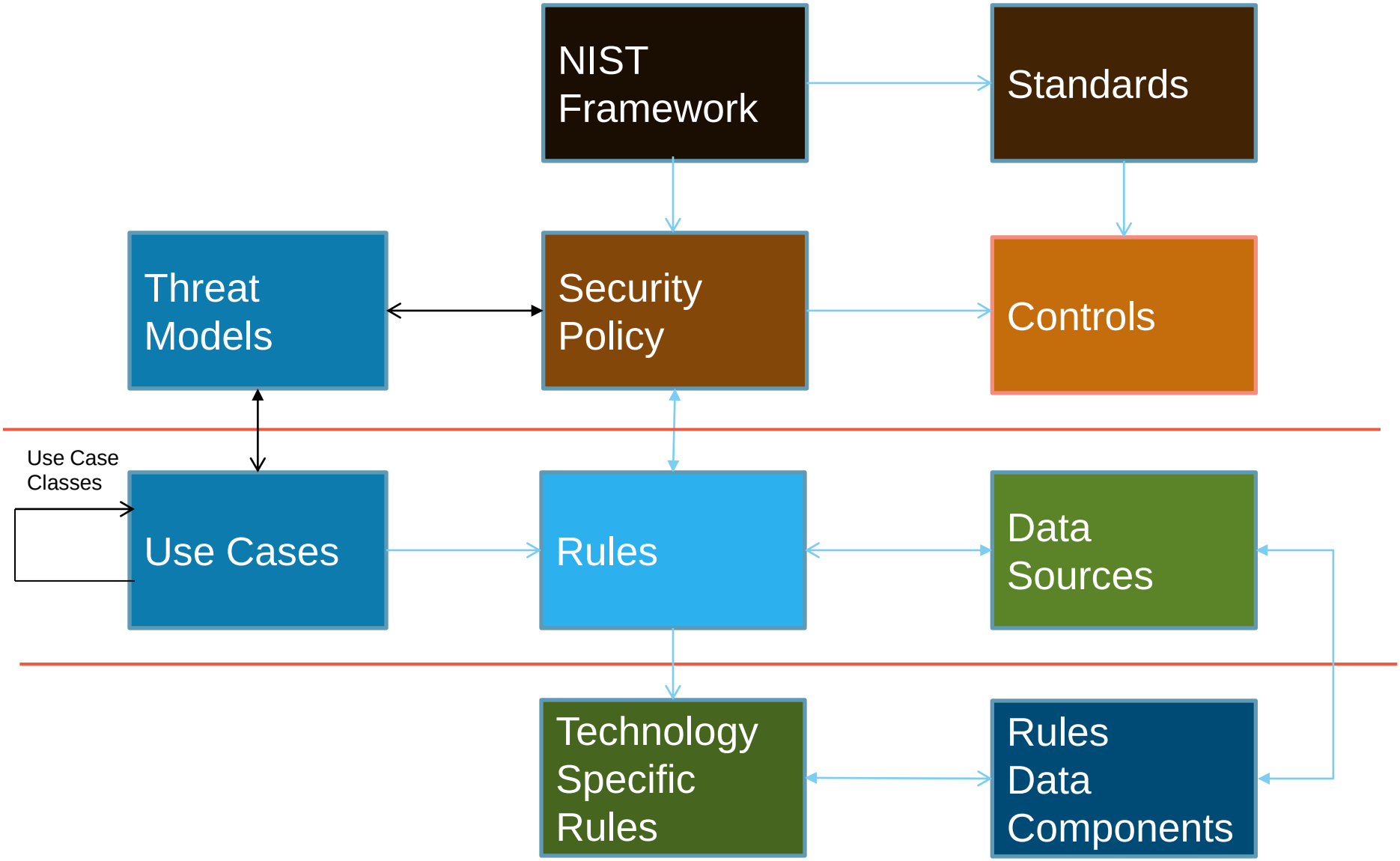
IBM Security Operations Operating Model



The SIEM platform must support a clearly defined incident management process



Use Case Framework



Use Case Example: Detect - Monitor Network Events (DE.CM-1.1)

- **Category:** Security Continuous Monitoring
  - Track, control, and manage cybersecurity aspects of development and operation (e.g., products, services, manufacturing, business processes, and information technology) to identify cybersecurity events.
- **Sub Category:** Network Security Monitoring
  - Perform network monitoring for cybersecurity events flagged by the detection system or processes.
- **Use Case Number/Name:** DE.CM-1.1 Monitor Network Events
  - Monitor network events for signs of malicious and/or anomalous activity.
- **Regulatory References:**
  - NIST SP 800-53 Rev. 4 CM-3, CA-7, AC-2, IR-5, SC-5, SI-4
  - ISO/IEC 27001 A.10.10.2, A.10.10.4, A.10.10.5
  - COBIT DSS05.07
  - PCI 10
  - SANS Top 20: CSC 14, 16
- **SIEM Output/Presentation:**
  - Dashboard: Yes
  - Alert: Yes
  - Case: Manual
  - Report: No
- **Log Sources:**
  - FW, IDPS, WIDS, AD, Windows Security, Mainframe, Server or Appliance Syslog
- **Rule Name(s):**
  - Failed Authentication
  - Network Probes
  - Malware Detection
  - Rogue Wireless Detection
  - Intrusion Alerts
- **Sample Rule Description:** Rouge Wireless Detection
  - Identify any wireless IP access points that are not contained on the pre-defined authorized WAP list.

Use Case Classes

Low to Moderate Value:

- Configuration
- Security Devices
- Network
- Data Flow
- Back Doors
- Vulnerabilities
- Compliance (privileged users)
- Key Control monitoring
- Physical Security
- Risk Monitoring
- Real Time Forensics

Moderate to High Value:

- Business Policy
- Cloud
- Third Party Monitoring
- Identify and Access Management
- Mobile
- Social (e.g. Phishing, Threat Intel.)
- Application
- Data Privacy
- Secure workplace (Internal threats)
- Anomaly (Behavior)
- Fraud
- Crown Jewels

Richer set of events enable moderate to high value uses cases, rules, analytics and reporting

- Application Logs
  - Transactions
  - Table maintenance
  - Base users activity profile
  - Privileged users activity profile
  - Access change requests
  - Normalized patterns by user role
- Social
  - Company mentions/content
  - User mentions/context
- Business Policy
  - BP rules
  - BP compliance
- Fraud
  - User classification
  - User activity profile
  - High risk trans. (defined/calculated)
  - High risk behaviors (defined)
  - High risk behaviors (calculated)
  - Anomaly behaviors (calculated)
  - Actions
    - Monitor
    - Pause
    - Authenticate
    - Stop
    - Block

Contextual, dimensional data provides context, which improves resolution, value and response – example one

Security Intelligence:

- Bad actors targeting my industry
- Method they are using is new form of phishing attack
- Leveraging a new set of hacking tools associated with a group in Russia
- Target is network access through comprised email credentials
- Exploit relies on Windows APIs to collect MAC Address, Username, Hostname, IP Address, Timestamp, dest. domain name
- Exfiltrate data or take control of machine

Dimensional data:

- Specific version of windows is vulnerable
- CMDB has a detailed listing of machines with this version
- Vulnerability scans data has this information as well
- Using this information determined that approximately 126 windows devices are vulnerable
- These devices are located on the network in end user only segments

Contextual, dimensional data provides context, which improves resolution, value and response – example two

Malware infection is detected:

- 15 machines show signs of malware infection
- These machines are generating an unusual amount of network traffic
- The machines may be attempting either data exfiltration or machine control
- Data appears to be encrypted representing a more sophisticated attack

Dimensional data:

- 9 of the machines are associated with one GL department code
- The department related to this GL code does merger and acquisition due diligence
- Employee information ties back to the same GL department code
- 2 of the machines are associated with a cost center project code
- The cost center project code was established for a ‘special project’

Security analytics provide the visibility and insight to completely manage the environment and act with speed and conviction to protect the enterprise

Security Posture

- Application Security
- Asset Security
- Environment Vulnerabilities
- Environment Threats
- Attacks
- Alarms
- Identification Response Time
- Investigations
- Incidents (by Priority)
- Incident Remediation

Workload & Efficiency

- Workload per Tier
- Process Cycle Efficiency
- Average Cycle/Handling Time
- Tickets Opened vs. Closed
- Staff Utilization
- Defects
- Availability

Security Financial Analysis

- Average Cost per Threat
- Average Cost per Alarm
- Average cost per Investigation
- Average cost per Incident
- Planned Costs vs. Actual Costs (plan, build, run)
- Cost per Department (Tier)

Illustrative SOC Metrics

ILLUSTRATIVE

SECURITY METRICS

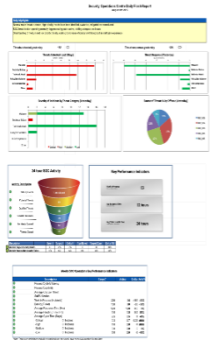
- **Funnel Metrics:**
  - Total Events last 24 hours
  - Events Processed Percentage
  - Threats
  - Qualified threats
  - Incidents Opened
  - Incidents closed

- **Operational Metrics:**
  - Validated threats Summary
  - WIP
  - Response Time (Queue Wait Time)
  - Detection Time (From Event Alert to Incident Validation)
  - Cycle time Global / trends last 30 days
  - Regional Cycle time / Trends last 30 days
  - Defect rate (quality measure)
  - Hours of Operation / Availability
  - Process Capability

- **Protection from Global Threats**
  - Threat Source Location /Geography
  - Target Business Units
  - Target Geography
  - Target Function

- **Detect Attacks**
  - New rules, refined rules
  - False Positive% vs. target
  - Self Detected vs. Reported %
  - Remediation
  - #plays in playbook, # of time used MTD, QTD, YTD
  - Recidivism Rate (reopened incidents)
  - Top Ten Validate Threats MOM, QOQ, YOY (Pareto Chart)

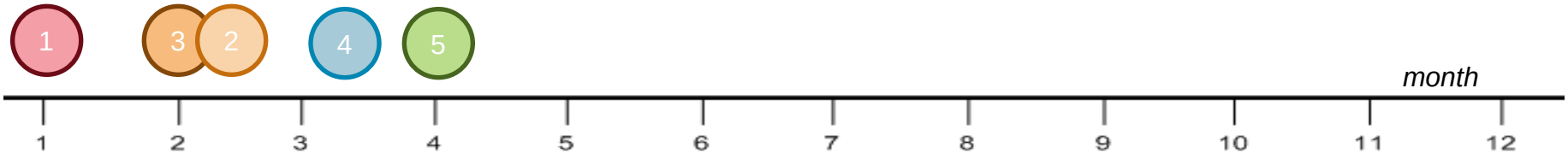
- **Financial Measures**
  - PCE
  - Cost Per Threat
  - Value Added Time
  - Waste
  - Staff utilization
  - Production Rates
  - Threat Intelligence
  - Proactive Threats Analyzed
  - % of PATA Relevant
  - Counts of new proactive Threats detected



SIEM Methodology and timeline

1	2	3	4	5
Project Initiation and Planning	**SIEM System Design**	**Implementation**	**Integration and Transition**	**Ongoing Operational Support**
▪ Kickoff ▪ General information ▪ Key stake holders ▪ Business goals ▪ Compliance Analysis ▪ Locations ▪ Requirements ▪ SIEM Infrastructure ▪ Data Retention ▪ HA, DR, Backup restore ▪ Network Topology ▪ Reporting ▪ Deliver Service Plan	▪ Architecture ▪ Use Cases ▪ Network Hierarchy ▪ Asset Classification ▪ Data/Log Source Integration ▪ Vulnerability Management & Integration ▪ Flow source integration ▪ Incident Life Cycle ManagementReporting and Dashboard ▪ Design Review ▪ Update Service Plan	▪ Install and Configure Server Appliance ▪ Customize Server Appliance ▪ Configure External Collectors, Appliances and Additional DSMs ▪ Configure uDSMs ▪ Test Data Integrity land GUIs	▪ Conduct Readiness Assessment ▪ Stage Transition to Operational Support ▪ Reports Definition and Validation ▪ Initiate Steady State Operations ▪ Deliver Application Support & Control Documentation ▪ Communication Plan	▪ Real-Time Event Monitoring and Notification ▪ Reports Generation, Review and Analysis ▪ SIEM System Management ▪ SIEM PCRs ▪ X-Force Threat Analysis Service ▪ Delivery Monthly Operational Report
▪ SIEM Manager ▪ Transition Architect	▪ SIEM Manager ▪ Transition Architect ▪ SIEM Admin	• SIEM Manager • Transition Architect • SIEM Admin • SIEM Lead	• SIEM Manager • Transition Architect • SIEM Admin • SIEM Lead	• SIEM Manager • SIEM Admin • SIEM Lead & Analysts

Project Timeline



SIEM Critical Success Factors

- **A SIEM strategy is required**—A comprehensive understanding of the threats that effect the business is necessary to establish clear and actionable SIEM deployment and operations strategy.
- **Quality data sources are needed**— A SIEM can only be as insightful as the data sources that it is analyzing.
- **Fine tuning is required to filter out the noise** —The ability to ignore, suppress, or block irrelevant and non-critical event traffic is required to be able to focus on the most critical events.

SIEM Deployment Challenges

- **Getting Required Data** — “Right” event sources, logging in the “right” way is absolutely critical to the success of your SIEM. The SIEM cannot consider information that does not exist.
- **Filtering and tuning** —Ability to ignore, suppress or block certain event records or messages from being processed or displayed. Too suppress or not suppress messages is the question. Filtering reduces “noise”, but it is also a very good way to lose very important event records.
- **Defining Governance and Strategy** — identify the key regulatory requirements, and the associated business-risk driven strategy and priorities. Is the design and implementation of the SIEM system architecture driven by an enterprise information security governance and cybersecurity controls that clearly define goals, objectives and strategy.

The IBM Security Maturity Model

The IBM Security Operations Maturity Model follows the structure of the Carnegie Mellon Capability Maturity Model Index (CMMI) and assesses five Components

	Maturity Level Descriptions				
Components	**Initial (Chaotic)**	**Managed**	**Defined**	**Quantitative Mgmt.**	**Optimizing**
Architecture & Technology	Capabilities at this level are (typically) undocumented and in a state of dynamic change and are characterized as ad hoc, uncontrolled and reactive. This level of maturity makes for a chaotic or unstable environment.	Capabilities at level 2 are repeatable, and when used can provide consistent results. Standardization is unlikely to be rigorous and are likely to be bypassed in times of stress.	Level 3 capabilities are defined, documented and standardized with moderate degrees of improvement over time and are characterized as more consistent internal to a department or team but are still subject to periods of instability when cross functional coordination is required.	Level 4 Capabilities are well standardized, cross-functional and make effective use of metrics to enable staff and management to effectively execute, monitor and manage the people, processes and technology. Processes at this level are efficient (Process Cycle Efficiency) and capable (operating within 3-4 Standard Deviations of target).	Capabilities at Level 5 are continually improving through both incremental and planned strategic changes/improvements. At maturity level 5, technology, processes and governance are cross-functionally integrated with shared goals, objectives and measures at the staff, management and leadership level.
Process & Procedures					
Organization					
Metrics & Analytics					
SOC Governance					
	Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**

The IBM SIEM Maturity Model follows the same CMMI structure, but assesses the Components of Event Type, Source Definition & System Analysis; Requirements and Use Cases; Log Management; Correlation and Analytics; and SIEM Governance

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security