

Unified Security Platform

Transforming Security for Enterprise Mobility

James Hamilton

Department Manager, Information Security

Enterprise Mobility

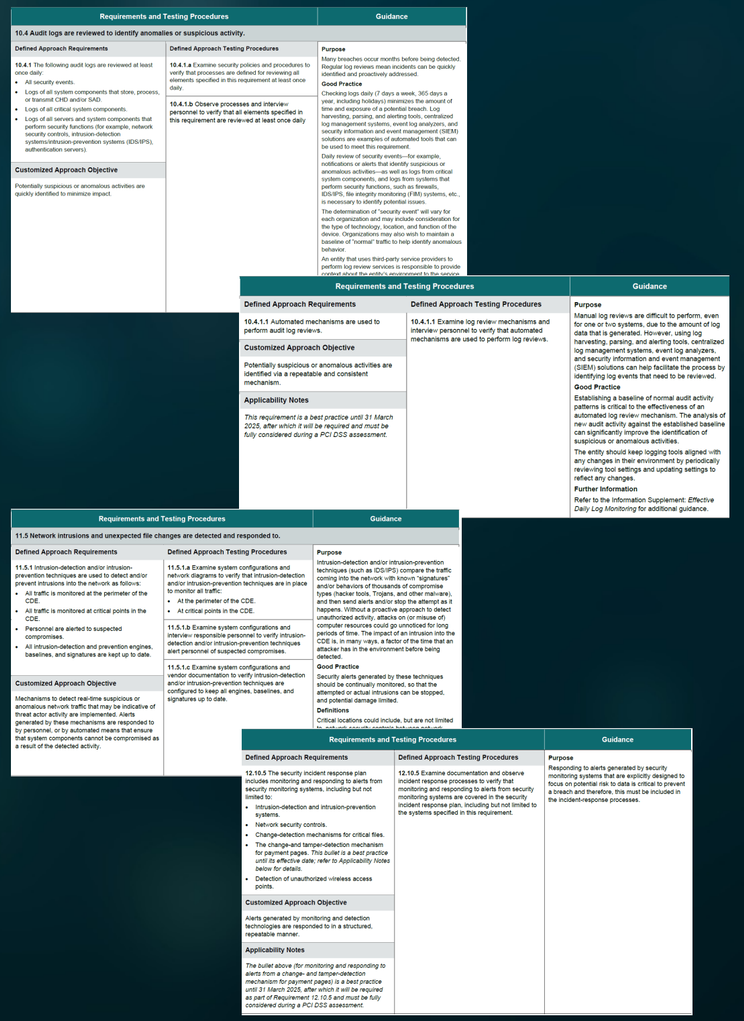
20 YEARS OF SECURING PAYMENT DATA

PCI Security Standards Council



A Security Transformation Journey

PCI DSS has put focus on the importance of logging, log reviews, monitoring and detection, and incident response for some time.



Requirements and Testing Procedures	Guidance
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.	
Defined Approach Requirements **10.4.1** The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers). **Customized Approach Objective** Potentially suspicious or anomalous activities are quickly identified to minimize impact.	**Defined Approach Testing Procedures** **10.4.1.a** Examine security policies and procedures to verify that processes are defined for reviewing all elements specified in this requirement at least once daily. **10.4.1.b** Observe processes and interview personnel to verify that all elements specified in this requirement are reviewed at least once daily.	**Purpose** Many breaches occur months before being detected. Regular log reviews mean incidents can be quickly identified and proactively addressed. **Good Practice** Checking logs daily (7 days a week, 365 days a year, including holidays) minimizes the amount of time and exposure of a potential breach. Log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions are examples of automated tools that can be used to meet this requirement. Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file integrity monitoring (FIM) systems, etc., is necessary to identify potential issues. The determination of "security event" will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of "normal" traffic to help identify anomalous behavior. An entity that uses third-party service providers to perform log review services is responsible to provide evidence about the entity's agreement to the service

Requirements and Testing Procedures	Guidance
Defined Approach Requirements **10.4.1.1** Automated mechanisms are used to perform audit log reviews. **Customized Approach Objective** Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**Defined Approach Testing Procedures** **10.4.1.1** Examine log review mechanisms and interview personnel to verify that automated mechanisms are used to perform log reviews.	**Purpose** Manual log reviews are difficult to perform, even for one or two systems, due to the amount of log data that is generated. However, using log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions can help facilitate the process by identifying log events that need to be reviewed. **Good Practice** Establishing a baseline of normal audit activity patterns is critical to the effectiveness of an automated log review mechanism. The analysis of new audit activity against the established baseline can significantly improve the identification of suspicious or anomalous activities. The entity should keep logging tools aligned with any changes in their environment by periodically reviewing tool settings and updating settings to reflect any changes. **Further Information** Refer to the Information Supplement: *Effective Daily Log Monitoring* for additional guidance.

Requirements and Testing Procedures	Guidance
11.5 Network intrusions and unexpected file changes are detected and responded to.	
Defined Approach Requirements **11.5.1** Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date. **Customized Approach Objective** Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.	**Defined Approach Testing Procedures** **11.5.1.a** Examine system configurations and network diagrams to verify that intrusion-detection and/or intrusion-prevention techniques are in place to monitor all traffic: • At the perimeter of the CDE. • At critical points in the CDE. **11.5.1.b** Examine system configurations and interview responsible personnel to verify intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises. **11.5.1.c** Examine system configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured to keep all engines, baselines, and signatures up to date.	**Purpose** Intrusion-detection and/or intrusion-prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and then send alerts and/or stop the attempt as it happens. Without a proactive approach to detect unauthorized activity, attacks on (or misuse of) computer resources could go unnoticed for long periods of time. The impact of an intrusion into the CDE is, in many ways, a factor of the time that an attacker has in the environment before being detected. **Good Practice** Security alerts generated by these techniques should be continually monitored, so that the attempted or actual intrusions can be stopped, and potential damage limited. **Definitions** Critical locations could include, but are not limited to, web server security settings, key server configu

Requirements and Testing Procedures	Guidance
Defined Approach Requirements **12.10.5** The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Detection of unauthorized wireless access points. **Customized Approach Objective** Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner. **Applicability Notes** *The bullet above (for monitoring and responding to alerts from a change- and tamper-detection mechanism for payment pages) is a best practice until 31 March 2025, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.*	**Defined Approach Testing Procedures** **12.10.5** Examine documentation and observe incident response processes to verify that monitoring and responding to alerts from security monitoring systems are covered in the security incident response plan, including but not limited to the systems specified in this requirement.	**Purpose** Responding to alerts generated by security monitoring systems that are explicitly designed to focus on potential risk to data is critical to prevent a breach and therefore, this must be included in the incident-response processes.

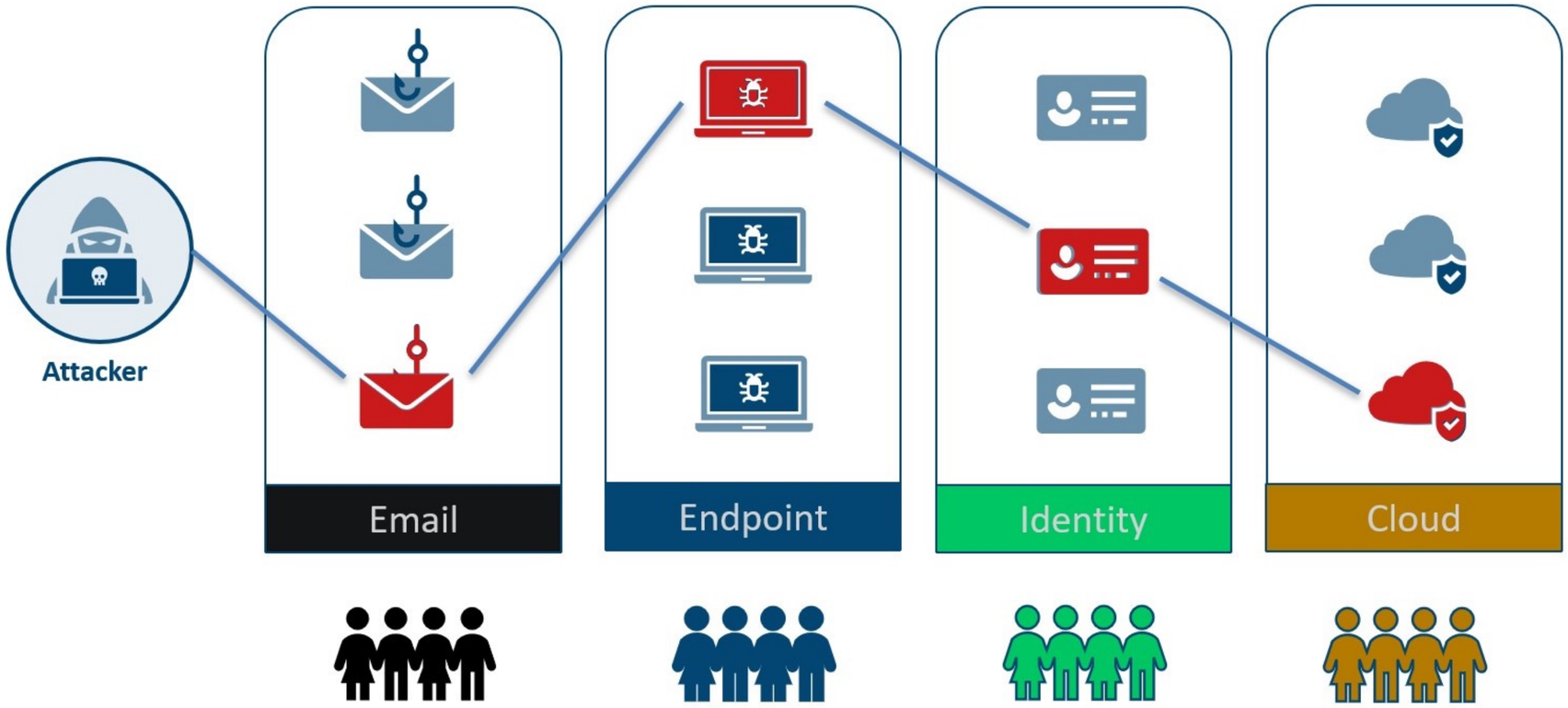
Pleased to share our journey and how investments made toward unification have led to:

- Broader and richer security context faster than ever before
- Analysis efficiency
- Accelerated detection and response

Ultimately strengthening our ability to protect our customers, brand, and business.

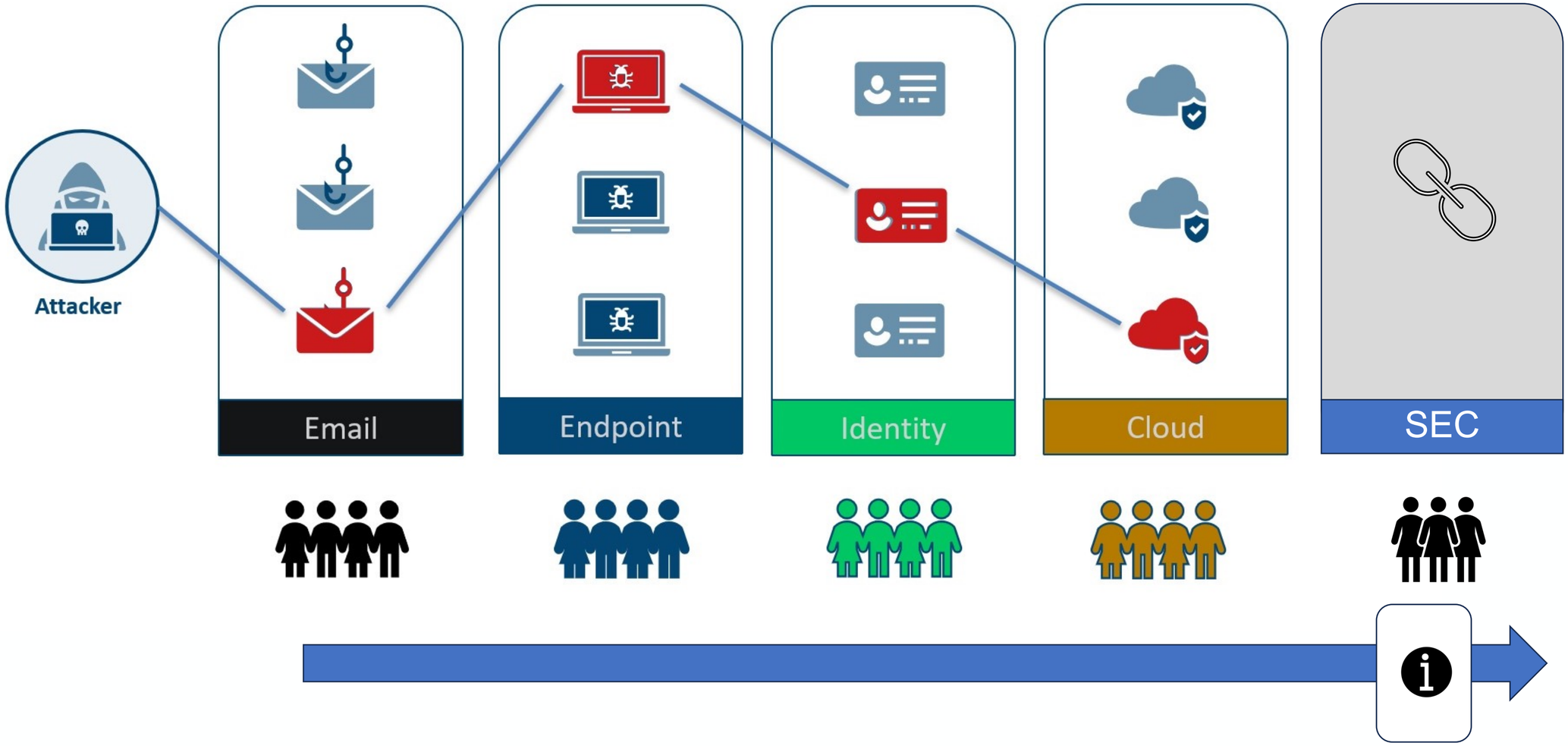
Detect in Silos

Attack in Chains

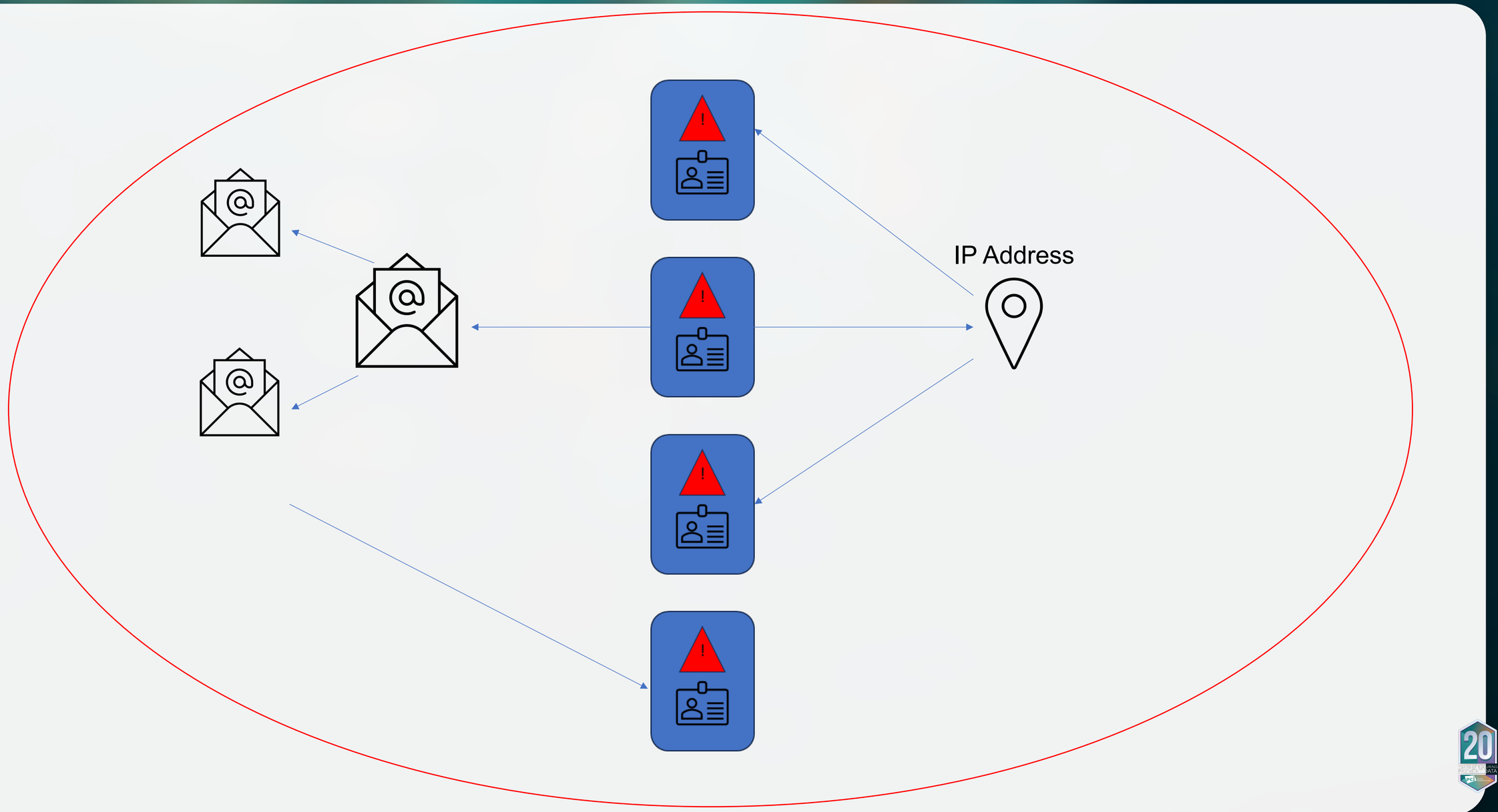


Detect in Silos

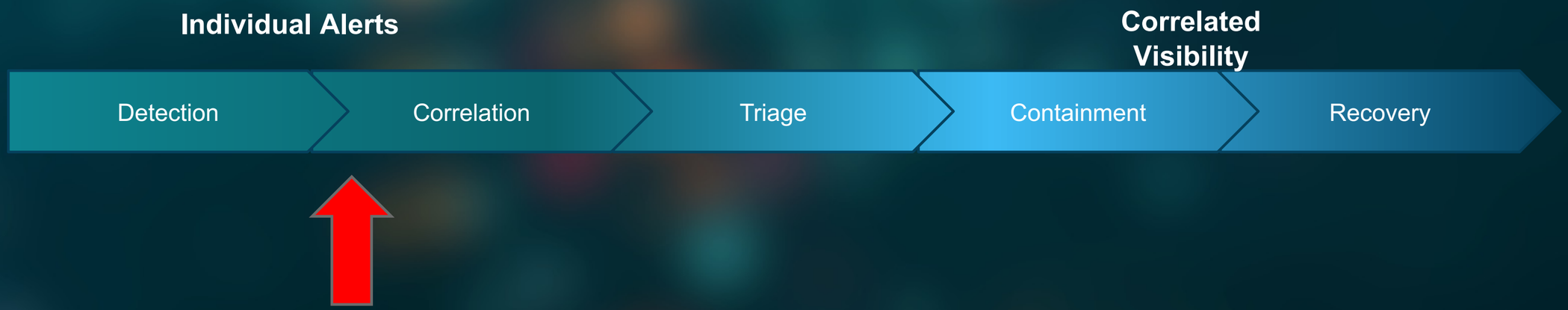
Attack in Chains



Manual Correlation in Action



Unified Security Platform
Focused Capacity



Unified Security Platform

Different than “a single pane of glass”

Objective: Replace existing security stack (best of breed) with a single ecosystem:



- **Correlated Threat Visibility**
- **Faster Mean Time to Contain**
- **Faster Mean Time to Triage**
- **Strategic Security Solution**

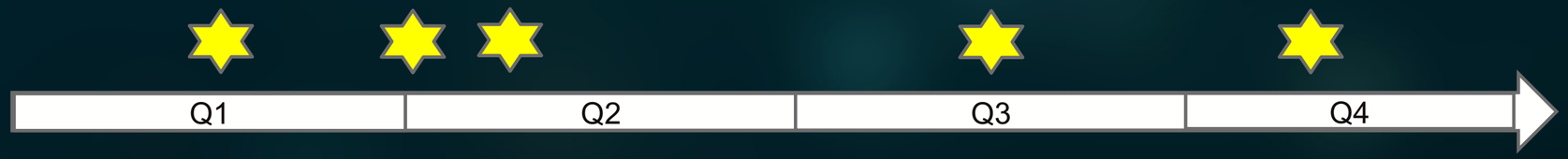
Outcome: Transformation of individuals, teams, processes, AND technology

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Unified Security Platform (USP)

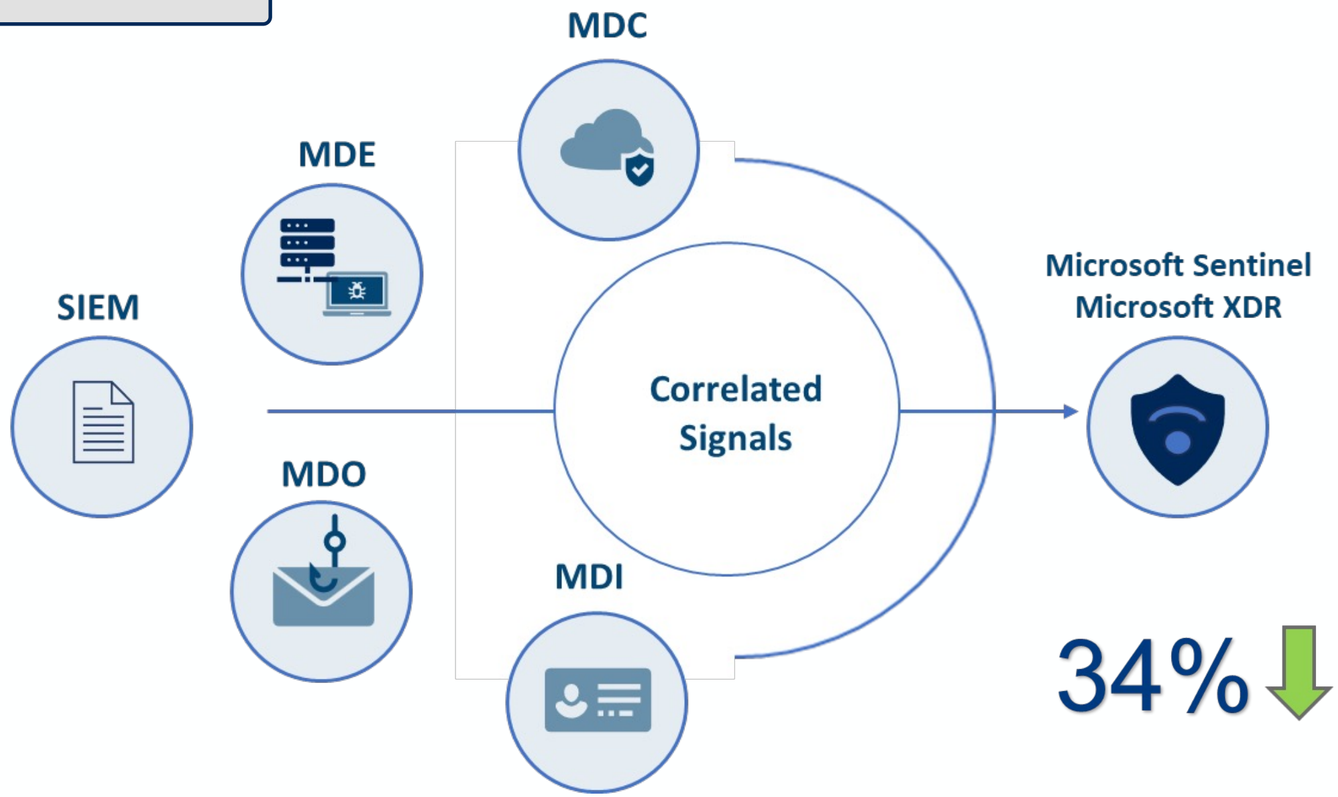
Full Scope-MVP

Capability	Legacy Solution	Replacement Solution
SIEM-Custom Alerts	Splunk ES	Sentinel
Cloud Security	Prisma Cloud CSPM	Defender for Cloud
Identity Threat Detection	Exabeam	Defender for Identity
Endpoint D&R	Cortex XDR	Defender for Endpoint
Email Security	Trend Scan Mail	Defender for Office 365
Data Loss Prevention	Symantec DLP	Purview

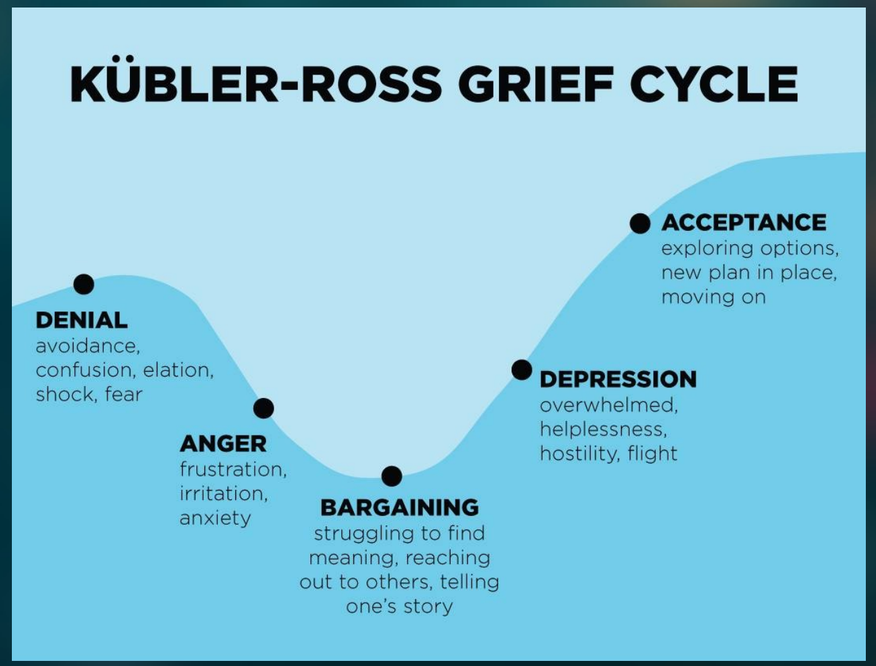


Unified Security Platform

Correlated Threat Visibility



Team Acceptance



Team Grief: Attitude ranged from ***DENIAL*** to ***BARGAINING***

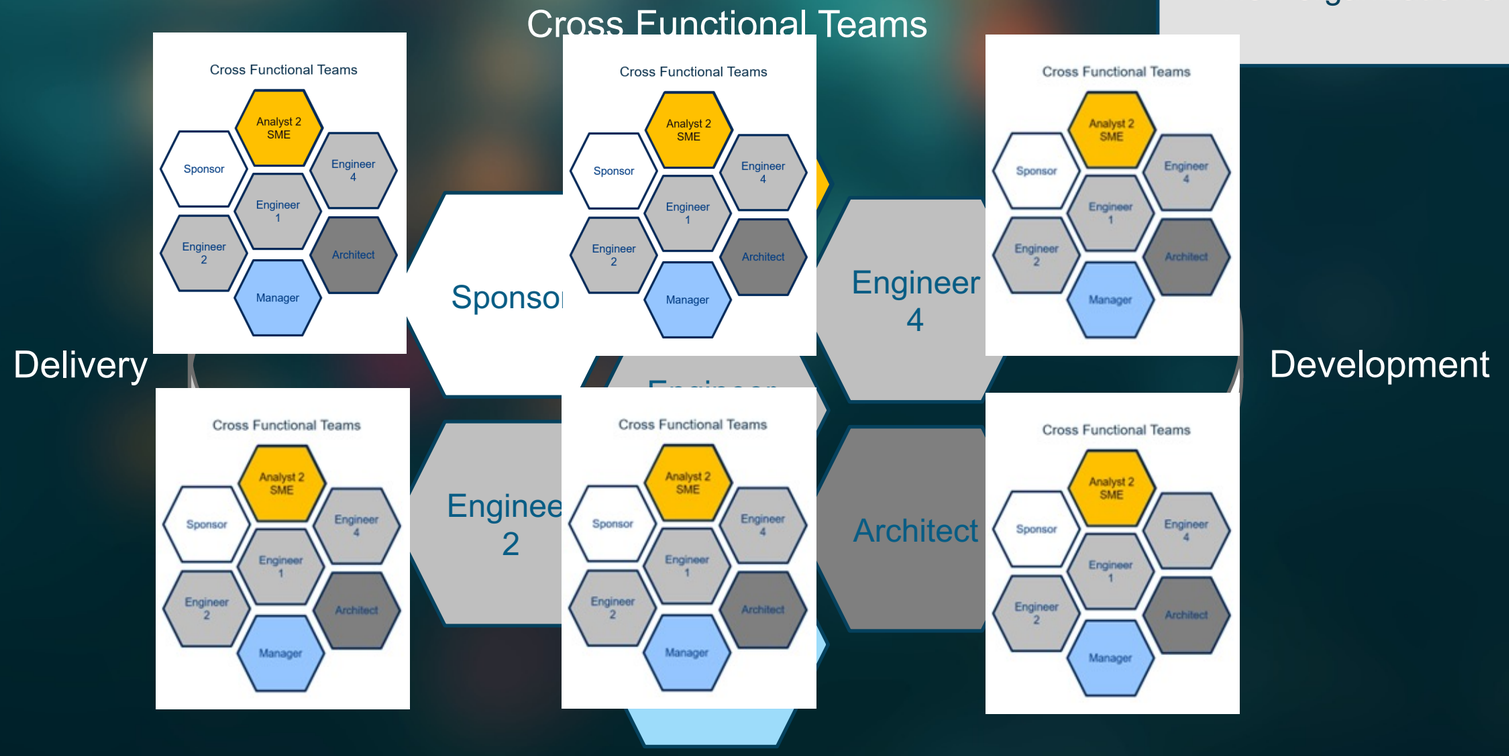
Our Change Approach

- **Rallied the innovators** and early adopters
- **Directly asked the team** about the resistance
- **Communicated the vision-**Turning Point!
- **Immersed the team** in the program

Unified Security Platform
People Focus

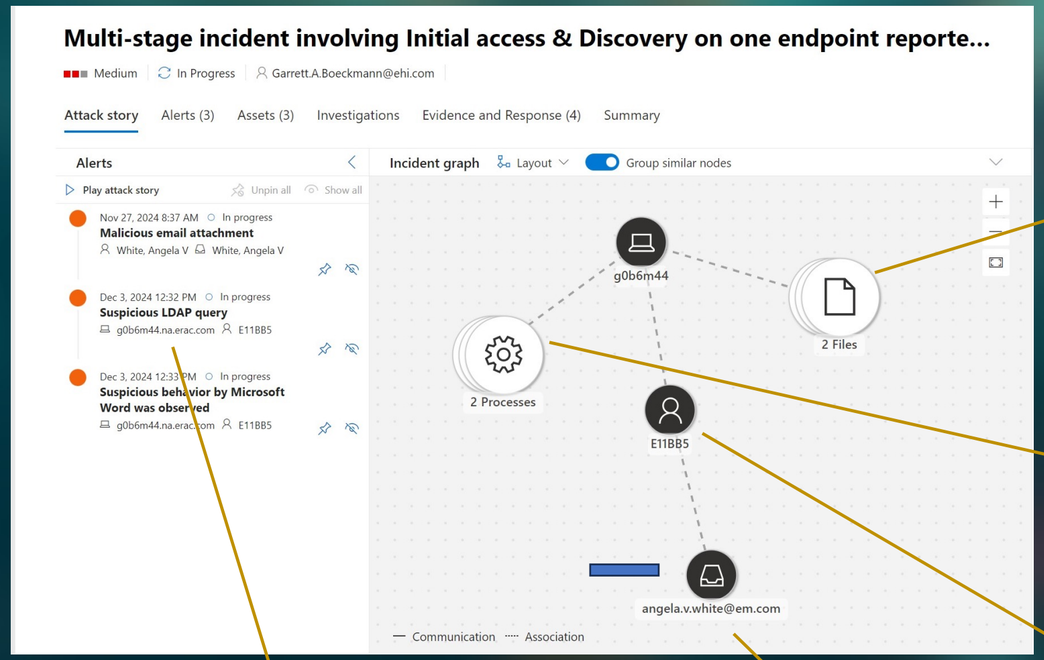
In-Department Delivery

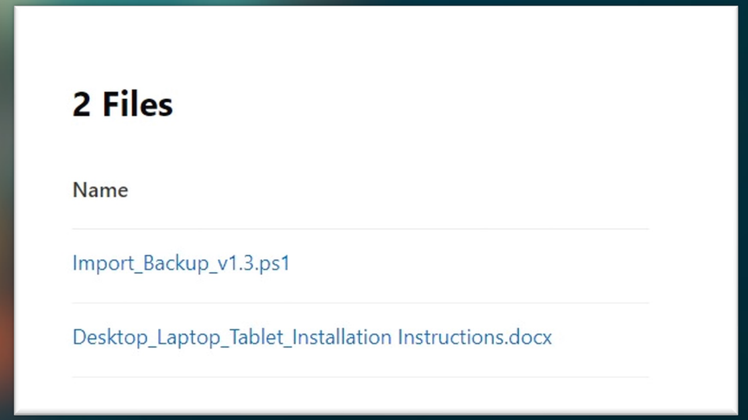
- Created Excitement and Enthusiasm
- 90 new processes and procedures
- 1000 hours of USP training
- New organization and mindset

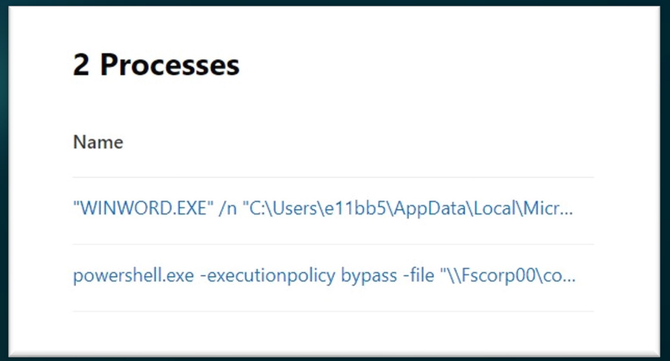


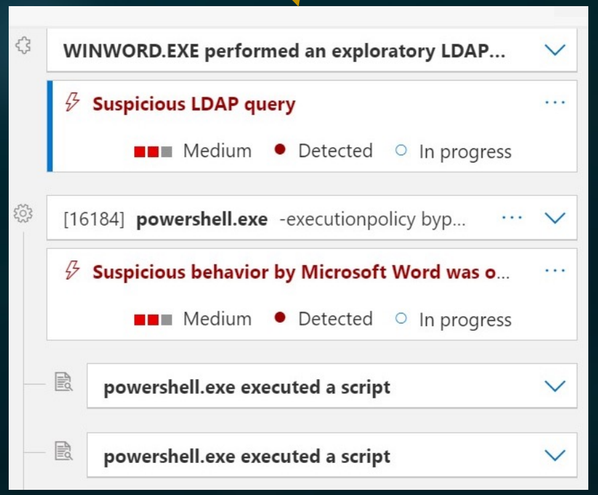
Technical Leadership Team

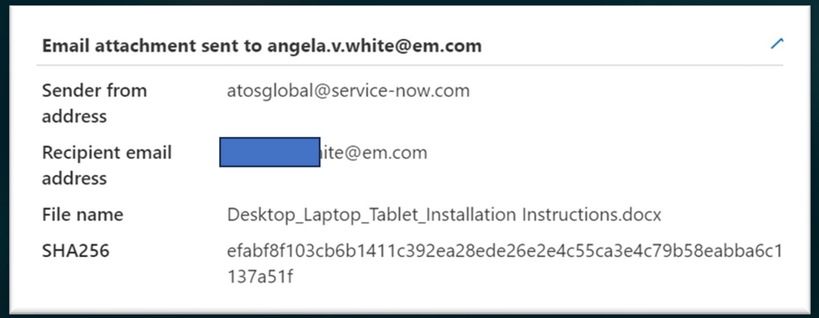
Correlation in Action

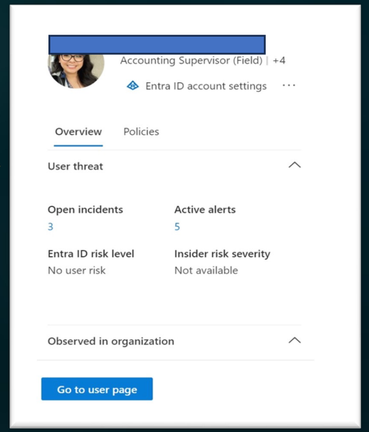




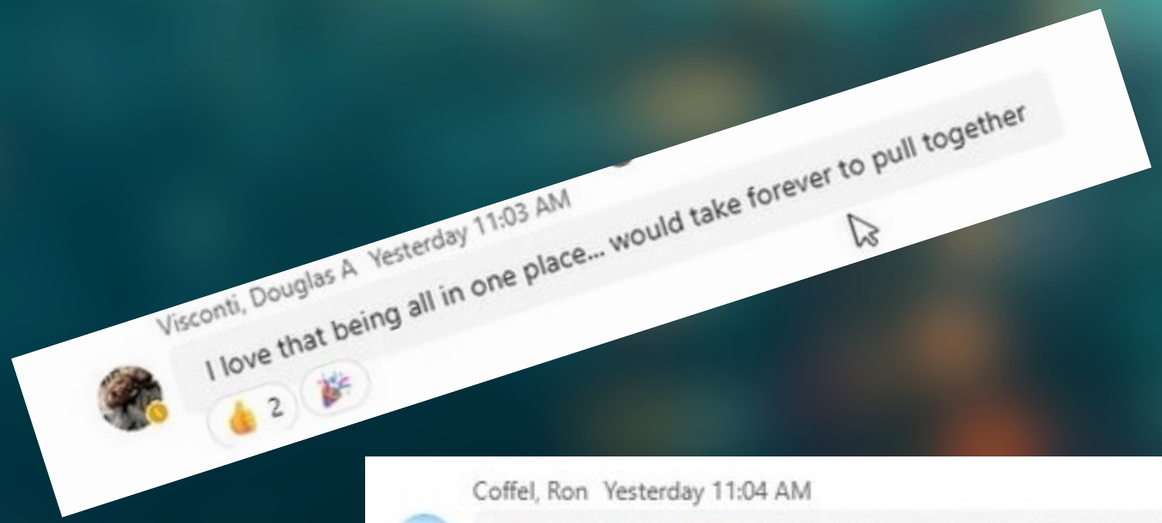


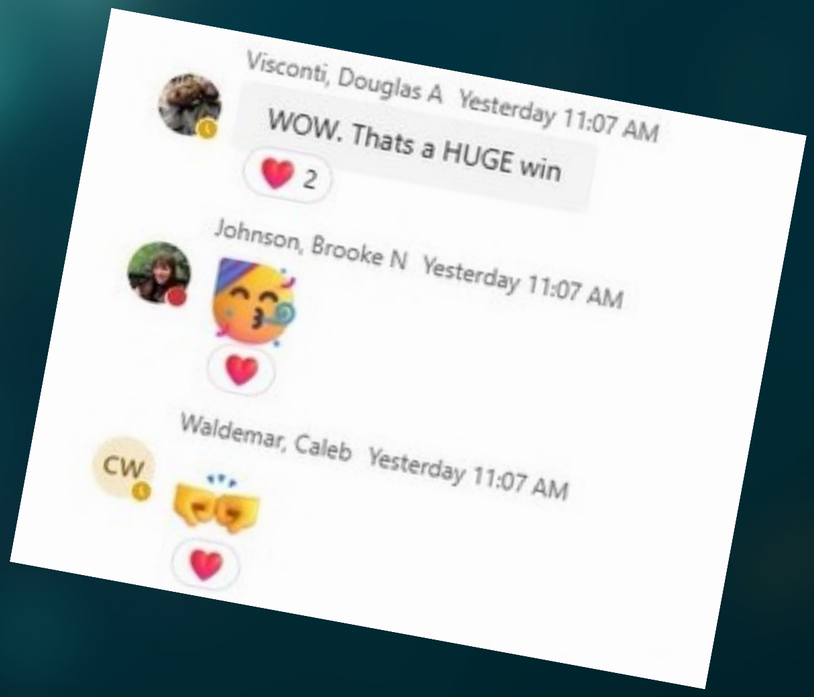


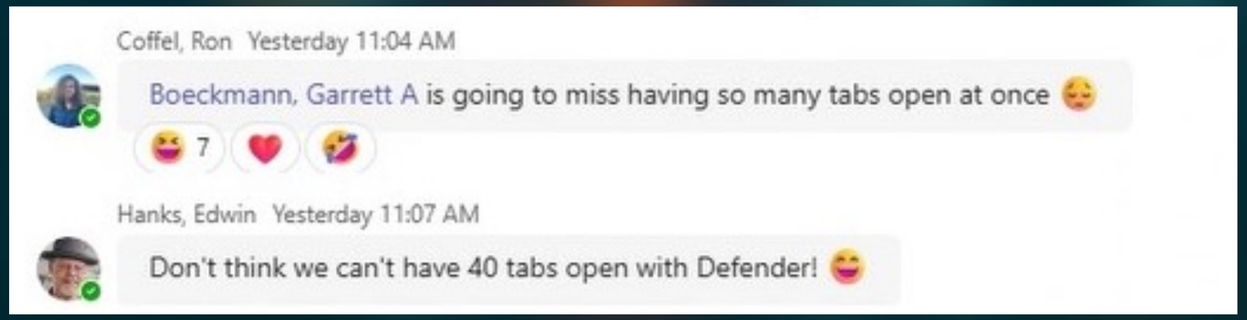


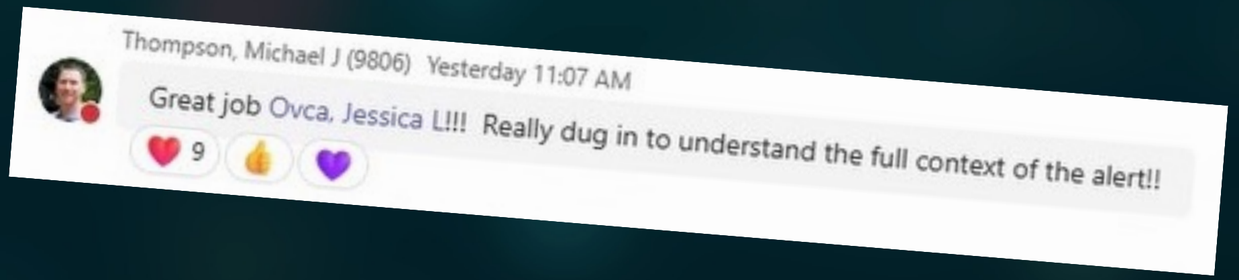


Team Chat

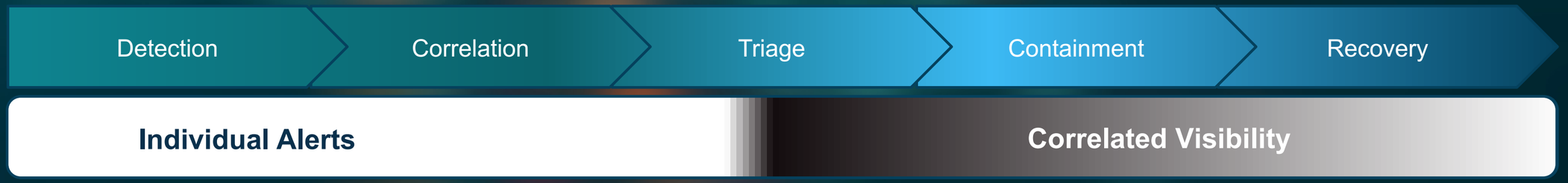

Visconti, Douglas A Yesterday 11:03 AM
I love that being all in one place... would take forever to pull together
2


Visconti, Douglas A Yesterday 11:07 AM
WOW. Thats a HUGE win
2
Johnson, Brooke N Yesterday 11:07 AM
Waldemar, Caleb Yesterday 11:07 AM
CW


Coffel, Ron Yesterday 11:04 AM
Boeckmann, Garrett A is going to miss having so many tabs open at once
7
Hanks, Edwin Yesterday 11:07 AM
Don't think we can't have 40 tabs open with Defender!


Thompson, Michael J (9806) Yesterday 11:07 AM
Great job Ovca, Jessica L!!! Really dug in to understand the full context of the alert!!
9

Unified Security Platform Shift in Capacity



Faster Mean Time to Triage

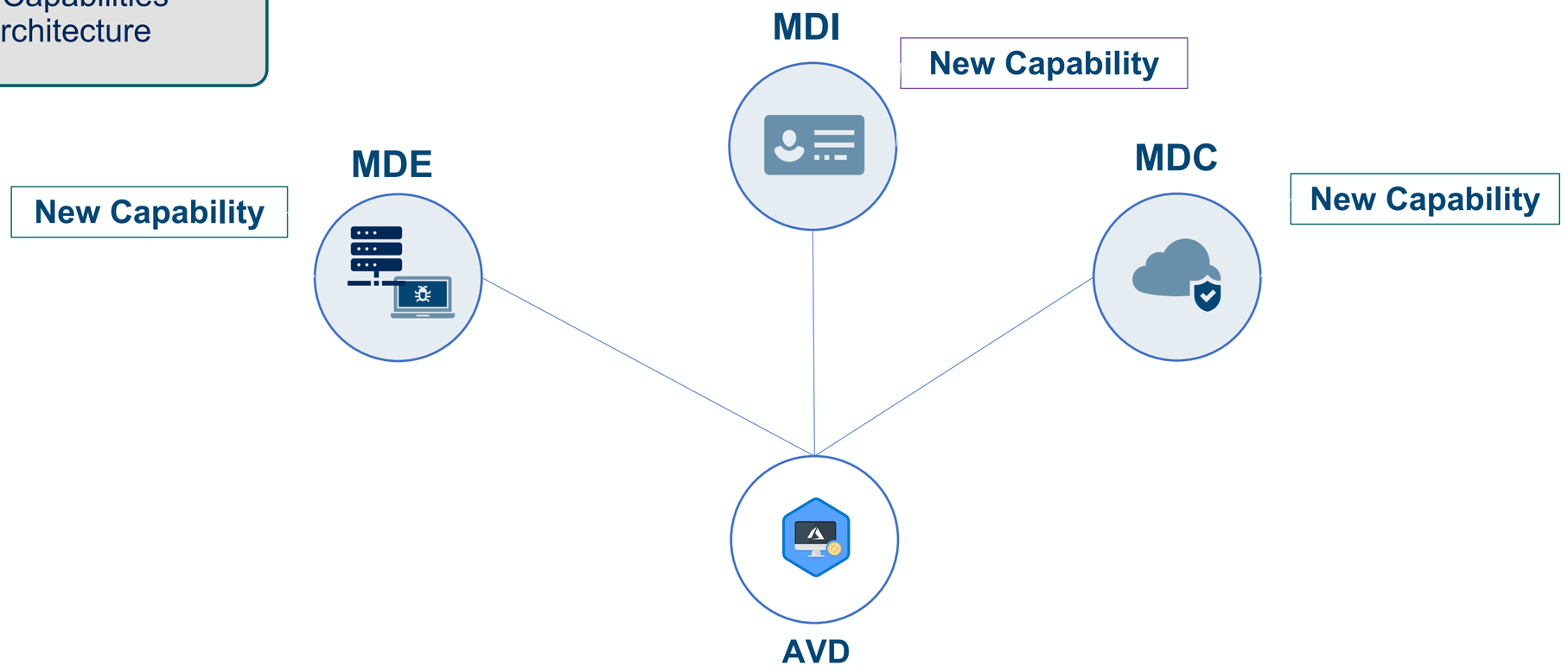
Faster Mean Time to Contain

Unified Security Platform

Tech Transformation

Plug and Play Security

- Native integration
- Ease of implementation
- Expandable Capabilities
- Reference Architecture



Lessons Learned



- Develop a strategic partnership



- Immerse your leaders, analyst, and engineers in into the program



- Embrace misses and problems as opportunities for growth and development



- Stay the course with an MVP approach

Security For Enterprise Mobility

Transformation

People



Processes



Technology



What's Next for 2026

AI for Security
- Accelerate and Enhance Security with Co-Pilot

Shift our approach
- Moving from Detection to Prevention

Product Maturity
- Responsibly adding capabilities and influencing changes

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Takeaways

PCI DSS continues to set the foundation for disciplined security operations — logging, review, monitoring, detection, and incident response.

Our Unified Security Platform journey has not only strengthened our ability to meet these requirements, it has fundamentally elevated how we operate as an enterprise-class security organization.

Through this transformation, we have achieved:

- **Deeper, correlated security visibility** - enabling PCI-aligned monitoring at significantly greater scale and speed
- **Higher-quality analysis and decision-making** - through unified context across logs, signals, identities, and assets
- **Accelerated detection and response** - reducing exposure windows and improving overall resilience
- **A more capable and engaged security team** - equipped to support not just PCI requirements but the broader threat landscape