

Security Operations Center (SOC): The beating heart of risk management

Naif Alotaibi, CISM, CISSP
Saudi Aramco

Who am I?

- Leading Security Operations Center (SOC) at Saudi Aramco
- 10+ years experience in cyber security
- MS degree in Information Security from Carnegie Mellon University – USA
- BS degree in Computer Engineering from King Saud University – Saudi Arabia
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)

Cyber Security Risks

Equifax breach could be most costly in corporate history

www.reuters.com

1 min read

NEW YORK/TORONTO (Reuters) - Equifax Inc (EFX.N) said it expects costs related to its massive 2017 data breach to surge by \$275 million this year, suggesting the incident at the credit reporting bureau could turn out to be the most costly hack in corporate history.

The projection, which was disclosed on a Friday morning earnings conference call, is on top of \$164 million in pretax costs posted in the second half of 2017. That brings expected **breach-related costs through the end of this year to \$439 million**, some \$125 million of which Equifax said will be covered by insurance.

Cyber risks must be viewed as business risks

Saudi Aramco: Public

Cyber Security Risks

Who's behind the breaches?

73% of breaches were perpetrated by outsiders

28% of breaches involved internal actors

2% of breaches involved partners

2% of breaches featured multiple parties

50% of breaches were carried out by criminal groups

12% of breaches involved state-affiliated actors

What are other commonalities?

49% of non-POS malware was installed via malicious email

76% of breaches were financially motivated

13% of breaches were motivated by the gain of strategic advantage (espionage)

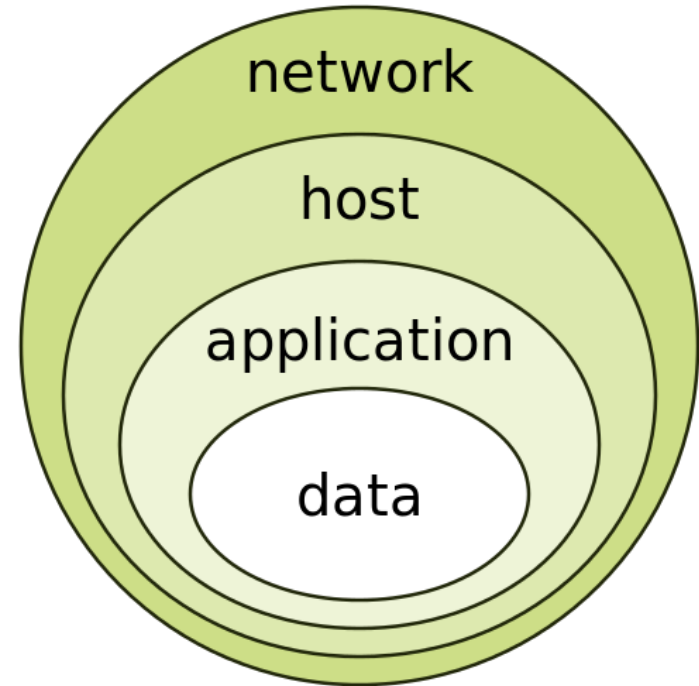
68% of breaches took months or longer to discover



Data Breach Investigation Report 2018

Defense in Depth

- Cyber breaches are inevitable
- Implement defense-in-depth
- Defenses will likely fail
 - Raise the bar high enough for attackers to make a mistake
 - Force them out to the surface
- Monitoring at every layer is a must
 - Security Operations Center (SOC)
- Effective SOC is key control to manage cyber risks



SOC Mission

- To detect, respond to, contain, eradicate, and recover from cyber incidents in a timely manner
 - Minimal disruptions to business operations
 - Protect assets confidentiality, integrity and availability
- Drive risks reduction and enhancements in organization protection controls & security posture



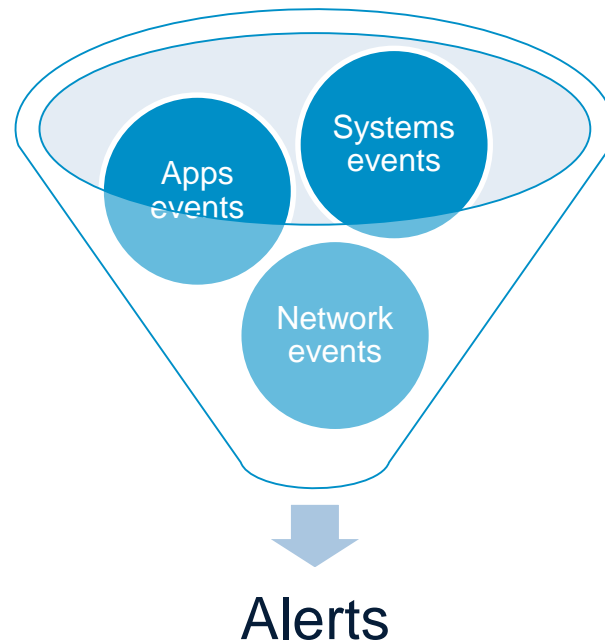
Traditional Security Operations Center (SOC)

Common SOC functions

24/7 monitoring	Incident Response	Forensics	Threats Management	Systems Support
<ul style="list-style-type: none">• Level 1• Triage alerts• Proactive Monitoring	<ul style="list-style-type: none">• Level 2• Advanced investigations• Response planning	<ul style="list-style-type: none">• Level 3• Deep dive artifact analysis• Malware analysis	<ul style="list-style-type: none">• Threats Modeling• Track campaigns and threats actors• Optimize and tune threats cases	<ul style="list-style-type: none">• Logs sources maintenance• Systems & software support

Traditional SOC

- Security Information & Events Management (SIEM)
- Collect security events
 - System logs (windows, Linux etc)
 - Security devices logs (proxy, IPS, VPN etc)
 - Network events (netflow, firewalls)
 - Application servers (web, middle-tier etc)
- Threats Correlation Engine



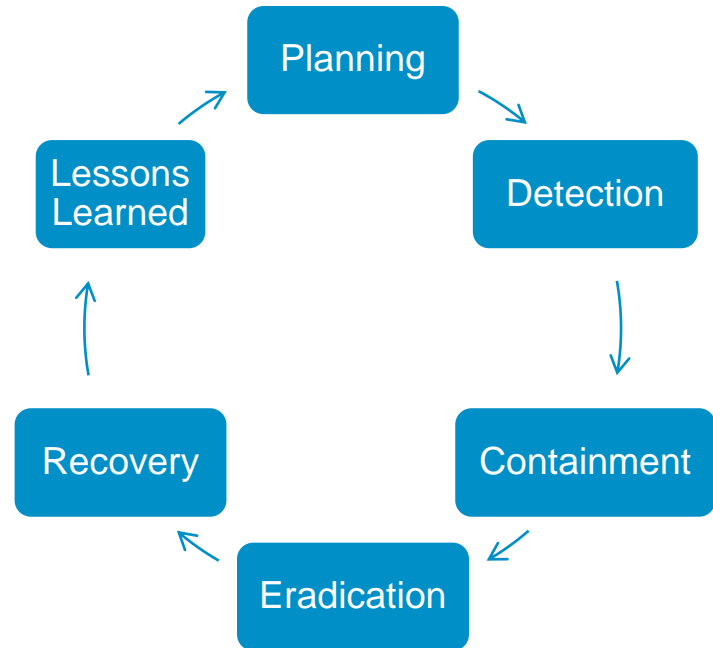
24/7 Monitoring

- Level 1
- Analysts on 24/7 work schedule
- Roles & Responsibilities:
 - Initial triage of security alerts
 - Proactive monitoring
- Skills set:
 - Analytical thinking
 - Good Systems, applications, networks knowledge
 - Well-versed in hackers craft
 - Curious (very important)



Incident Response

- Level 2
- Advanced logs and artifacts analysis
- 3-to-1 L1/L2 ratio is typical
- Maintain Incident Response Plan
 - Frequent cyber incidents drills
- Advanced skills set in intrusion analysis and hackers craft



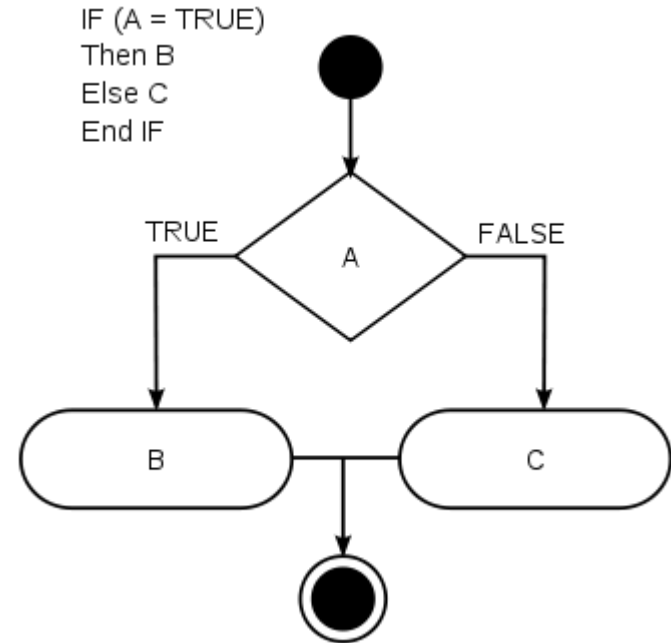
Forensics & Malware Analysis

- Level 3
- Deep-dive analysis of systems artifacts
- Forensic preservation of evidence
 - Chain of custody
- Malware analysis
- Advanced skills in operating systems internals & malware reverse engineering



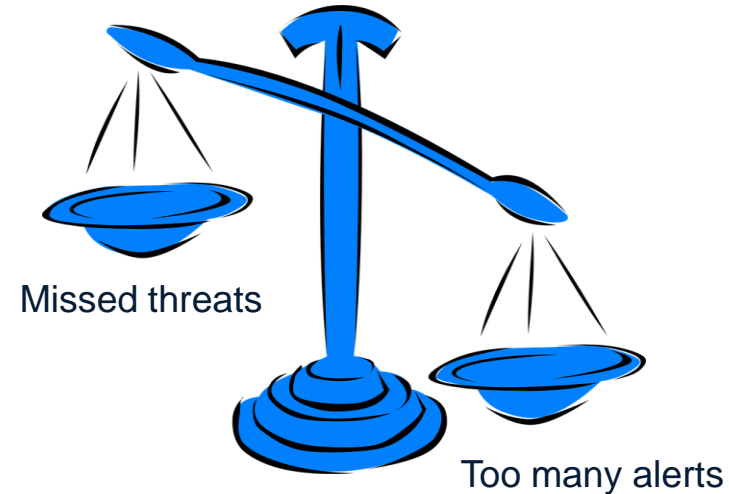
Threats Management

- Threats Modeling
 - Insider & external threats models
 - Threat Case definition
- Threat Case
 - Events Correlation Rules
 - Analytics Reports
- Examples
 - Virus detection and privilege escalation within +/- X minutes
 - Statistical analysis of potentially malicious changes to system configuration



Threats Management

- Must be Risk-Informed & Threats-led
- Balance between security and operations
 - False positives rates
 - Alerts vs. Analytics Reports
- Assets Inventory & classification required
 - Prioritize monitoring for high-value assets
- Continuous visibility enhancements
 - Optimize security events collection for maximum visibility and lowest overhead
 - New logs sources and event types



Systems Support

- Maintain and support monitoring and analytics infrastructure
 - Monitoring servers and agent software
- Maintain Incident Management system
 - KPIs, reporting, workflow management
- Support SOC detection and response systems
 - Forensics infrastructure
 - Network sniffers
 - etc...

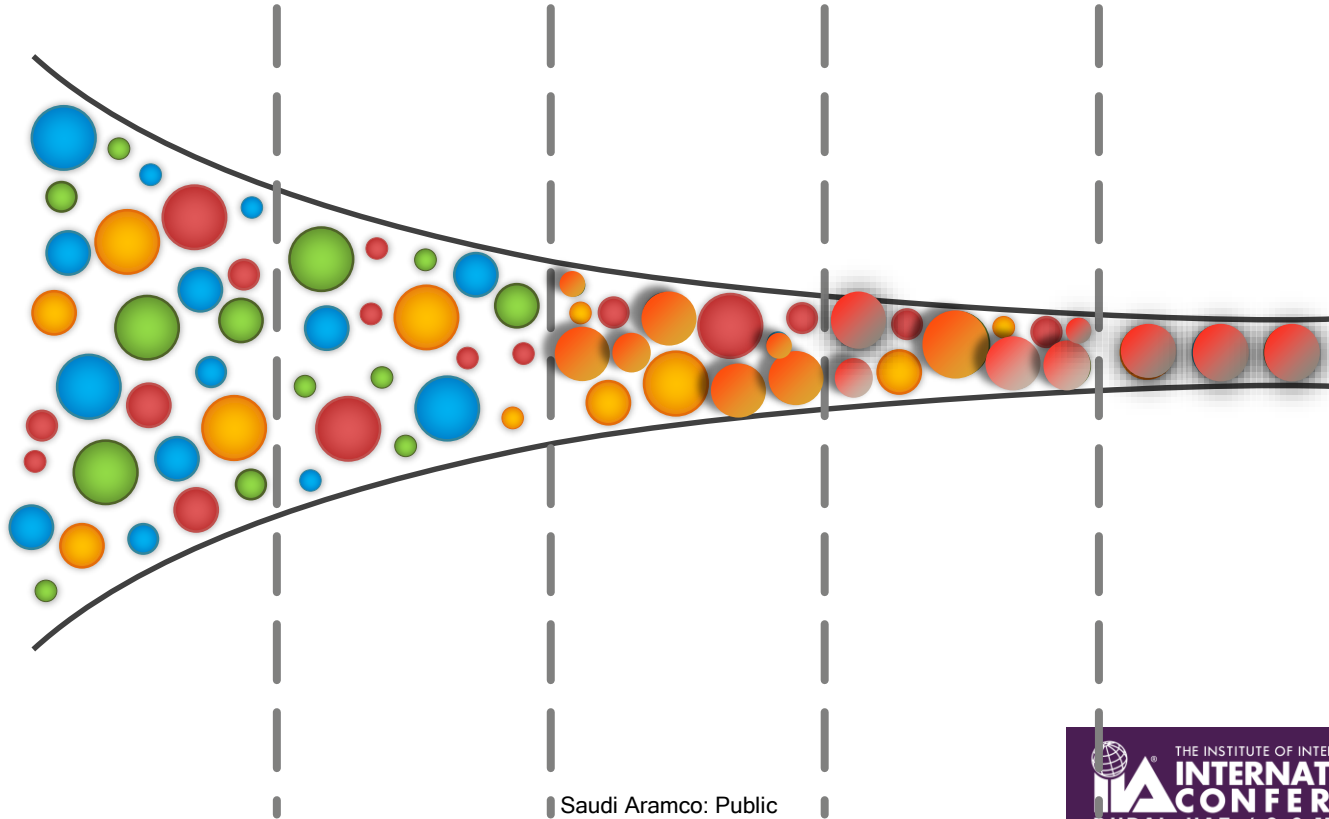


Visibility is crucial

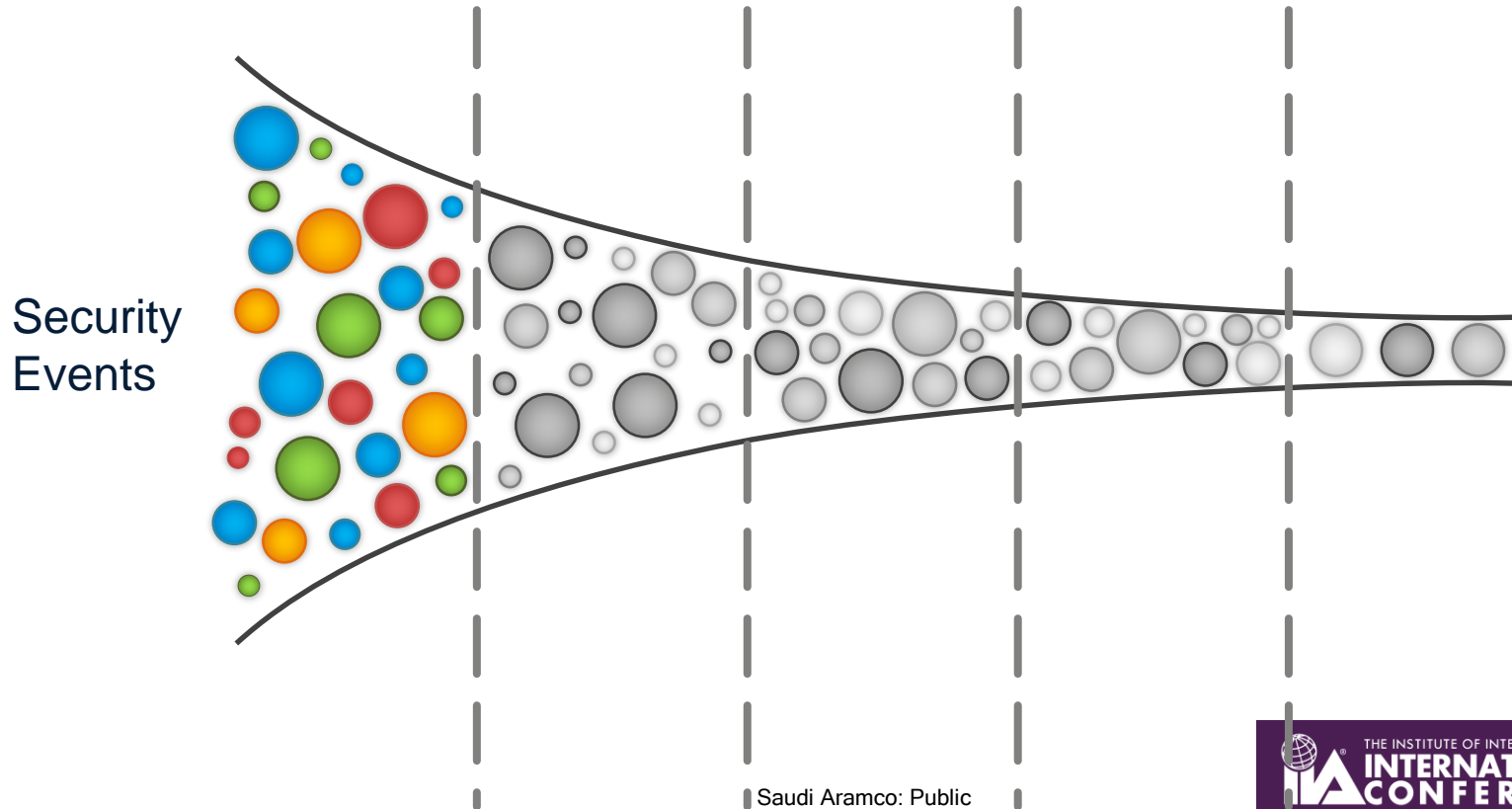
- Capture as many relevant security events types as possible
 - Network
 - Web
 - Email
 - Authentication
 - etc
- Retain for as long as required
 - Legal, Regulations, Policy
- Better threats modeling and response



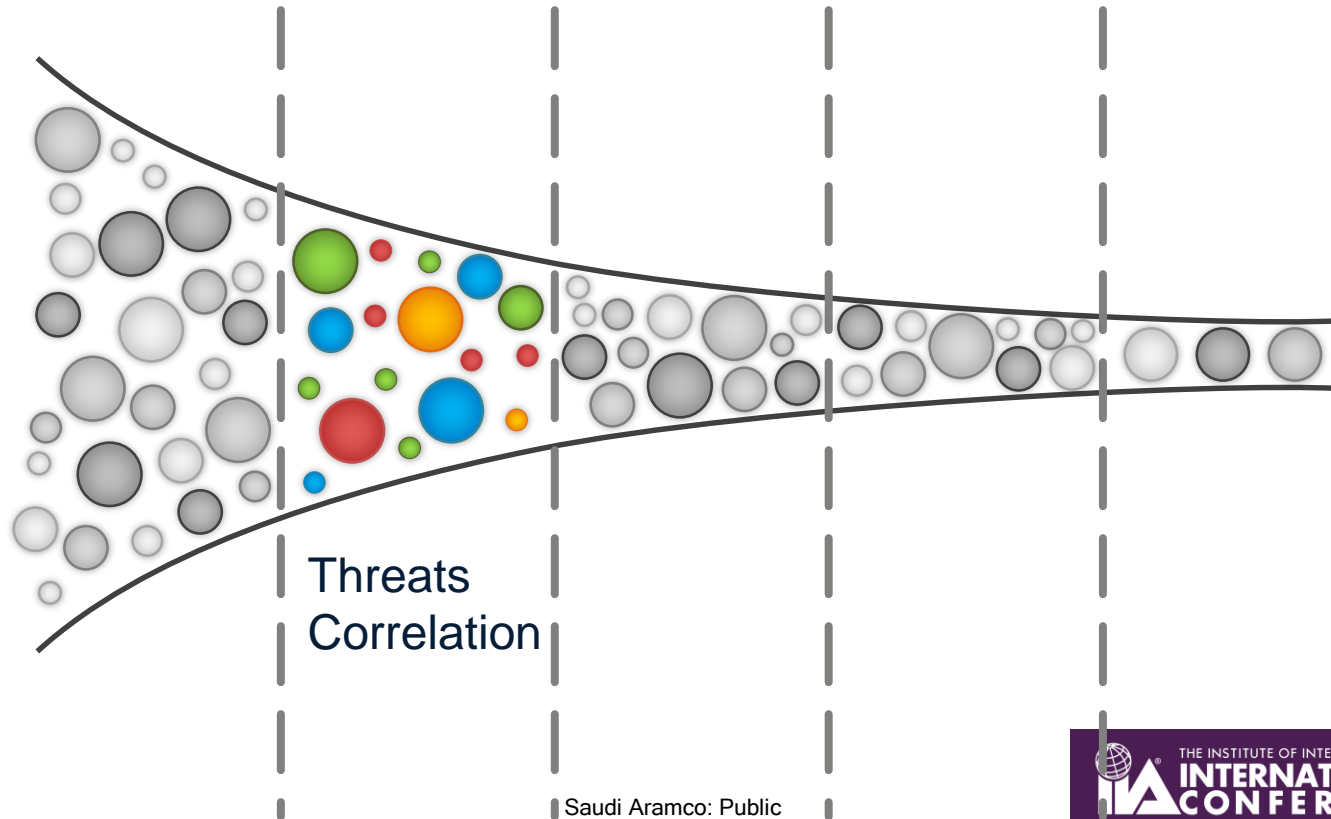
Traditional Security Monitoring



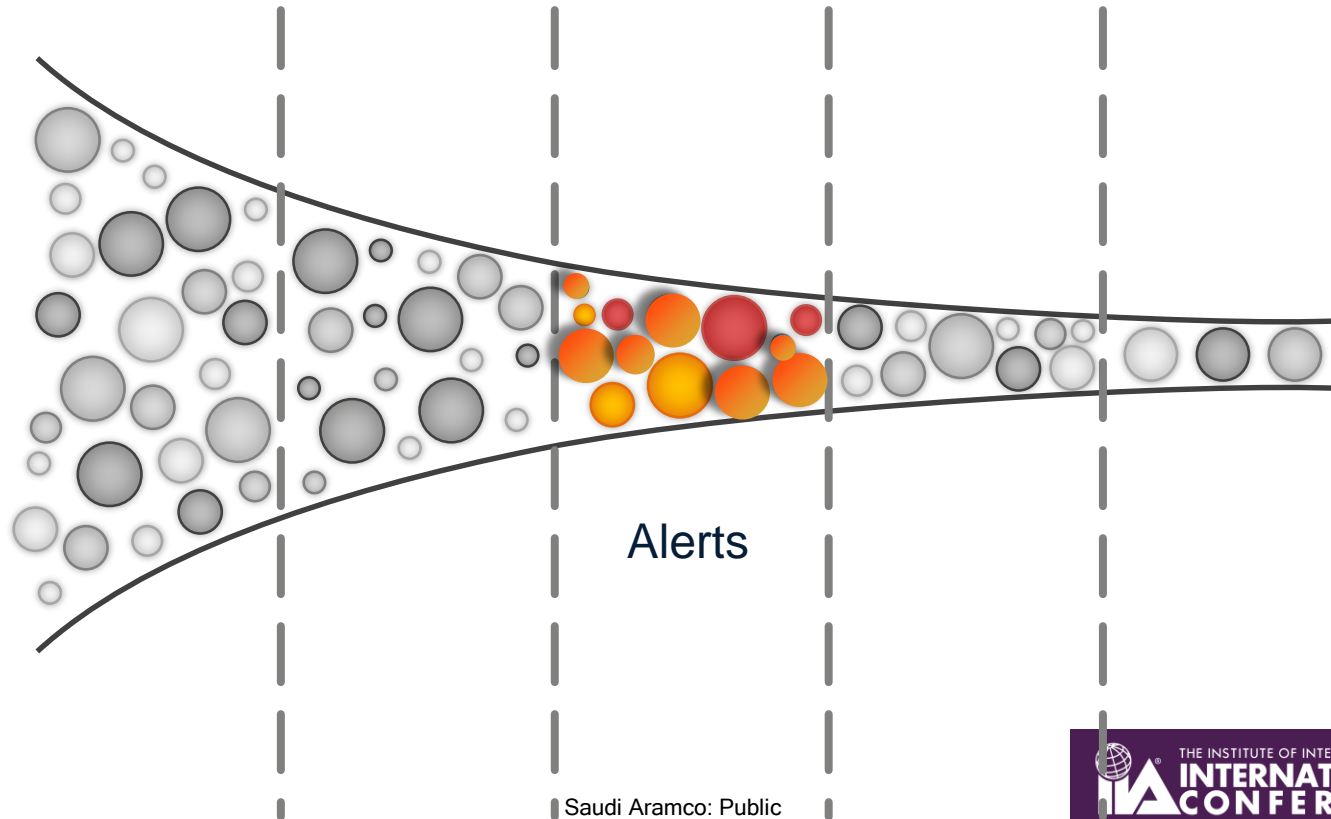
Traditional Security Monitoring



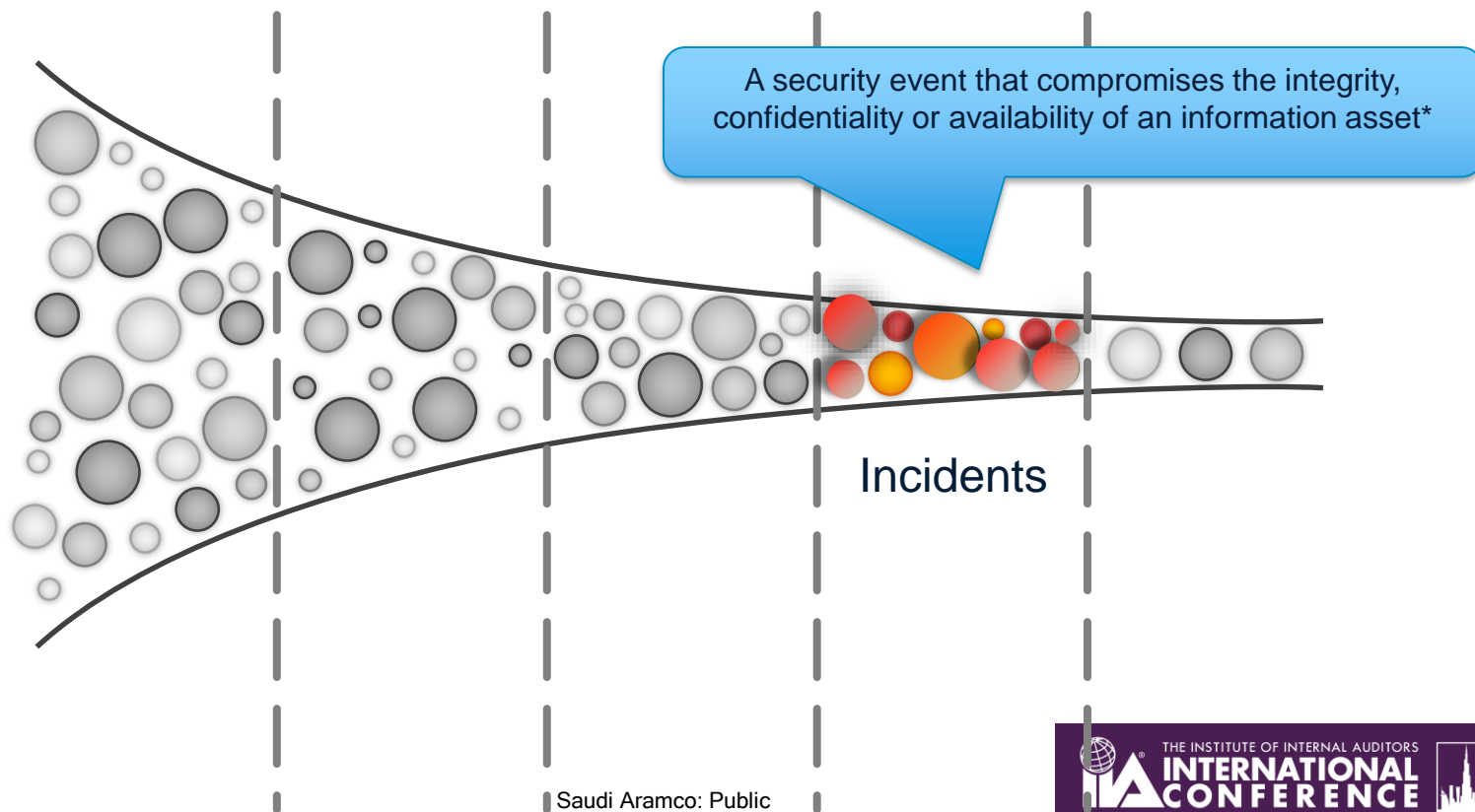
Traditional Security Monitoring



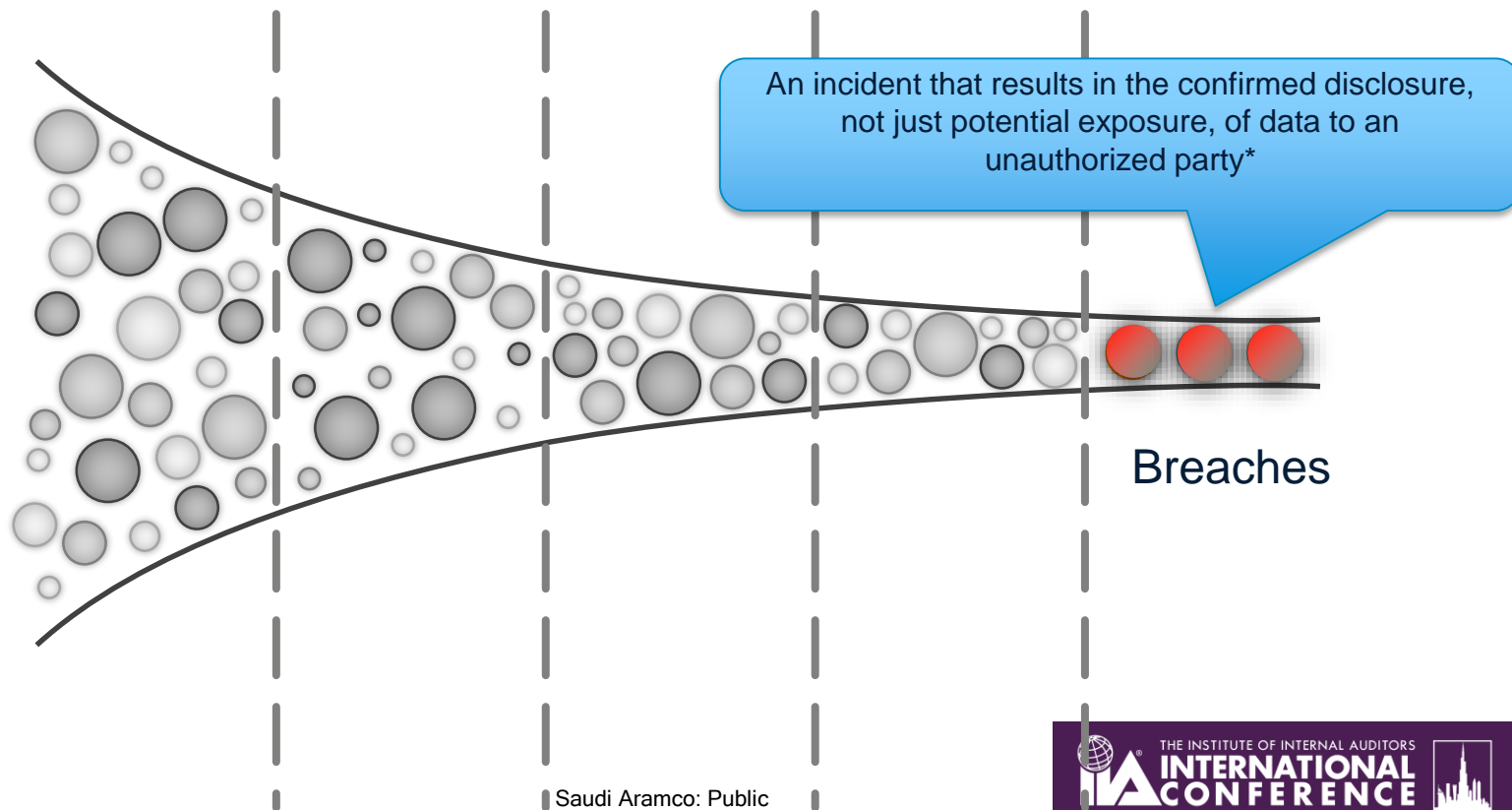
Traditional Security Monitoring



Traditional Security Monitoring



Traditional Security Monitoring



Threats are evolving

- Threats landscape is constantly changing
 - Attackers are more agile and innovative
- How to keep SOC current?
 - Cyber Threats intelligence
 - Situational awareness on latest cyber threats
 - Tools, Tactics & Procedures (TTPs)

**CSI:
CYBER**

Cyber Threats Intelligence

Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries

March 16, 2018 | by [FireEye](#)

Intrusions Focus on the Engineering and Maritime Sector

Since early 2018, FireEye (including our FireEye as a Service (FaaS), Mandiant Consulting, and iSIGHT Intelligence teams) has been tracking an ongoing wave of intrusions targeting engineering and maritime entities, especially those connected to South China Sea issues. The campaign is linked to a group of suspected Chinese cyber espionage actors we have tracked since 2013, dubbed TEMP.Periscope. The group has also been reported as “Leviathan” by other security firms.

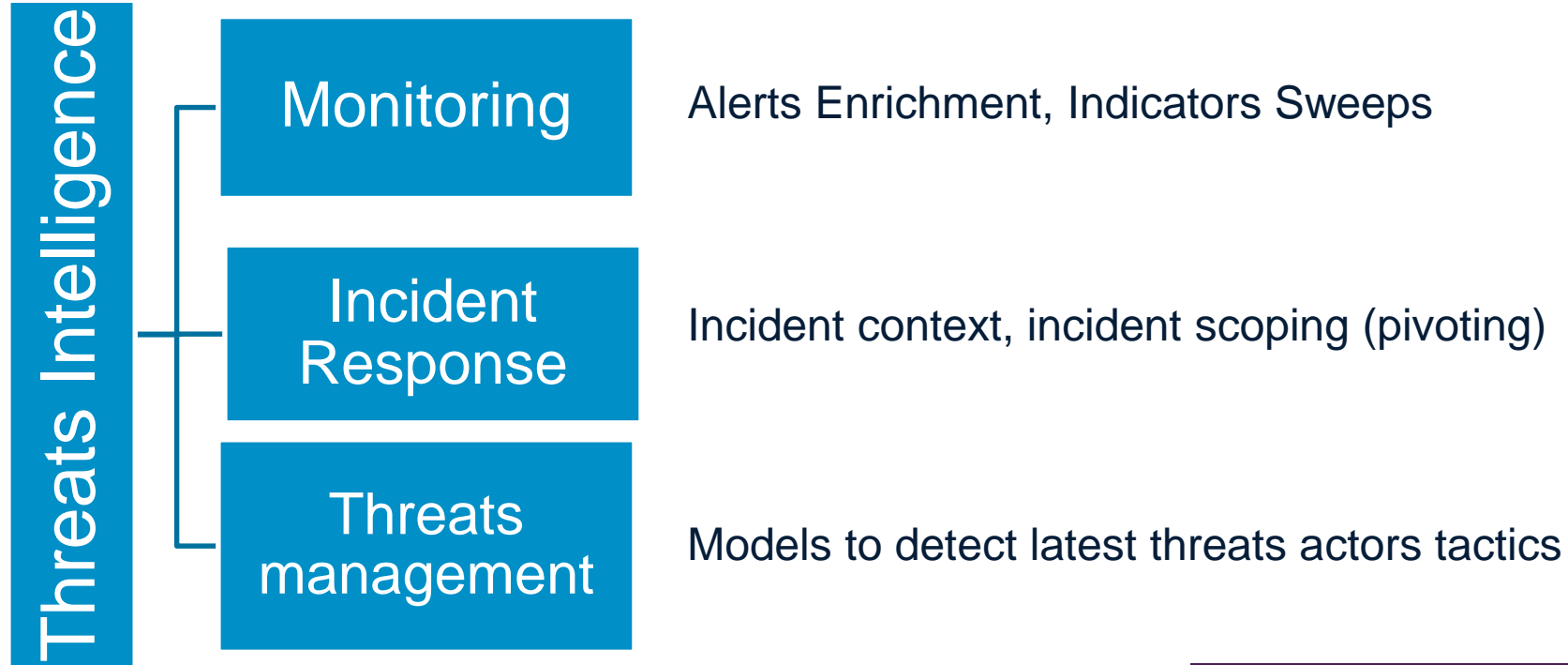
in-tel-li-gence (n): Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

Intelligence-Driven Defense (IDD)

- Basing SOC operations and processes on very keen understanding of cyber threats actors and their tools, tactics, and procedures (TTPs)

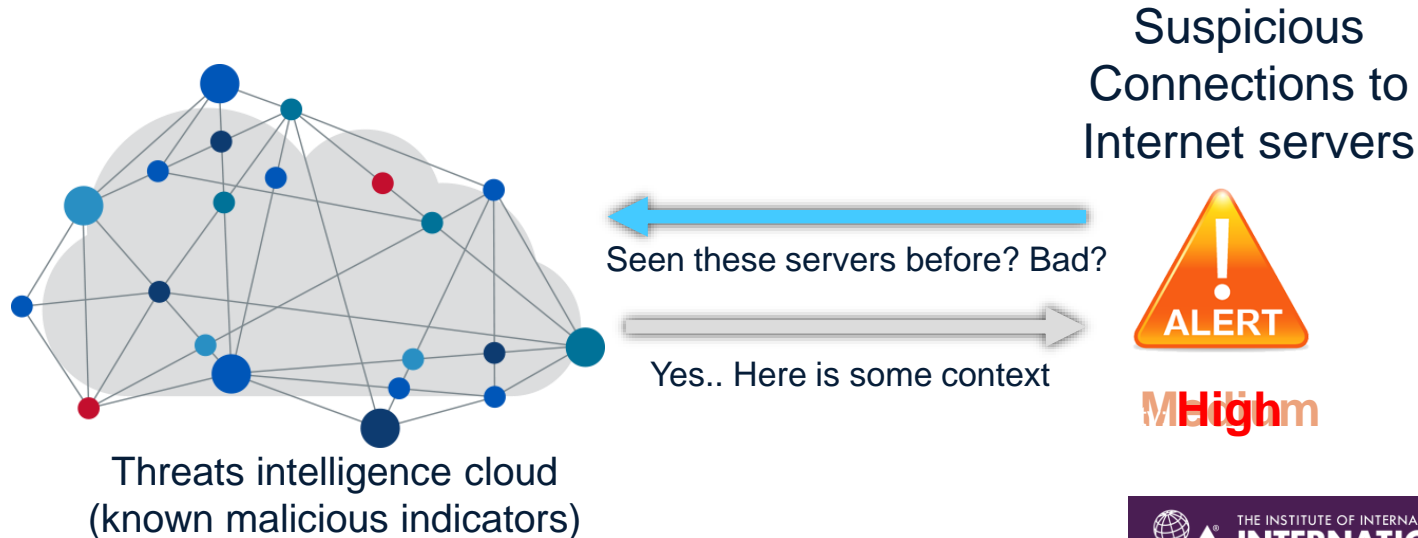


Intelligence-Driven Defense (IDD)



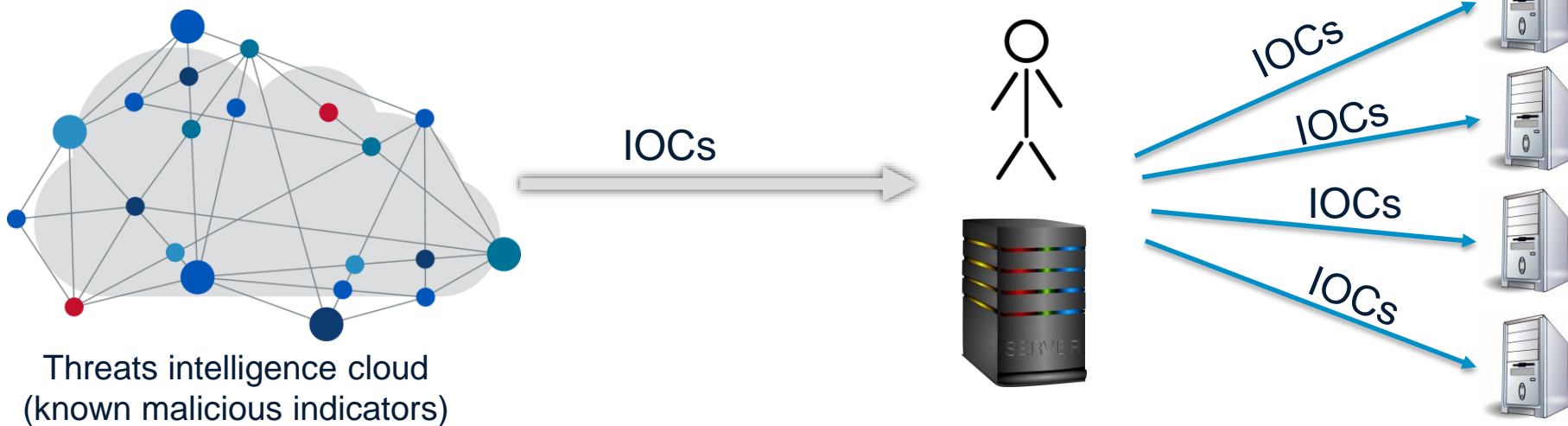
Alerts Enrichment

Leveraging threats intelligence to automatically enrich alerts data with intelligence that aid in quickly triaging and investigating an alert, and boosting severity of alerts with known bad indicators



Indicators of Compromise (IOC) Sweeps

Sweeping network for hits on threats Indicators of Compromise (IOCs); e.g., attackers infrastructure IPs, domain names, tools fingerprints, file names etc



Intel-Driven Incident Response

- Fusing intelligence with information from the incident at hand
 - Better context on the incident
 - Pivot on known attacker tactics and techniques to reveal the incident scope and compromise artifacts
- Example: pivot on attackers
Command & Control (C2) address to find out malware files and system persistence mechanisms



Intel-Driven Threats Modeling

- Create and tune threats cases to detect latest attackers tools, tactics, and procedures (TTPs)
 - Example: Novel ways to exfiltrate data
 - Example: Novel ways to move laterally on the network and maintain persistence
- Model across the Cyber Kill Chain, whenever possible



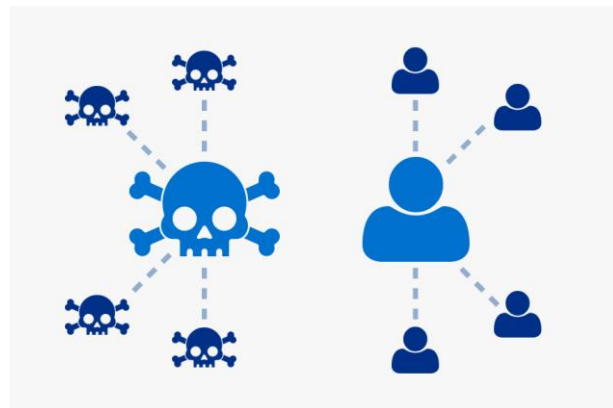
SOC Evolution

- Security Intelligence Center (SIC)
 - Not only consume threats intelligence
 - Produce intelligence
 - Track and anticipate threats actors moves



Threats Intelligence Sharing

- In the best interest of all
- National, industry, and global levels
 - National Cyber Security Centers
 - Information Sharing & Analysis Centers (ISACs)
- Government and private-sector partnerships
 - Protect critical national infrastructure
- Example regional initiatives
 - UAE Banking Federations Intel sharing among member banks

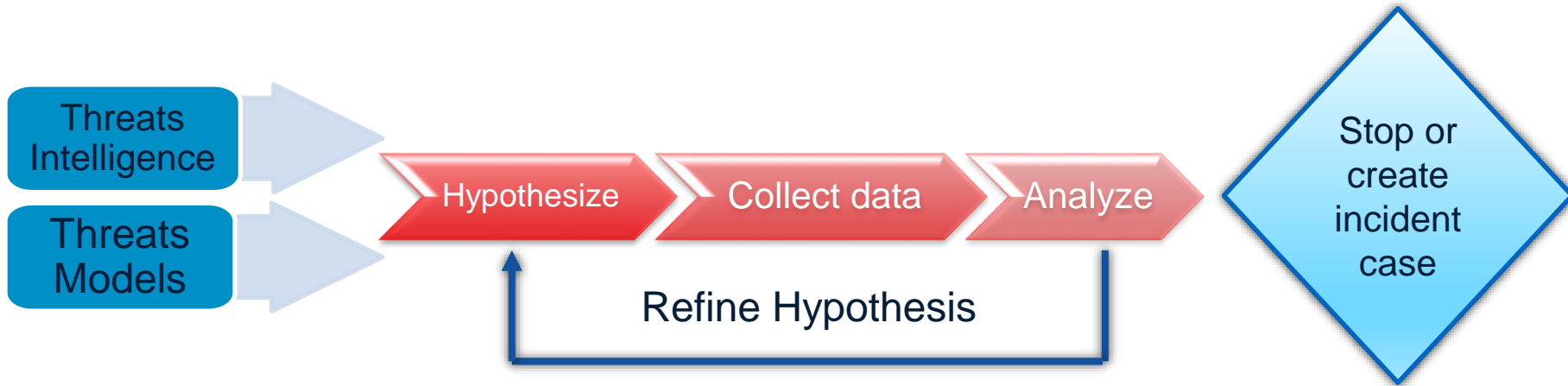


Threats Hunting

- Not all threats can be modeled as static threats detection rules
 - Not waiting for an alert
 - Data-driven
 - Proactively hunting for threats that evade static threats detection rules
 - Hypothesize the network is compromised and validate



Threats Hunting Process



Threats Intelligence: Situational Awareness on cyber threats actors, and their Tools, Tactics and Procedures (TTPs)

Threats Models: Internal models of potential cyber threats (e.g., insider threats, data exfiltration by external attackers)

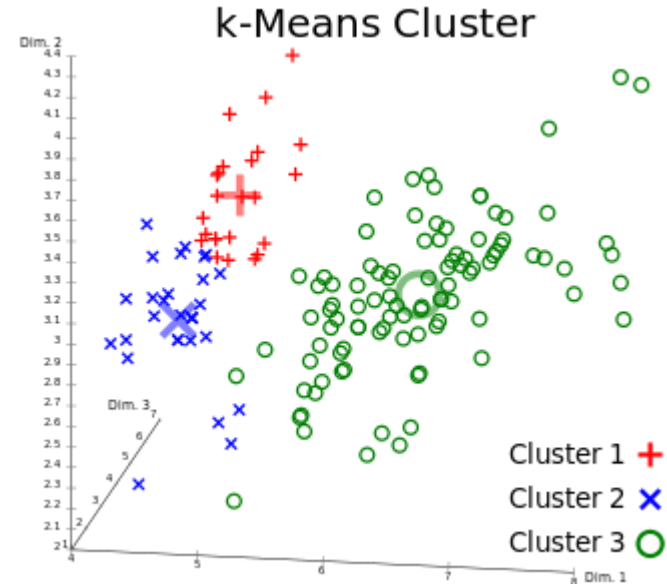
Big Data & Machine Learning

- Typical enterprise IT network generates billions of security events per day
 - Static threats correlation rules don't keep state (i.e. no memory)
 - Seen before? Normal? Abnormal?
 - Overhead to maintain huge list of exceptions of known normal
 - Known unknown threats
 - Unknown unknown threats
 - Input into Threat Hunting process



Big Data & Machine Learning

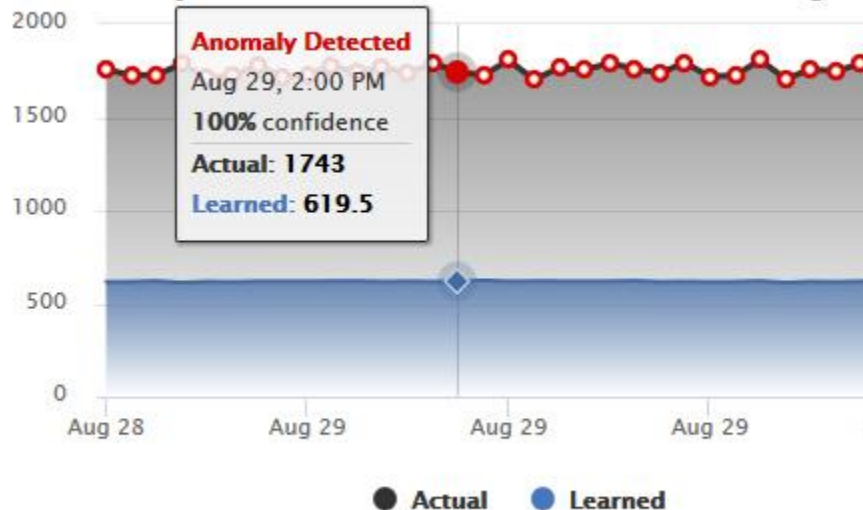
- Big data analytics and machine learning models
 - Reduce false positives by incorporating learning about what's normal
 - Detect anomalies and deviations from normal
- User Behavior & Analytics
 - Machine Learning models to learn normal user behavior
 - Detect insider threats



User Behavior Analytics (UBA)

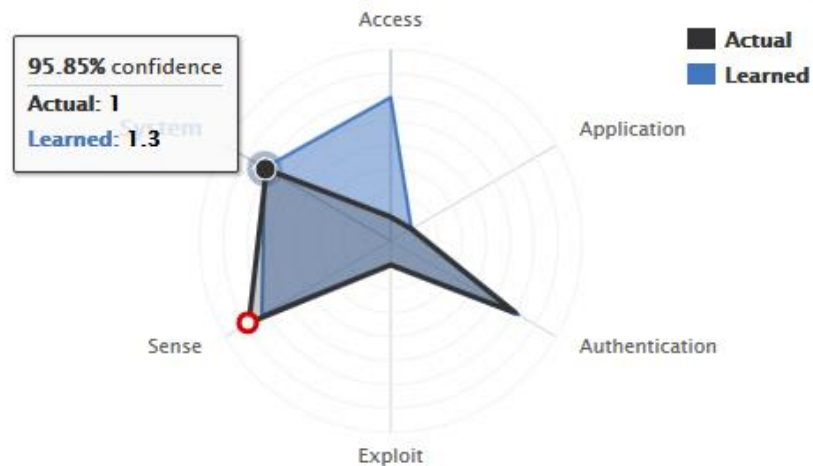
Total Activity

Aug 29 - Aug 30



User Activity by Category

Feb 24, 13:00

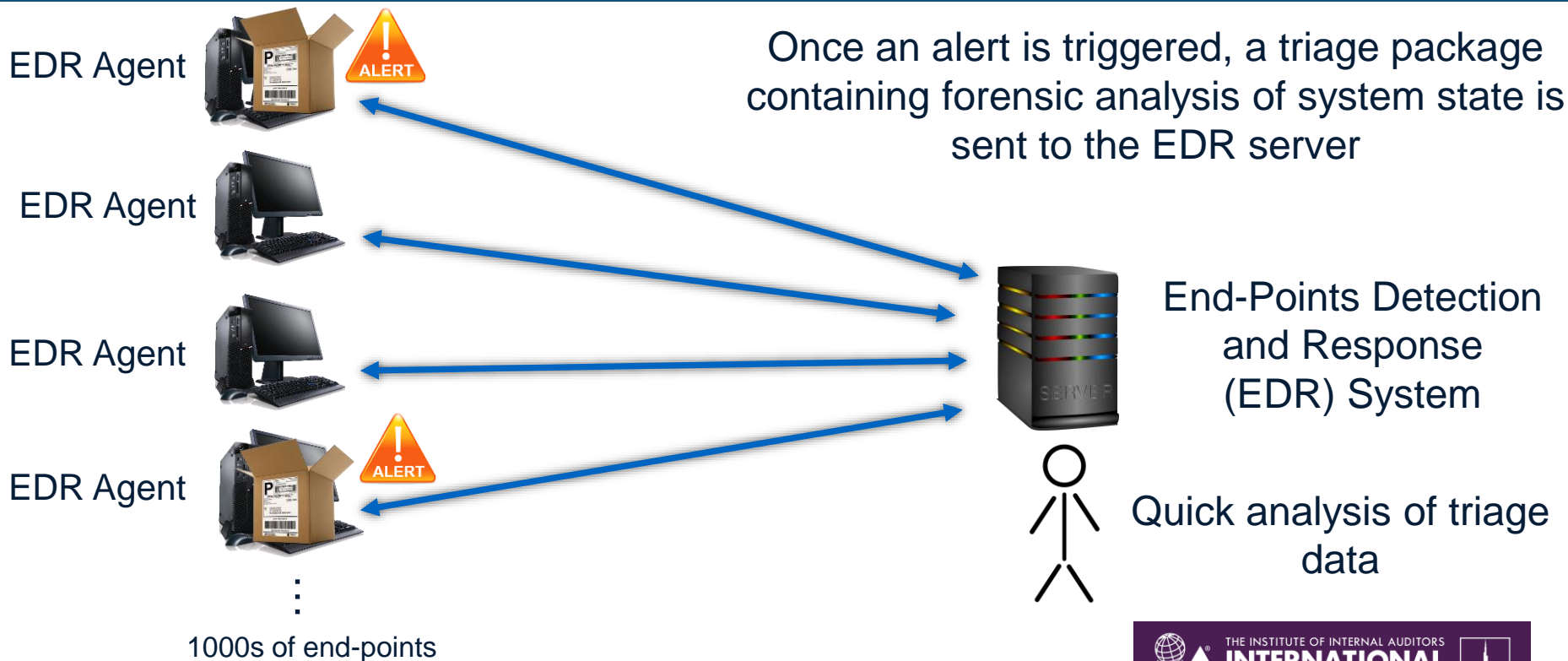


End-Points Detection & Response

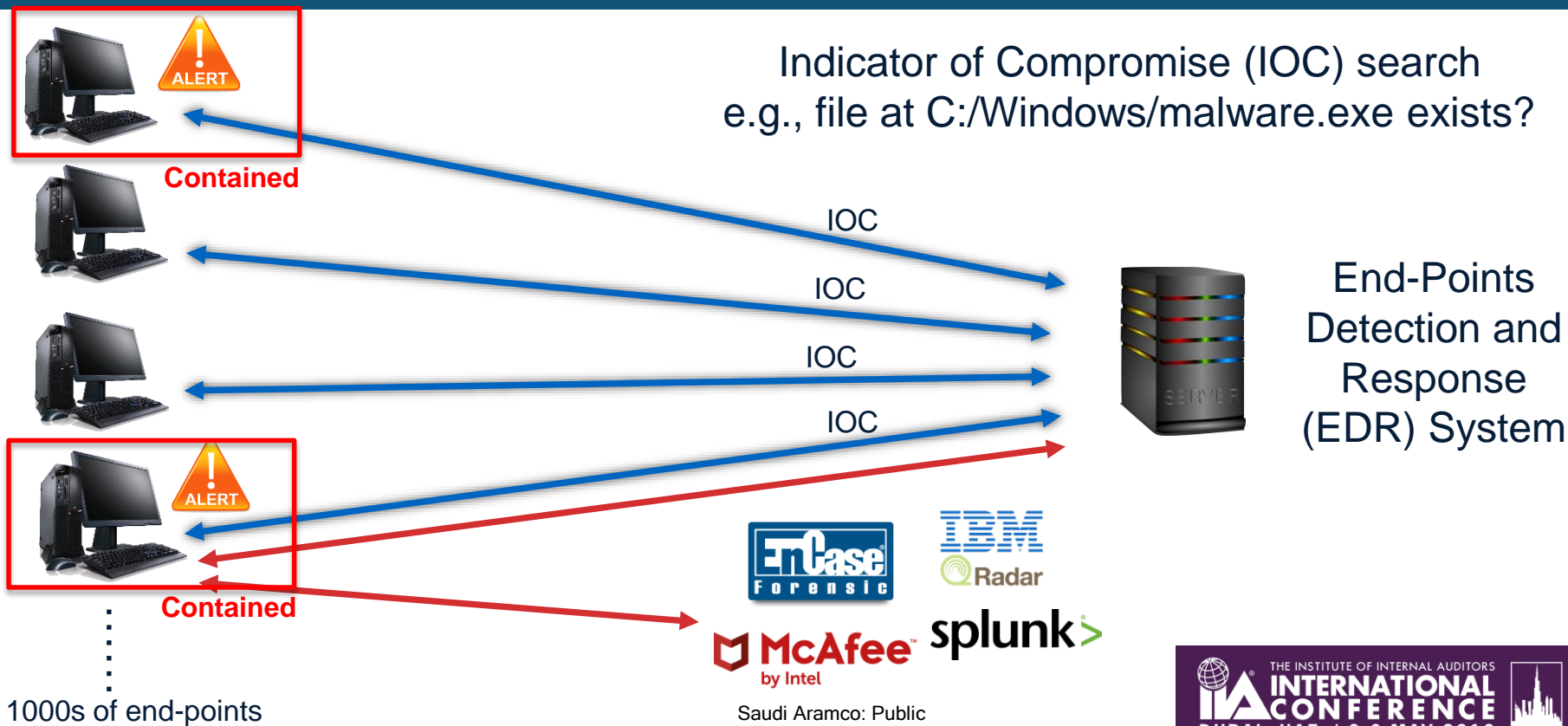
- Visibility into live state of systems (end-points)
 - Current state of system components (e.g. registry, files, running programs, system kernel etc)
 - Behavioral monitoring
- Addresses visibility issues with security events
 - Visibility bound by security events
 - Limited behavioral threats detection
- Enables incident response scaling



EDR: Cyber Forensics at Scale



EDR: Incident Response at Scale



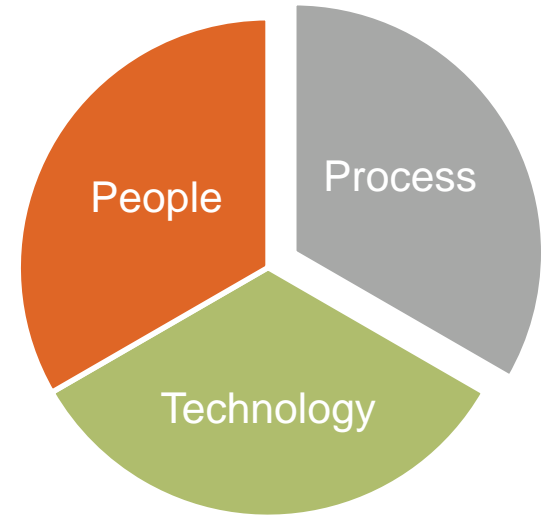
Network Forensics

- Visibility at the network level
- Intercept and capture network traffic from key points
- Extract forensic evidence from network data
- Reconstruct attacker activity
- Analyze Command & Control (C2) traffic



SOC Management

- Effective SOC management is key
 - A lot is at stake
- Operations oversight
- Standard Operating Procedures
- Maturity & Capability Enhancements
 - NIST Cyber Security Framework
 - Capability Maturity Model Integration (CMMI)
- Key Performance Indicators (KPIs)
 - Time-to-detect, response-time, resolution-time, downtime, etc
 - Compromise Vectors Trends: phishing, web, etc



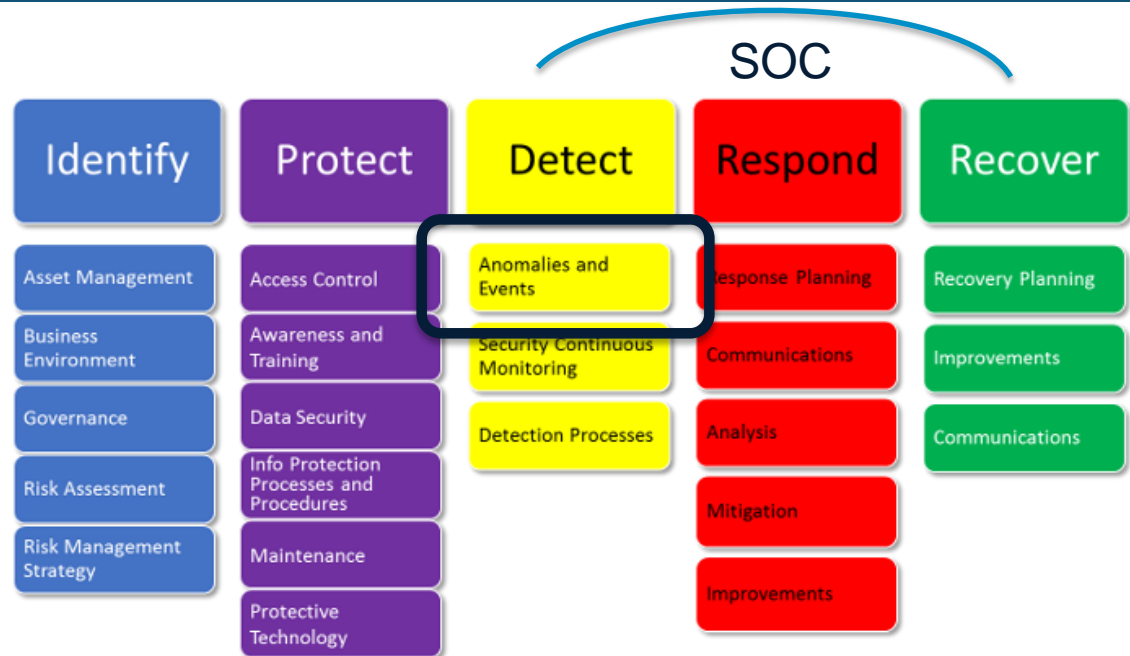
SOC Management

- Track incidents by kill chain phase



- Measure effectiveness of protection controls:
 - Anti-malware software
 - Firewall policies
 - Intrusion Prevention System (IPS) policies
 - Systems hardening levels
 - Phishing awareness campaigns
 - etc..

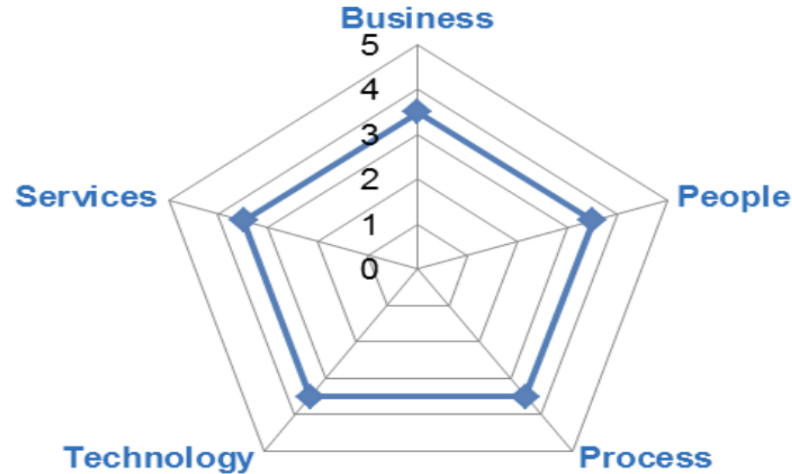
NIST Cyber Security Framework



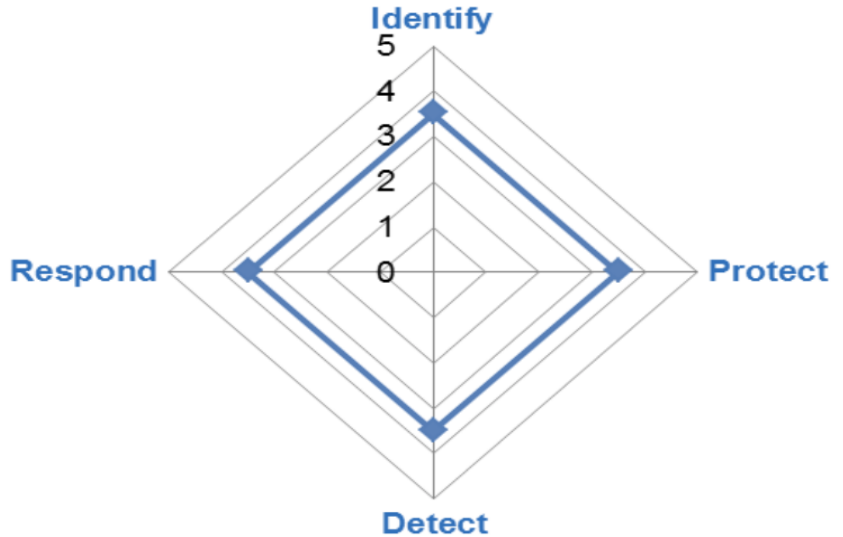
NIST Cyber Security Framework

Function	Category	Subcategory	References
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	<ul style="list-style-type: none"> • COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4.3.3 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	<ul style="list-style-type: none"> • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	<ul style="list-style-type: none"> • ISA 62443-3-3:2013 SR 6.1 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	<ul style="list-style-type: none"> • COBIT 5 APO12.06 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established	<ul style="list-style-type: none"> • COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.2.3.10 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

SOC Capability Maturity Model (CMM)

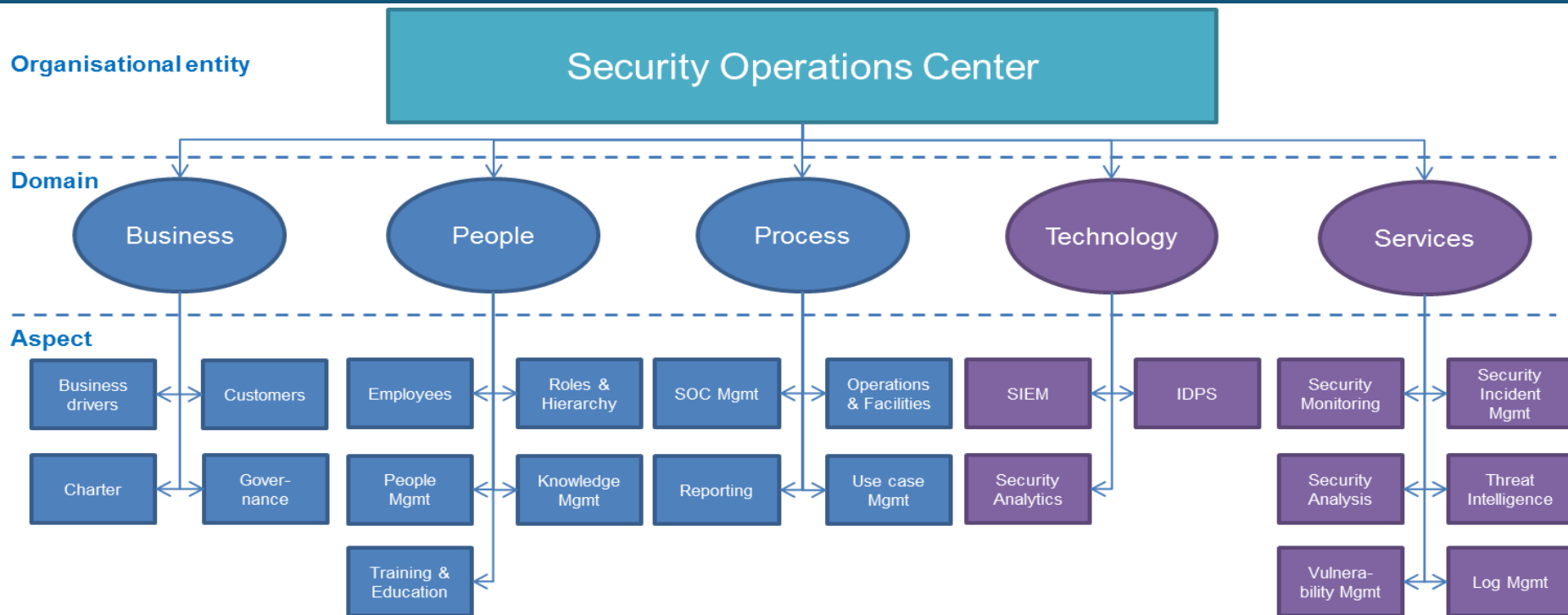


Measure across 5 domains

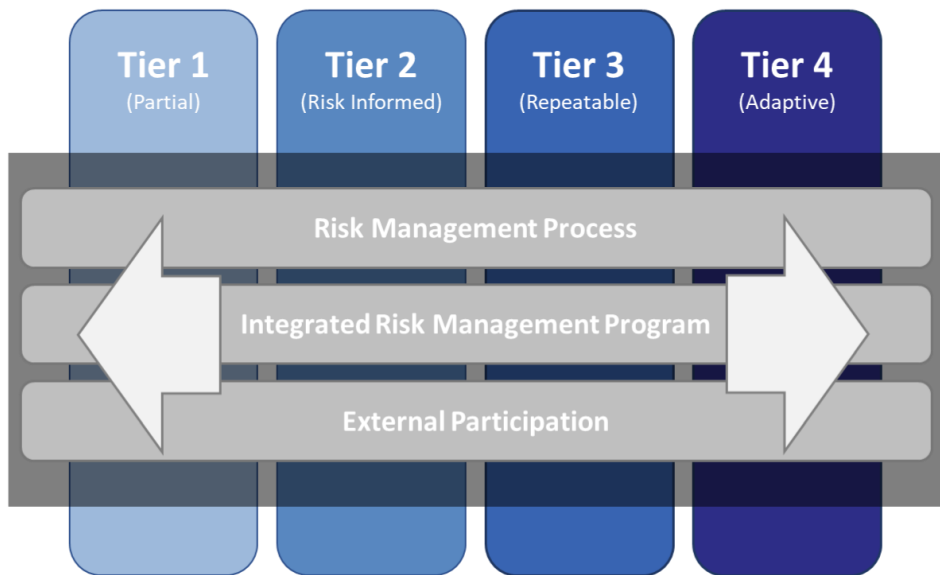


Aligned with NIST
Cybersecurity framework

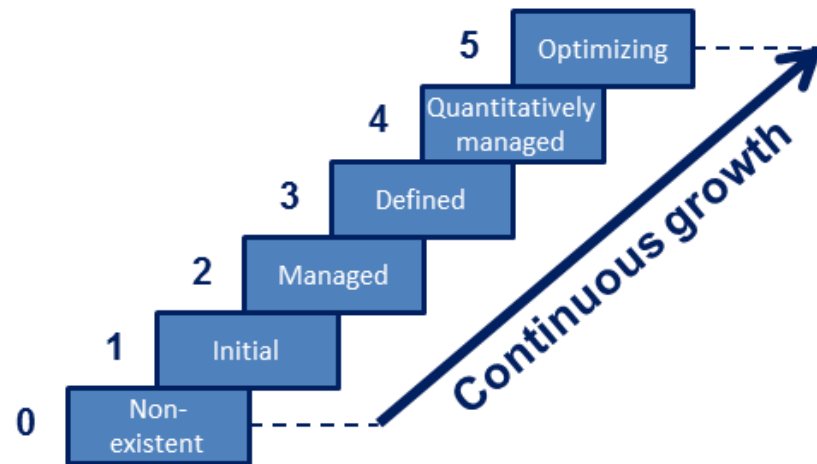
SOC Capability Maturity Model (CMM)



SOC Maturity



NIST CSF Implementation tiers



SOC Capability Maturity Model (CMM)
www.soc-cmm.com

Thank You