

Unified Security Platform

Transforming Security for Enterprise Mobility

Brian Mize

Director, Global Cyber Security
Enterprise Mobility

Professional | Cyber Security professional, second career
Personal | Father and husband



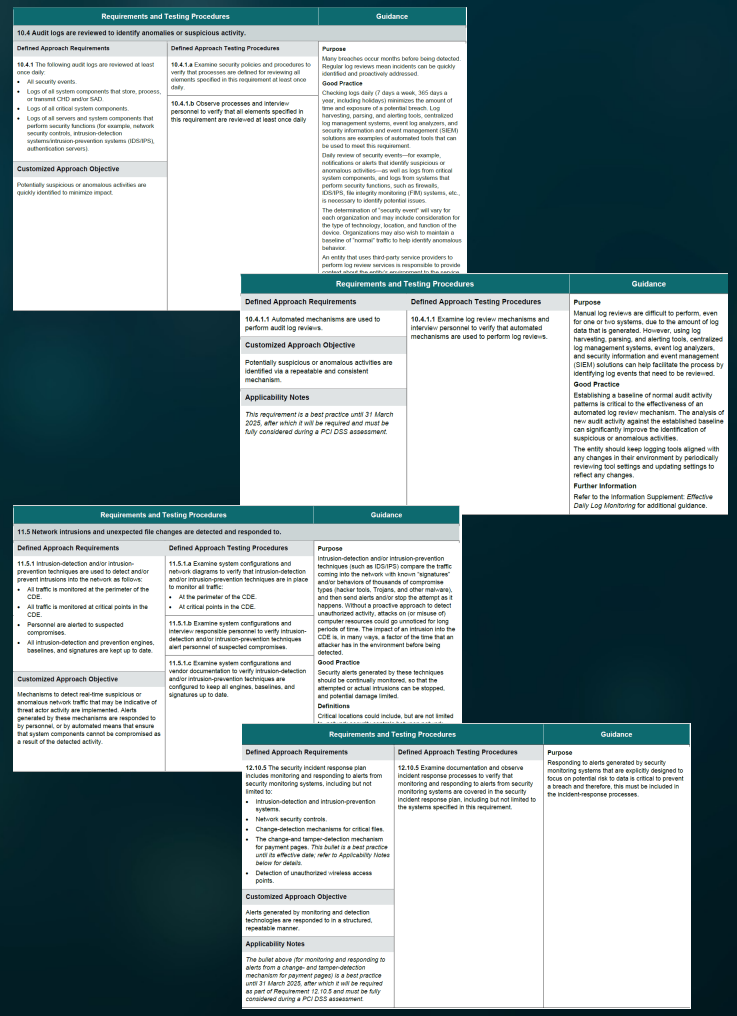
A Security Transformation Journey

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

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

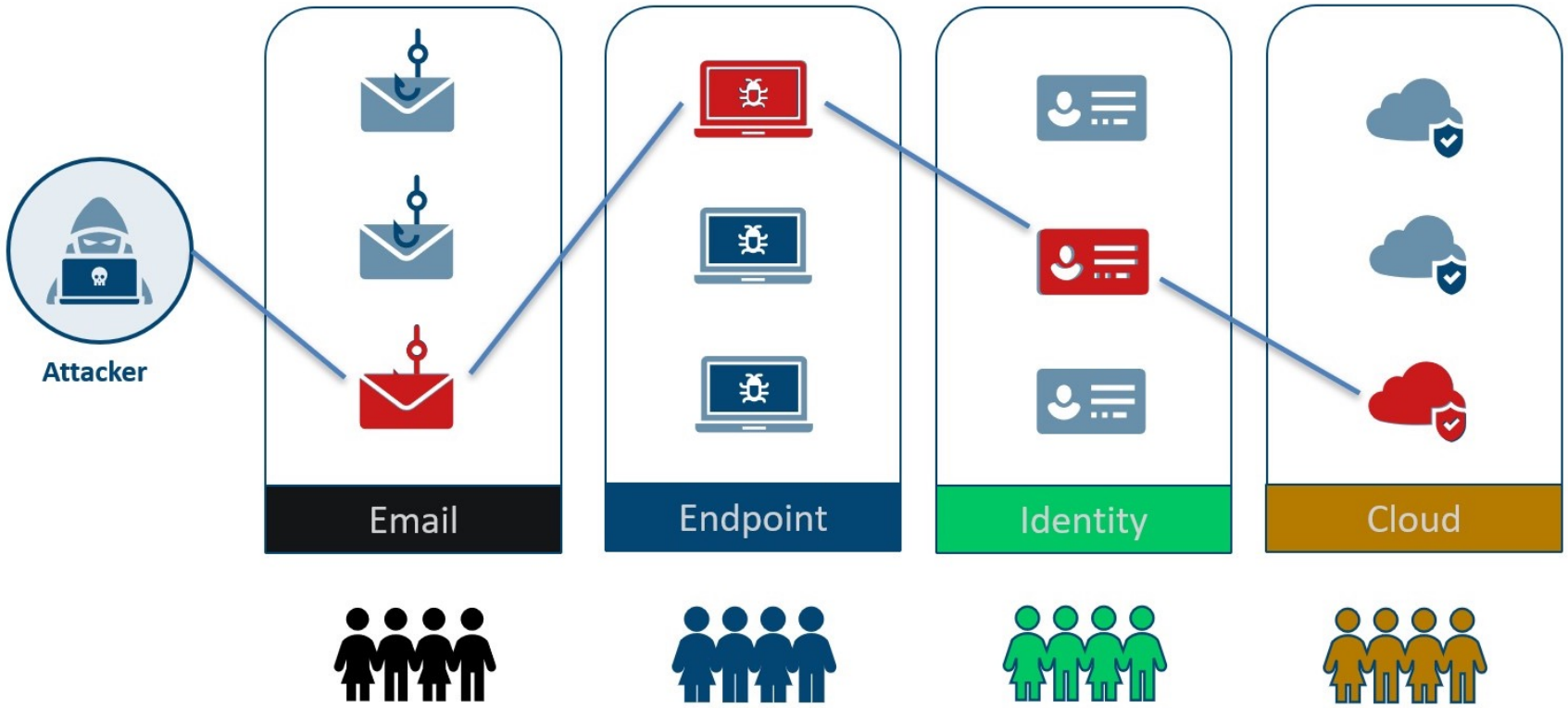
- Broader and richer security context faster than ever before
- Analysis efficiency
- Accelerated detection and response

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



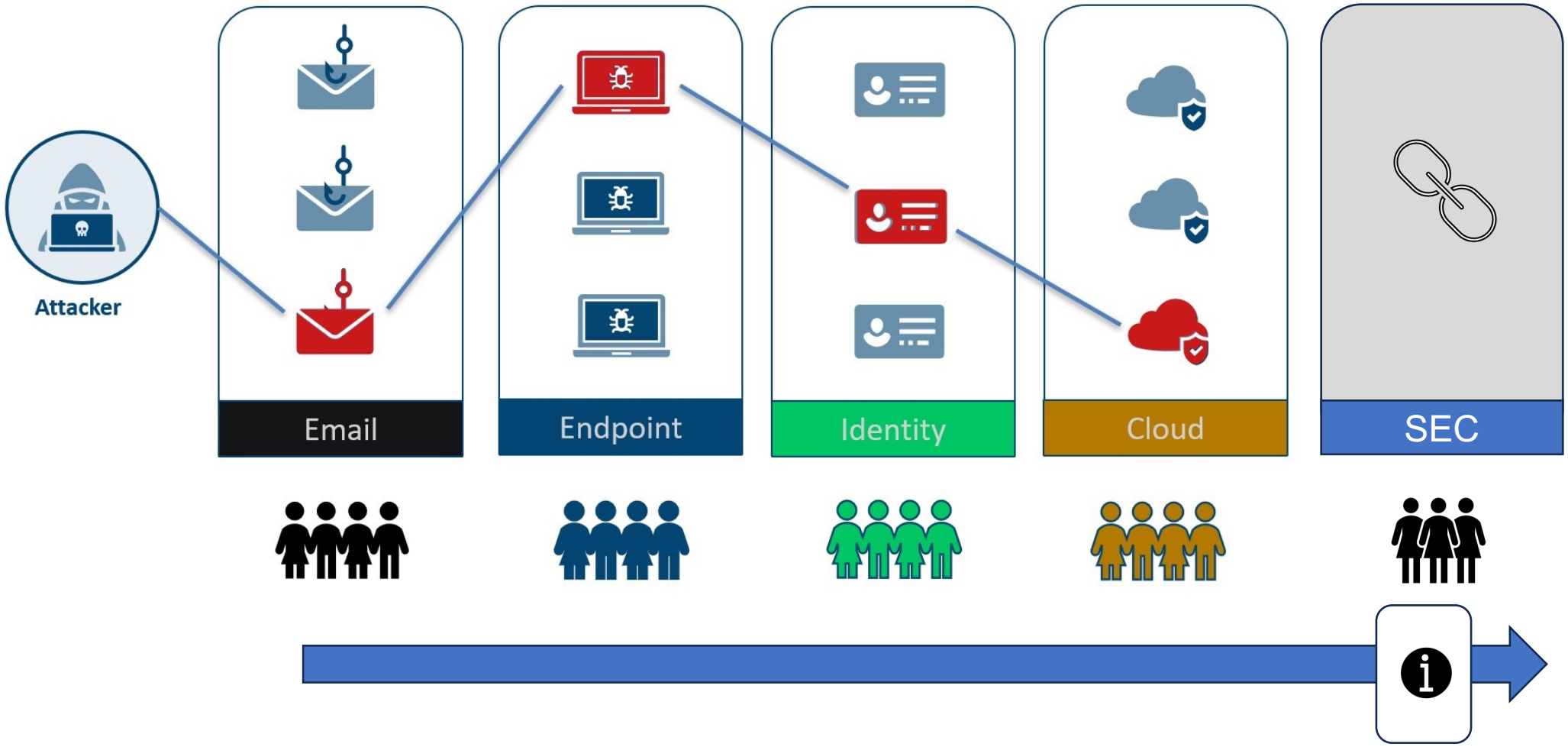
Detect in Silos

Attack in Chains

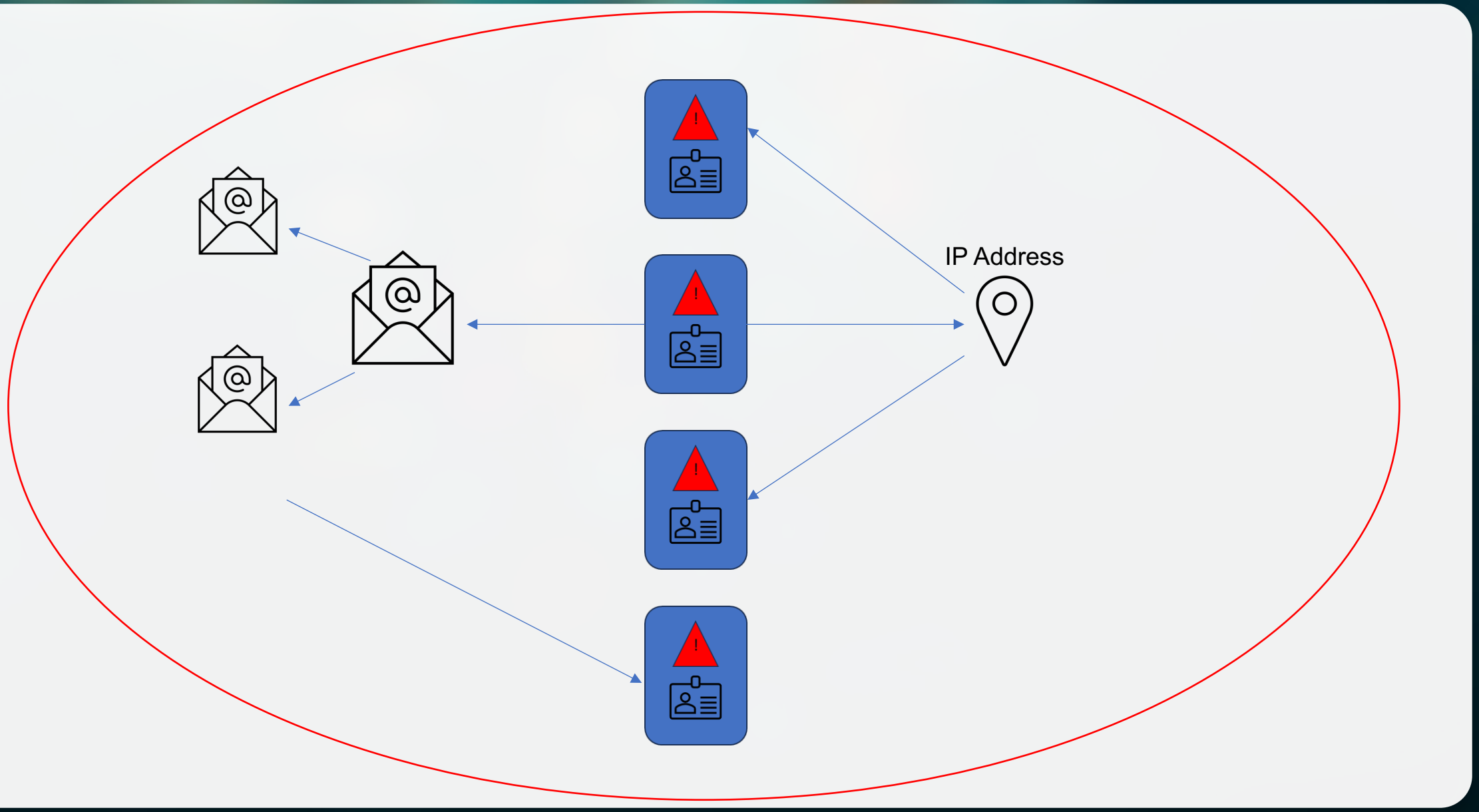


Detect in Silos

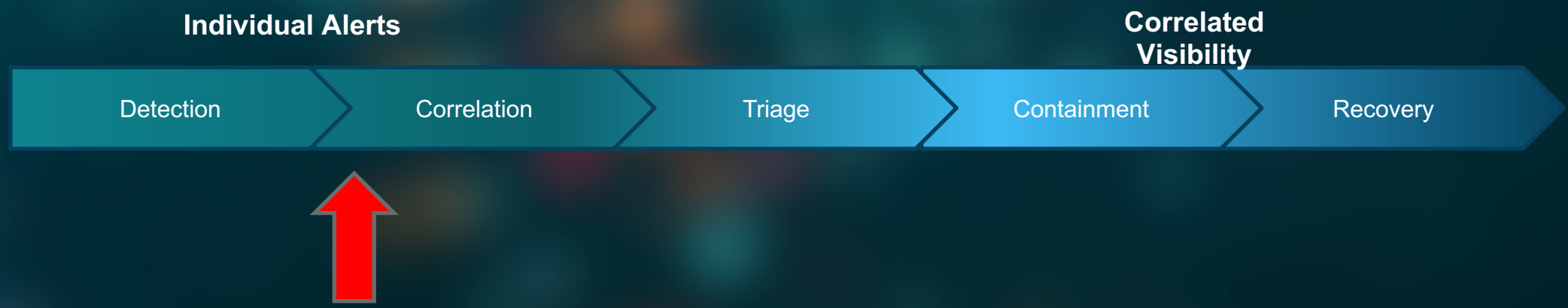
Attack in Chains



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

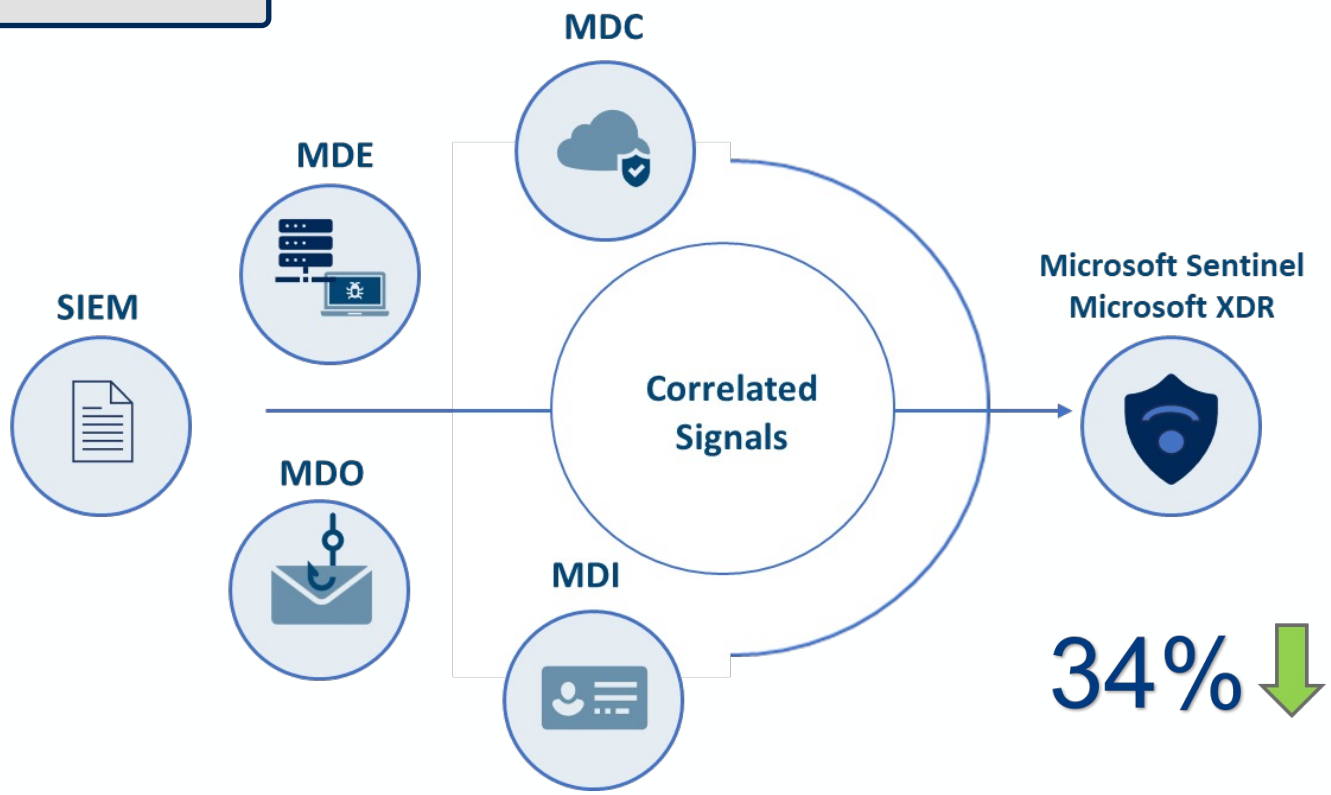
Unified Security Platform (USP)

Full Scope-MVP

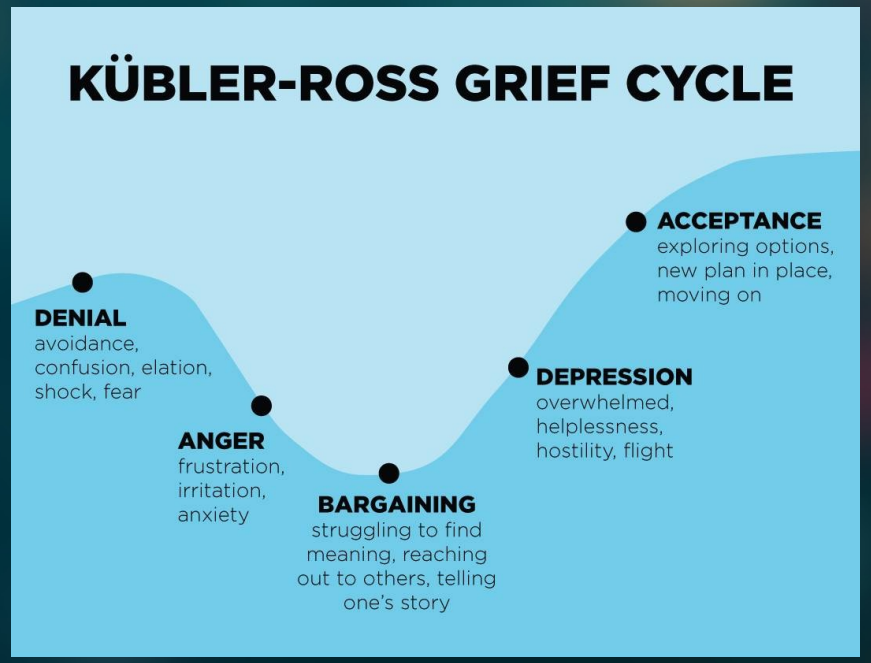


Unified Security Platform

Correlated Threat Visibility



Team Acceptance



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

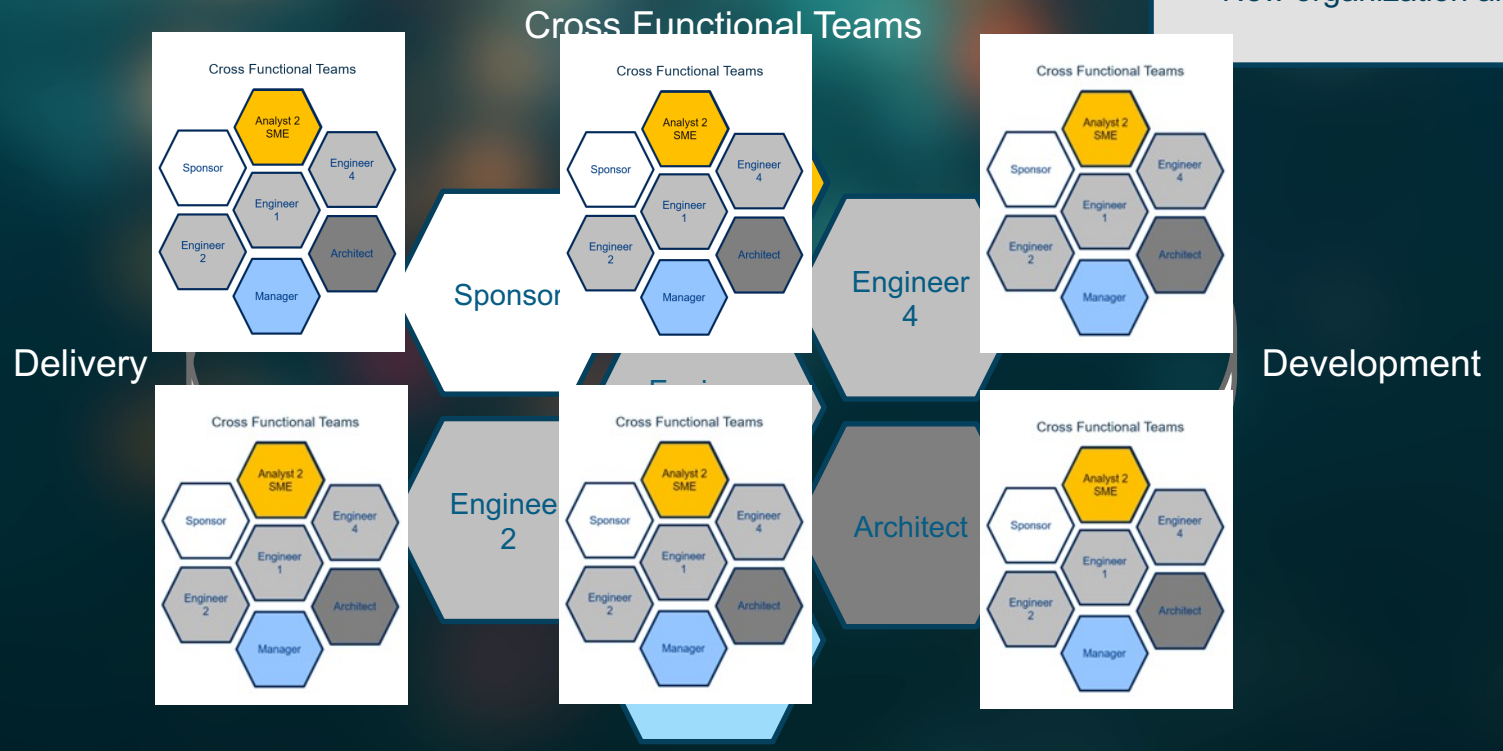
Our Change Approach

- **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

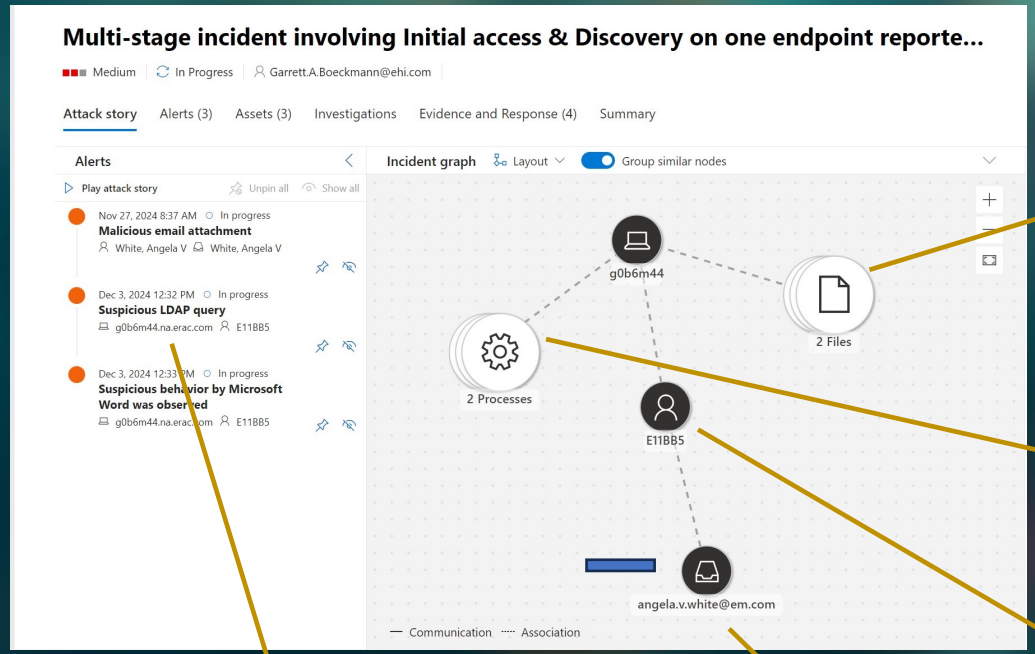
In-Department Delivery

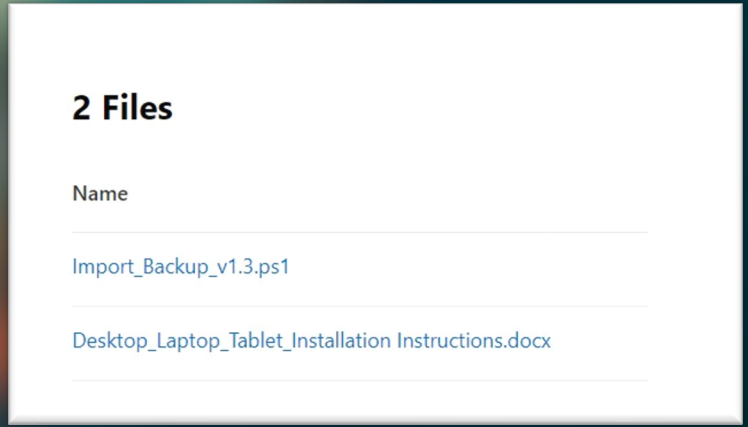
- Created Excitement and Enthusiasm
- 90 new processes and procedures
- 1000 hours of USP training
- New organization and mindset

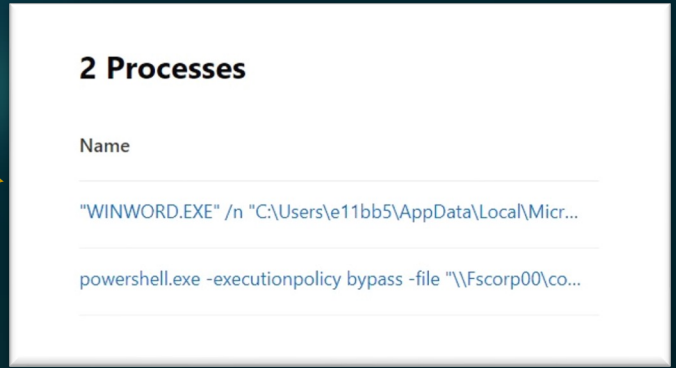


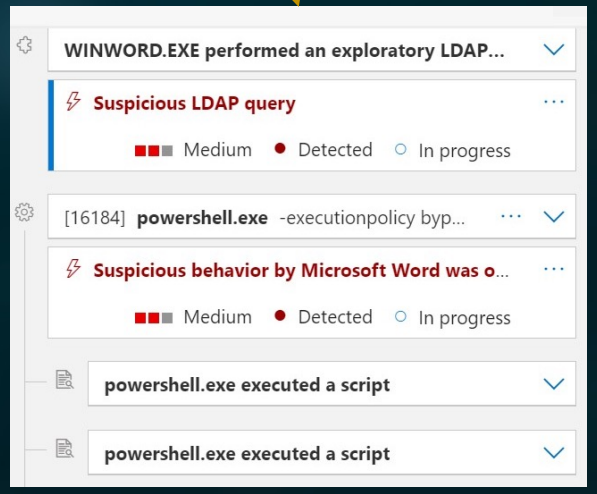
Technical Leadership Team

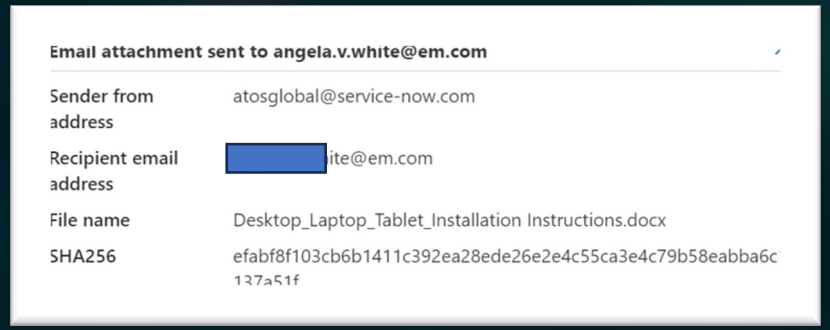
Correlation in Action

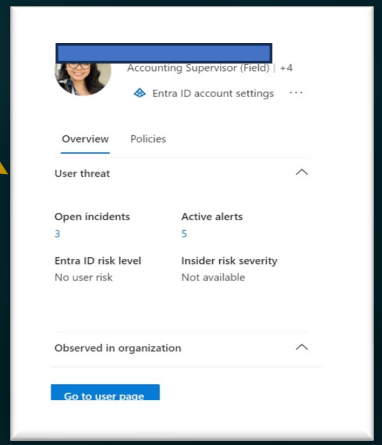




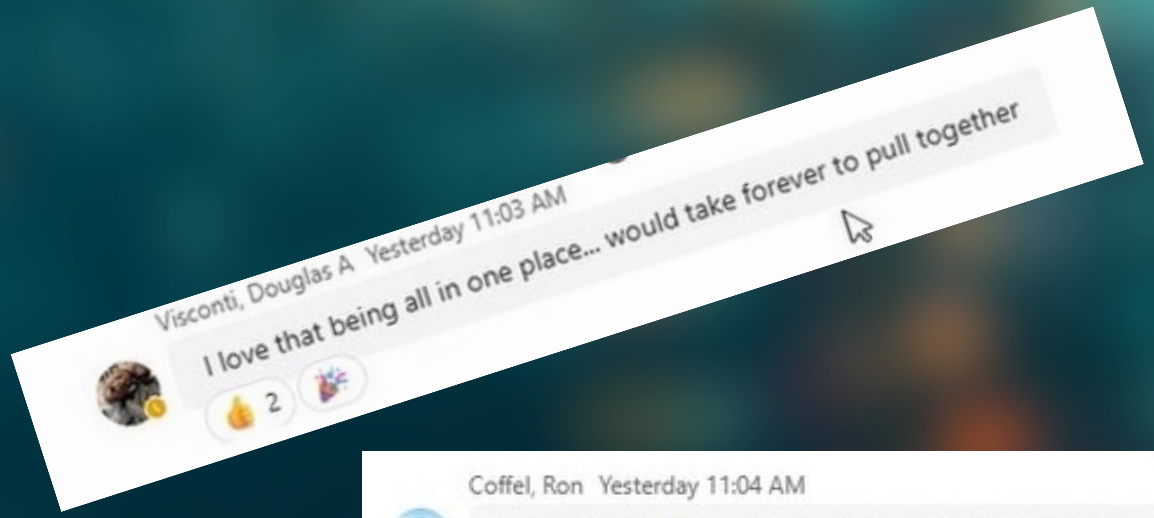


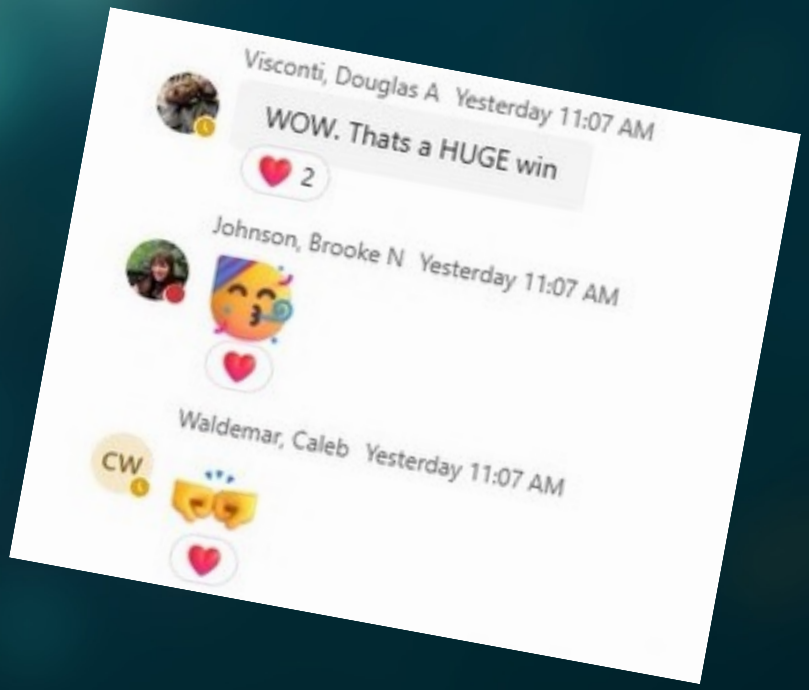


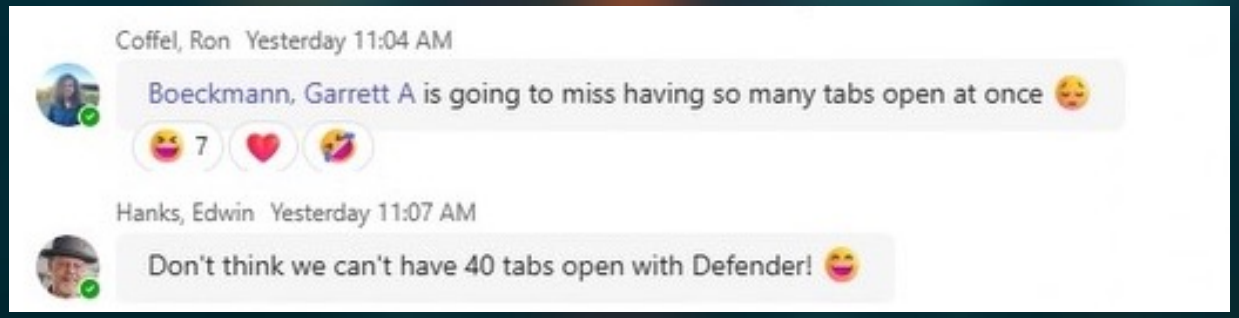


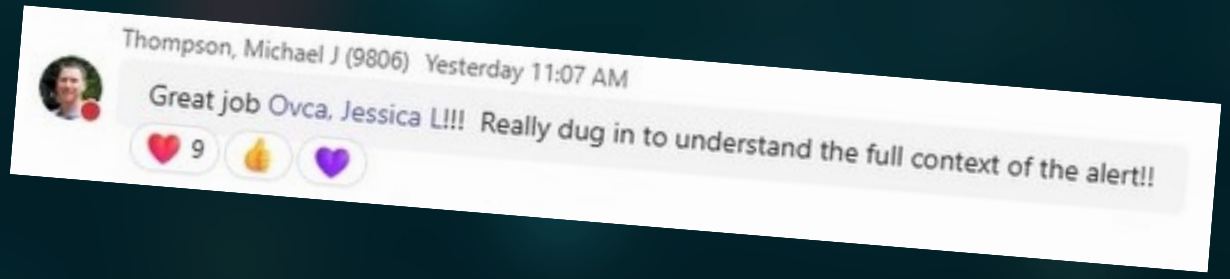


Team Chat

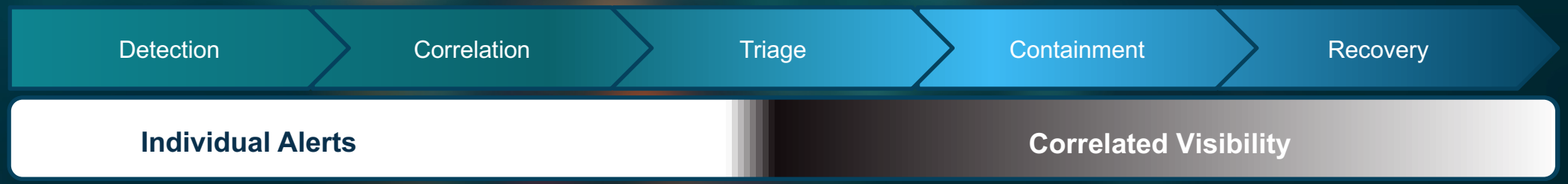

Visconti, Douglas A Yesterday 11:03 AM
I love that being all in one place... would take forever to pull together
2


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

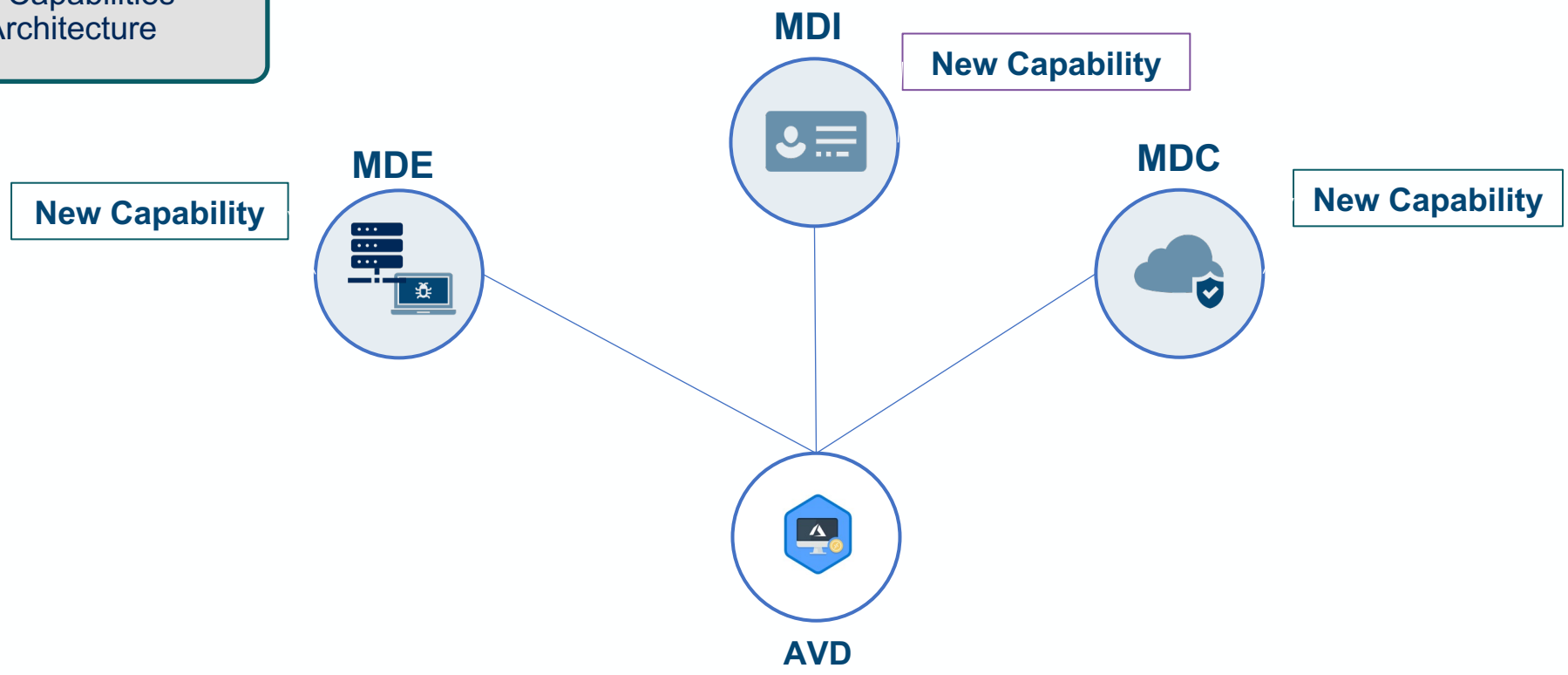
Faster Mean Time to Contain

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

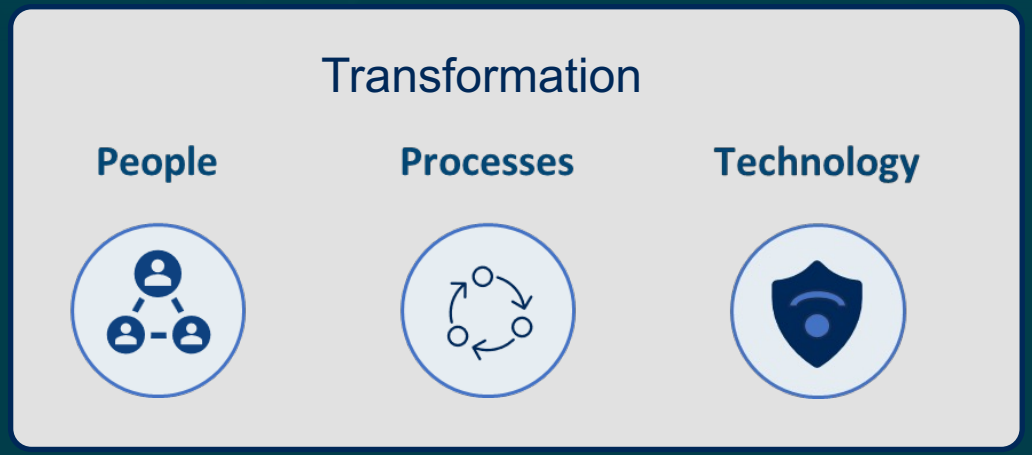


- Embrace misses and problems as opportunities for growth and development



- Stay the course with an MVP approach

Security For Enterprise Mobility



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

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