VIPSS
Victoria International Privacy & Security Summit

Assuming Failure Provides Better Defensive Outcomes

Jason Maynard
Field CTO Cybersecurity Canada
CCIE, CC[N|I|D]P, SFCE, C|EH, RCSS, GICSP, GRID, GPEN, GDAT, GCPN, AWS Cloud Practitioner, AWS Solutions Architect, AWS Security, Azure Fundamentals, Azure Security Engineer
MITRE ATT&CK: CTI, SOC Assessments, Threat Hunting Detection Engineering, Adversary Emulation Methodology, Purple Teaming Methodology
ATTACKIQ: Purple Team, Mitre Att&ck, Breach Attack Simulation
Splunk Power User, Splunk Administrator

Cyber is foundational when driving any digital resilience program

cisco

VIPSS
Victoria International Privacy & Security Summit

Agenda:

- Adversaries Opportunity
- Attack Chains & Assuming Failure
- Defenders Opportunity
- Business Relevance in the SOC
- AI Threats & Opportunity
- Business Flows Mapped to Cyber Capabilities

*Proactive based defense based by assuming failure (B * R * E * A * C * H)*

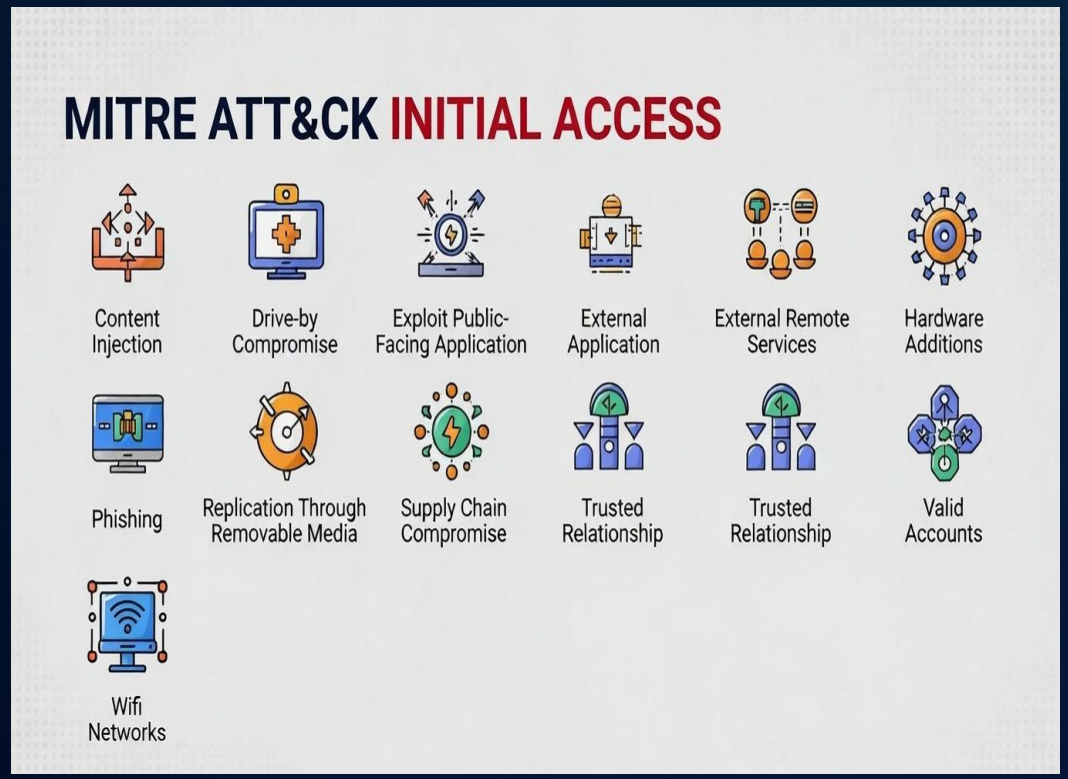
cisco

Level Setting

- We will never achieve 100% immunity
- The adversary will never be 100% correct
- The defender never needs to be 100% correct
- Time is a power play move for defenders
- Initial access is inevitable

Defenders have an opportunity to level the playing field

Initial Access



Adversaries are persistent and initial access will be achieved.

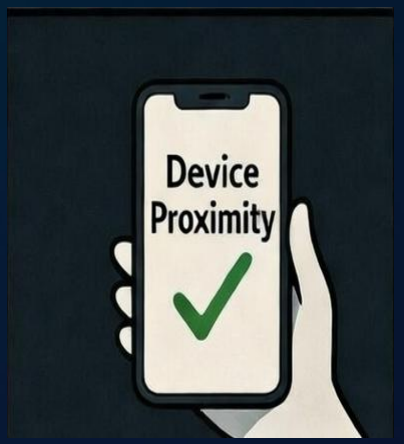
Valid Accounts

- Phishing
- Credential stuffing
- Leaked passwords
- Keyloggers

- SIM swapping - hijack SMS-based code
- MiTM attacks to intercept authentication tokens
- Exploiting weak MFA reusable codes in apps.

- Flood user with repeated MFA
- Combined social engineering claiming to be from support

- Steal MFA seed or token generator (e.g., via malware on the user's device)
- Session hijacking after initial authentication
- Exploiting time-based one-time password (TOTP) predictability in poorly configured systems.



- Hackers might use relay attacks to forward signals over distance
- Spoof device identifiers.
- Gain physical access to clone or pair with trusted devices.

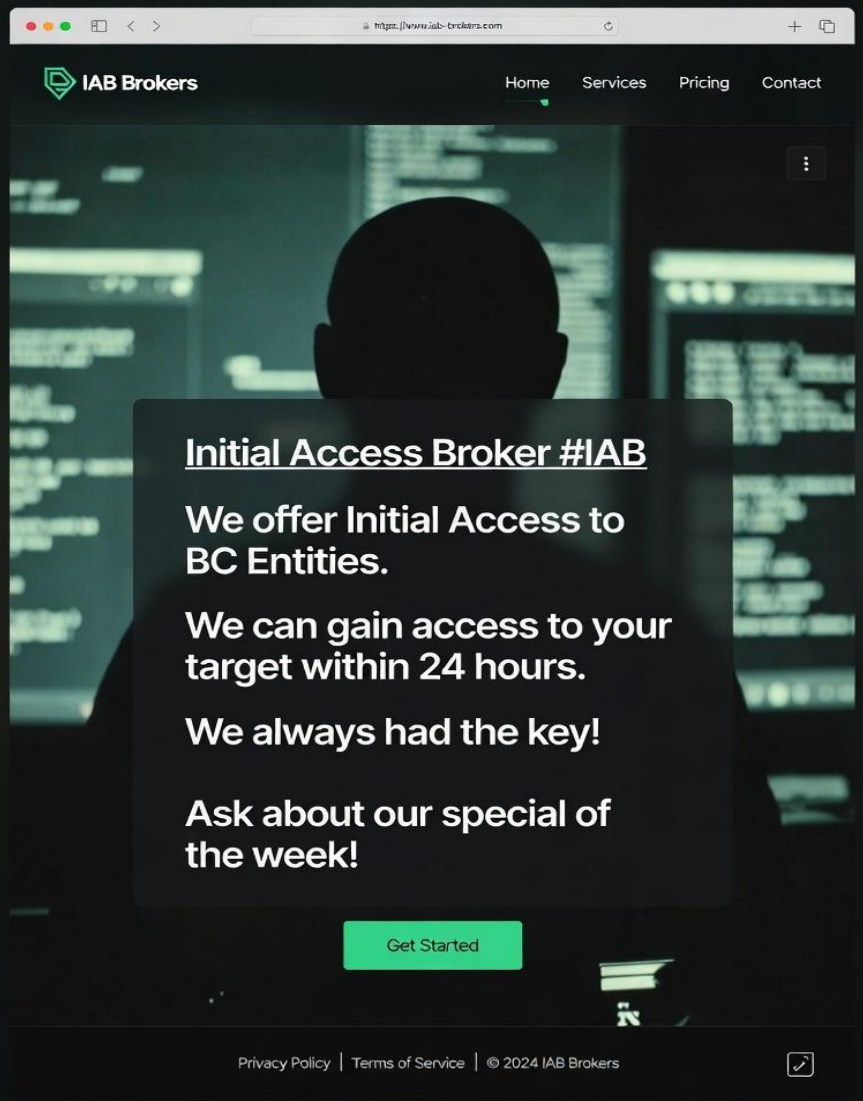
- Social Engineering identity verification (IDV) workflows which provide high-assurance of user identities

The adversary does not give up easily!

Have you heard about IABs?

Initial Access Brokers

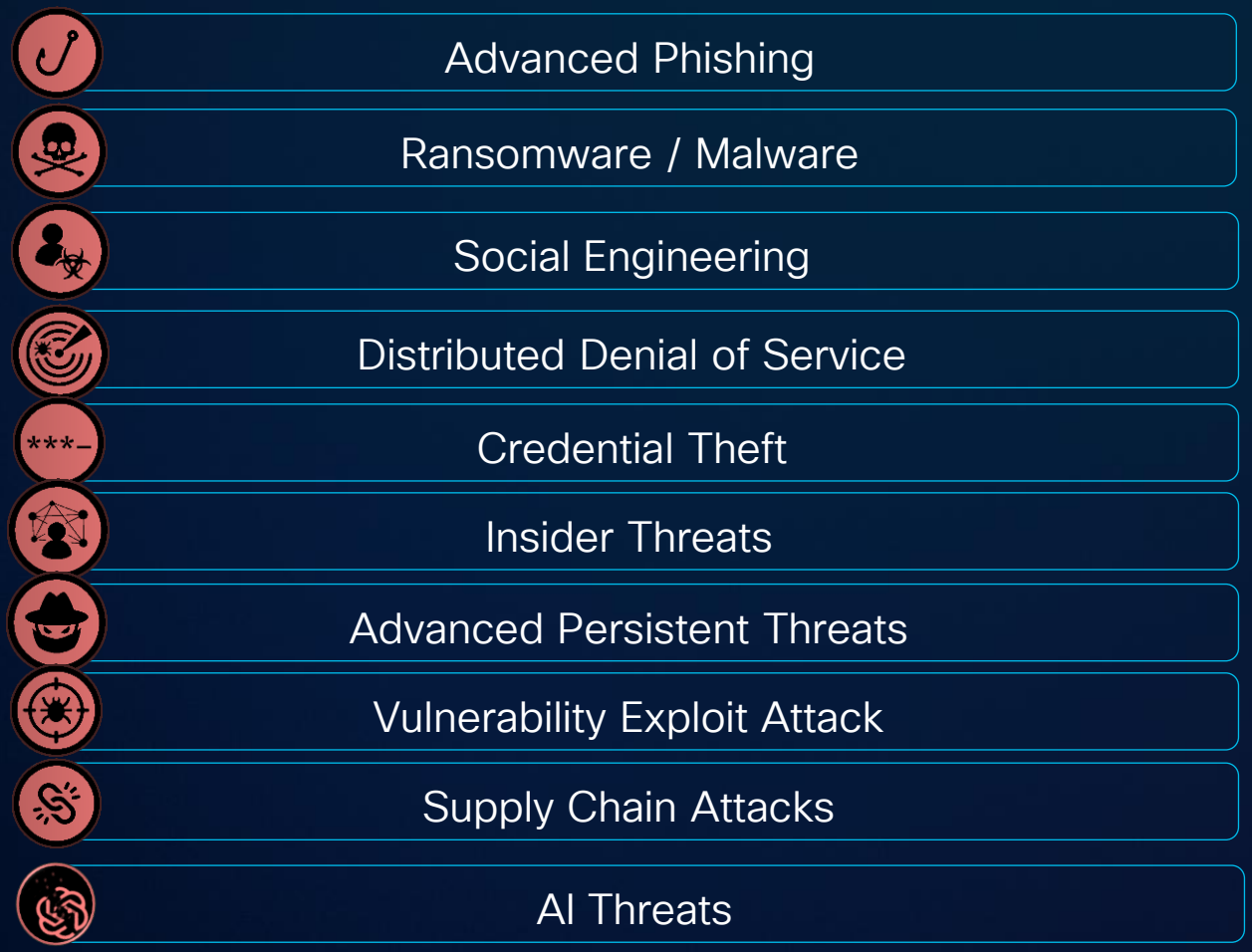
Initial Access Brokers (IABs) are cybercriminals who specialize in gaining unauthorized access to computer networks and systems, which they then sell to other threat actors, such as ransomware groups. They play a crucial role in the cybercrime ecosystem, facilitating attacks by providing access to compromised networks for a fee. The demand for IAB services has surged with the rise of Ransomware-as-a-Service (RaaS), leading to an increase in their listings on the dark web. IABs are known for their professionalism and operate within a structured market, often adhering to specific rules and conventions.



Fake: example purposes only

1-800 GIVE ME INITIAL ACCESS

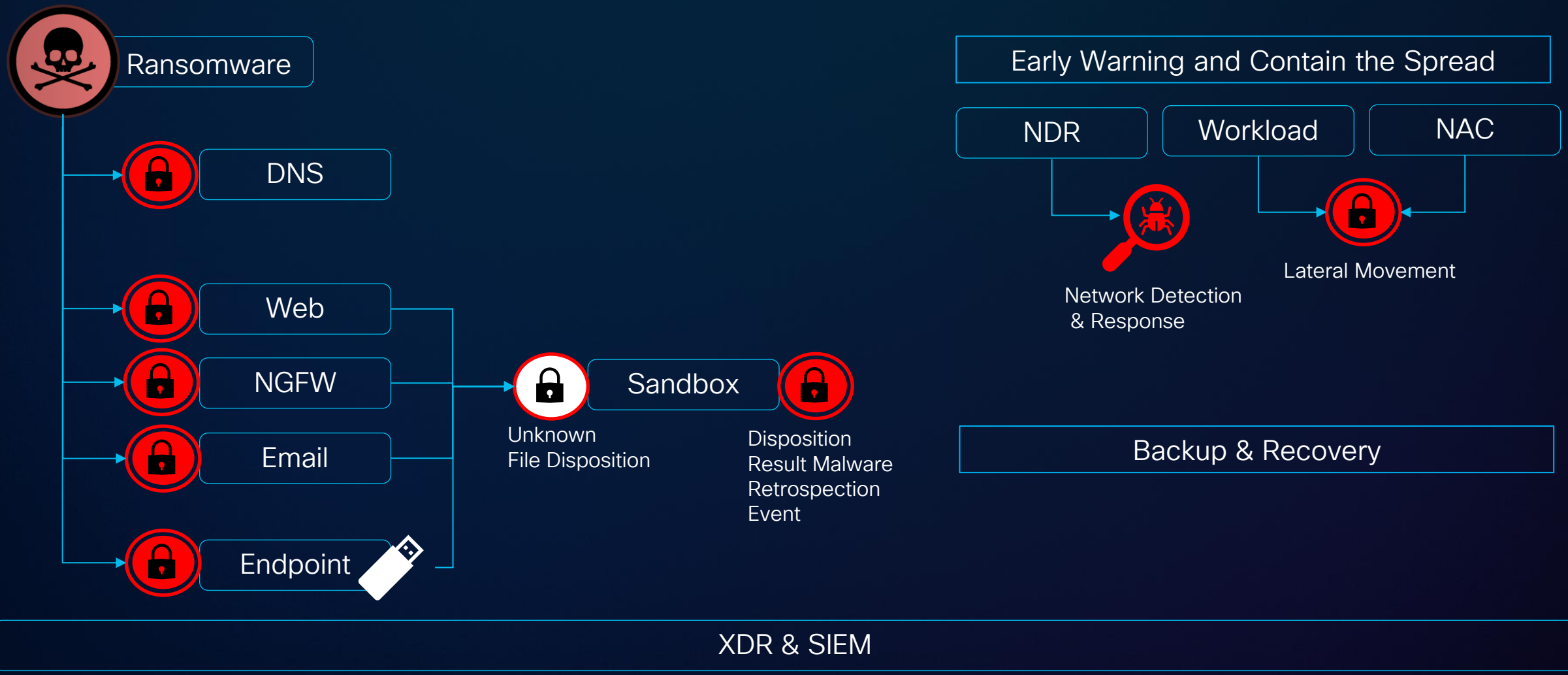
Top 10 Attacks & Common Themes



Preventative Controls

Prevention is key but 100% efficacy 100% of the time is unattainable.

Prevention Opportunity: Ransomware



Controls fail today and will fail tomorrow!

The Anatomy of an Attack: After Initial Access

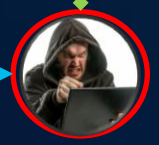
Detection / User Awareness
Prevention

Initial Access

- Email Security
- Endpoint Protection
- Endpoint Detection / Response
- DNS & Web Content Prevention
- Next Generation Firewall
- Network Detection & Response

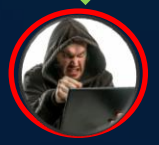
Initial Access
TA0001

- Endpoint Protection
- Endpoint Detection / Response
- Code Signing



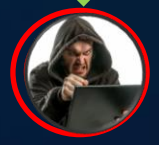
Execution
TA0002 (PowerShell)

- Endpoint Protection
- Endpoint Detection / Response
- Command Line Capture



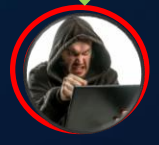
Persistence
TA0003
(Reg Run Key/Startup Folder

- Audit
- Privileged Account MGMT
- Update Software
- User Account Control



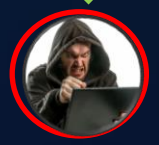
Privilege
Escalation
TA0004
Bypass User
Account Control

- Endpoint Protection
- Endpoint Detection / Response



Defense Evasion
TA0005
Obfuscated Files or
Information: Encrypted/E
ncoded File

- MFA Code Generation / Proximity
- User Training

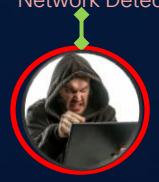


Credential Access
TA0006
MFA Request Generation

- Network Segmentation
- MFA / Encrypt Traffic
- Network Detection & Response

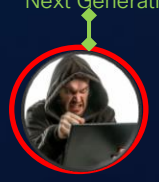
Discovery
TA0007
Network Sniffing

- Network Segmentation
- Workload Segmentation
- Network Detection & Response



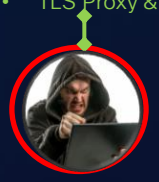
Lateral
Movement
TA0008
Remote Desktop Protocol

- Workload Segmentation
- Network Detection & Response
- Next Generation Firewall



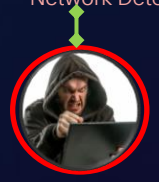
Collections
TA0009
Remote Data Staging

- Network Detection & Response
- Next Generation Firewall
- TLS Proxy & Encrypted Visibility



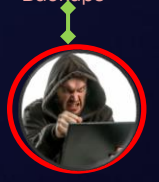
Command & Control
TA0011
Asymmetric Cryptography

- Next Generation Firewall
- Workload / Network Segmentation
- Network Detection & Response



Exfiltration
TA0010
Transfer Data to
Cloud Account

- Endpoint Detection & Response
- Backups



Impact
TA0040
Data Encrypted for
Impact

Understanding the Adversaries Abilities

The attack does not take these steps in order as outlined. There is nuance to the attack and how one defends. This is an example and not comprehensive

Defenders goal is to make it muddy, murky, and sticky

This buys you time-based defense for tech, people, and process to catch up!

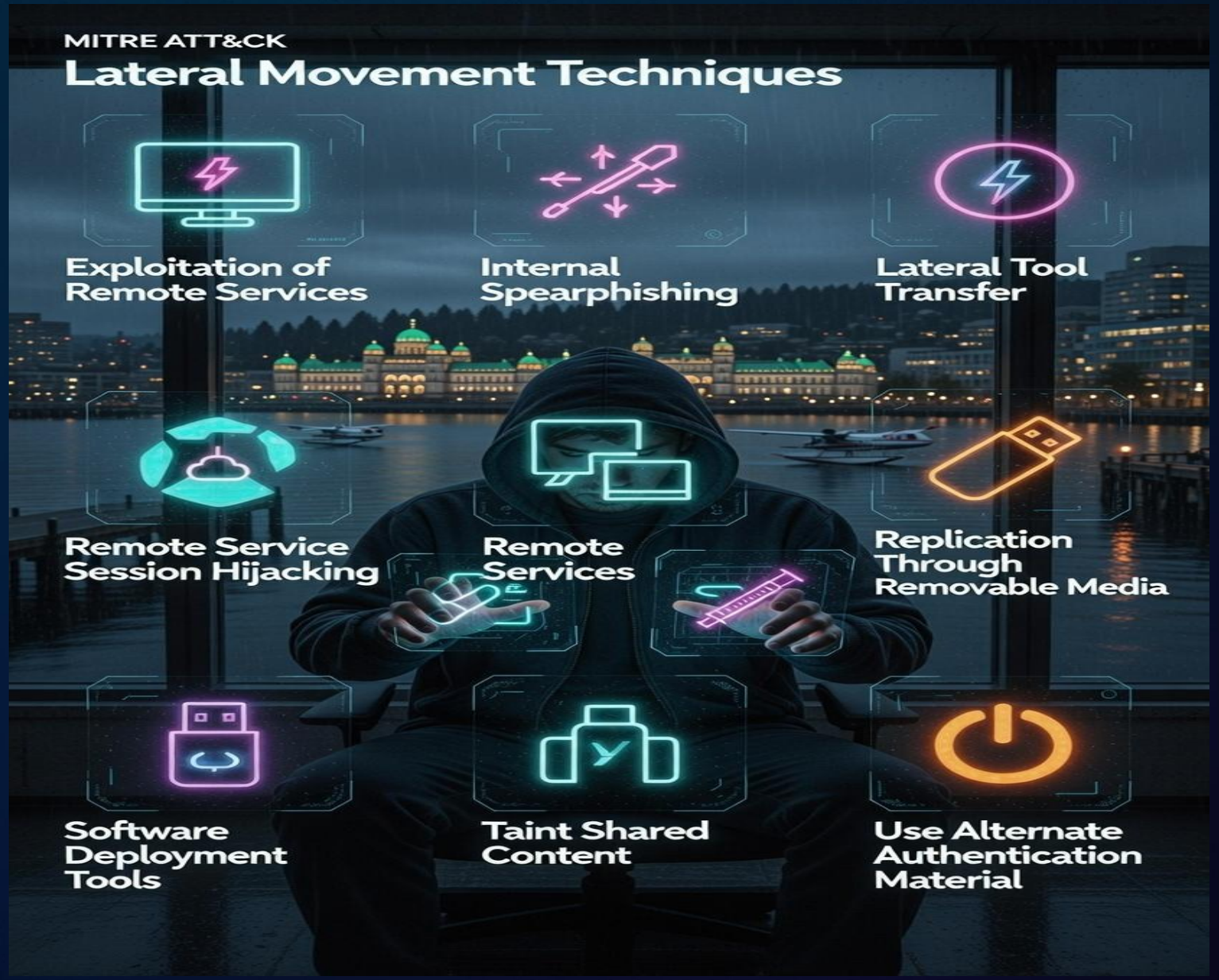
So, what is one of the greatest opportunities missed by defenders?

60-70% of all breaches involve.....

Lateral Movement
TA0008

The Adversaries Opportunity Unchecked

Lateral Movement

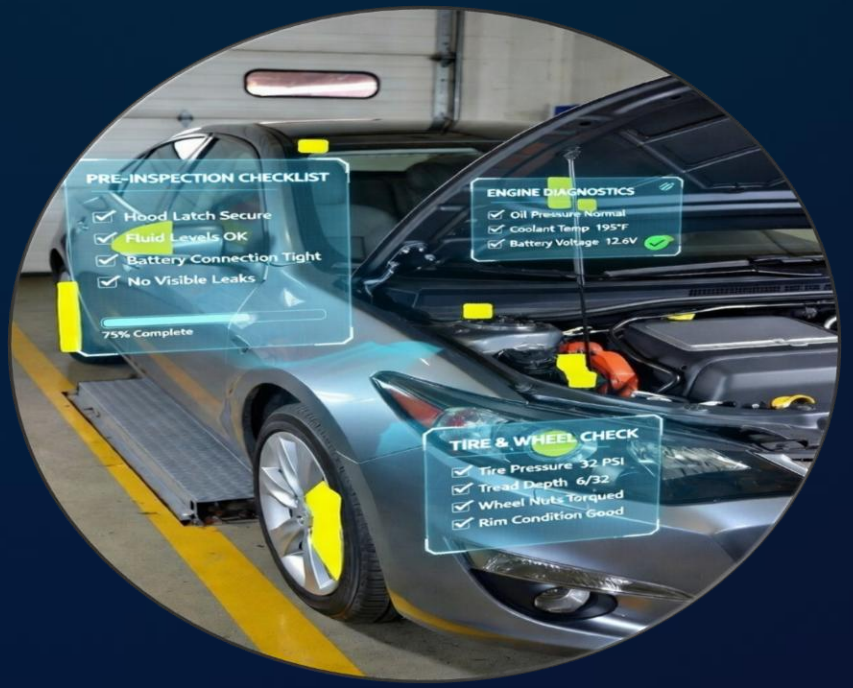


Why do defenders struggle so much removing the ability to move laterally?

Lateral Movement Game is Over!

New Employee Background Checks or Car Safety Requirements

REQUIRED!



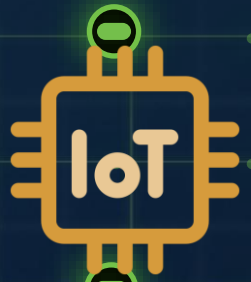
REQUIRED!

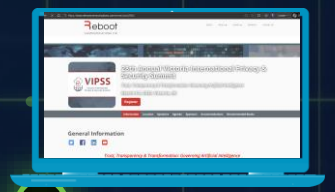
NOT REQUIRED!

Campus, Private Application Access, and Workloads MUST meet the standard

The Defenders Opportunity
Campus Network

- Visibility
- Policy
- Simulation
- Enforcement
- Zero Trust
- Defcon Policy
- Risk Profiles





The Defenders Opportunity
Private Applications

- Visibility
- Policy
- Enforcement
- Zero Trust
- Risk Profiles
- Step up Auth

The Defenders Opportunity
Datacenter

- Visibility
- Policy
- Simulation
- Enforcement
- Zero Trust
- Exploit Protection
- Risk Profiles

docker

eBPF

Microsoft Azure

aws

Google Cloud

Network DPU

CVE

OPENSHIFT

Server DPU

AIX

eBPF

eBPF

eBPF

Microsoft

Traditional Firewall

Identity Threat Detection and Response

Network Detection and Response

Endpoint Detection and Response

Policy Engine

Policy Administrator

Microsoft Entra ID

Identity Providers – Focus on Risk Based Identities

Enriched Identity & Context for Policy

Secure Campus

Secure Private Application Access

Secure Workload

Enriched Identity & Context for Policy

Policy Decision Points: 800-207

Policy Enforcement Points

Wired /Wireless

- Zero Trust Access
- Agent/Agentless
- Least-privileged Access
- Network Access Control
- Microsegmentation
- Posture and Profiling
- User & Machine Auth
- MFA Support

VPN

- Zero Trust Access
- Least-privileged Access
- Network Access Control
- Posture and Profiling
- User & Machine Auth
- MFA Support

VPNaaS

- Zero Trust Access
- Least-privileged Access
- Network Access Control
- Posture and Profiling
- User & Machine Auth
- MFA Support

Private Apps (ZTNA)

- Zero Trust Network Access
- Agent/Agentless
- Least-privileged Access
- Hiding apps from public internet
- Posture and Profiling
- User & Machine Auth
- Adaptive, context-aware access
- User device behavior monitoring
- MFA Support

Workload / Runtime

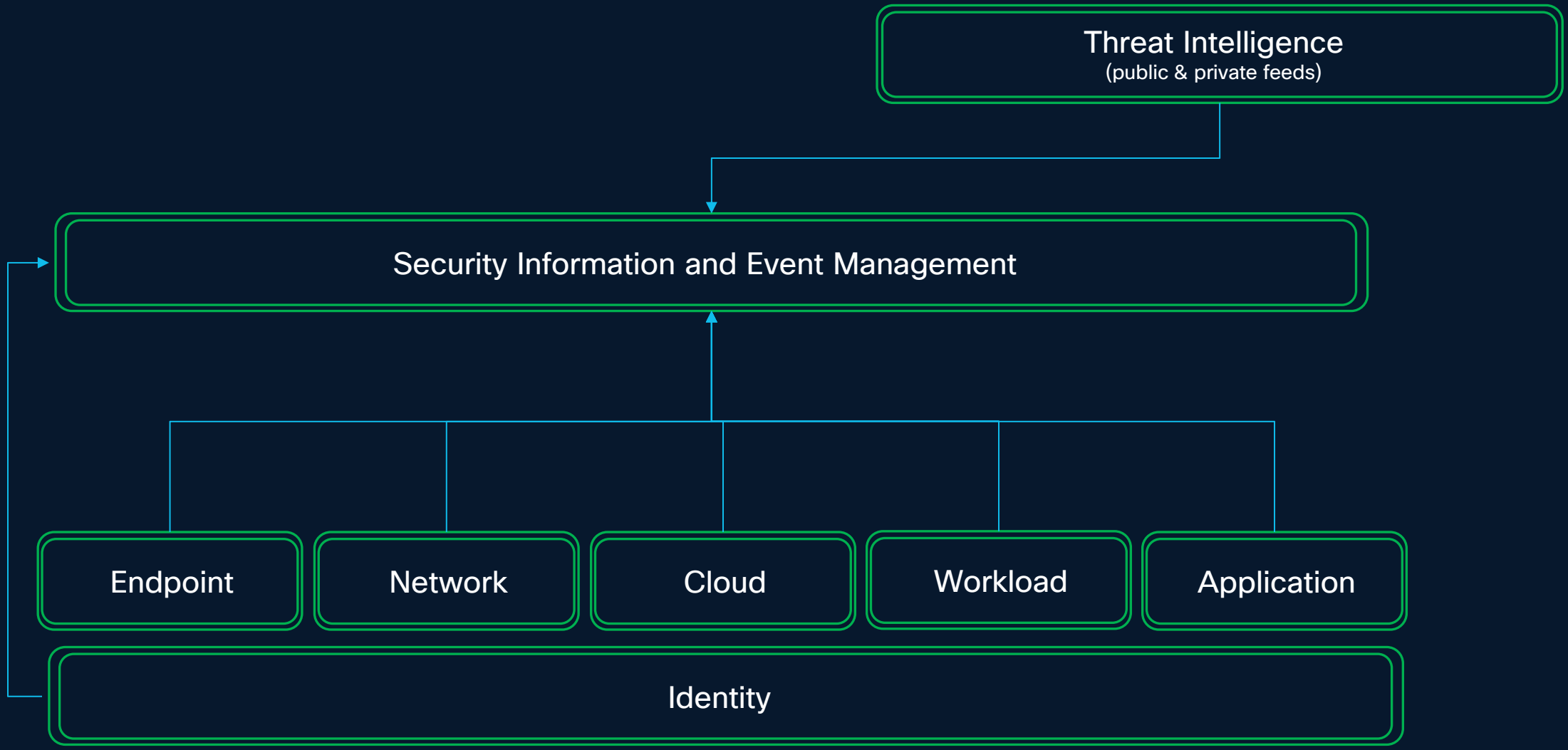
- Zero Trust Access
- Agent/Agentless
- Least-privileged Access
- Microsegmentation
- Vulnerability Insight and Forensics
- Application Dependency Mapping
- Policy Enforcement with Identity Based Control

aws Microsoft Azure Google

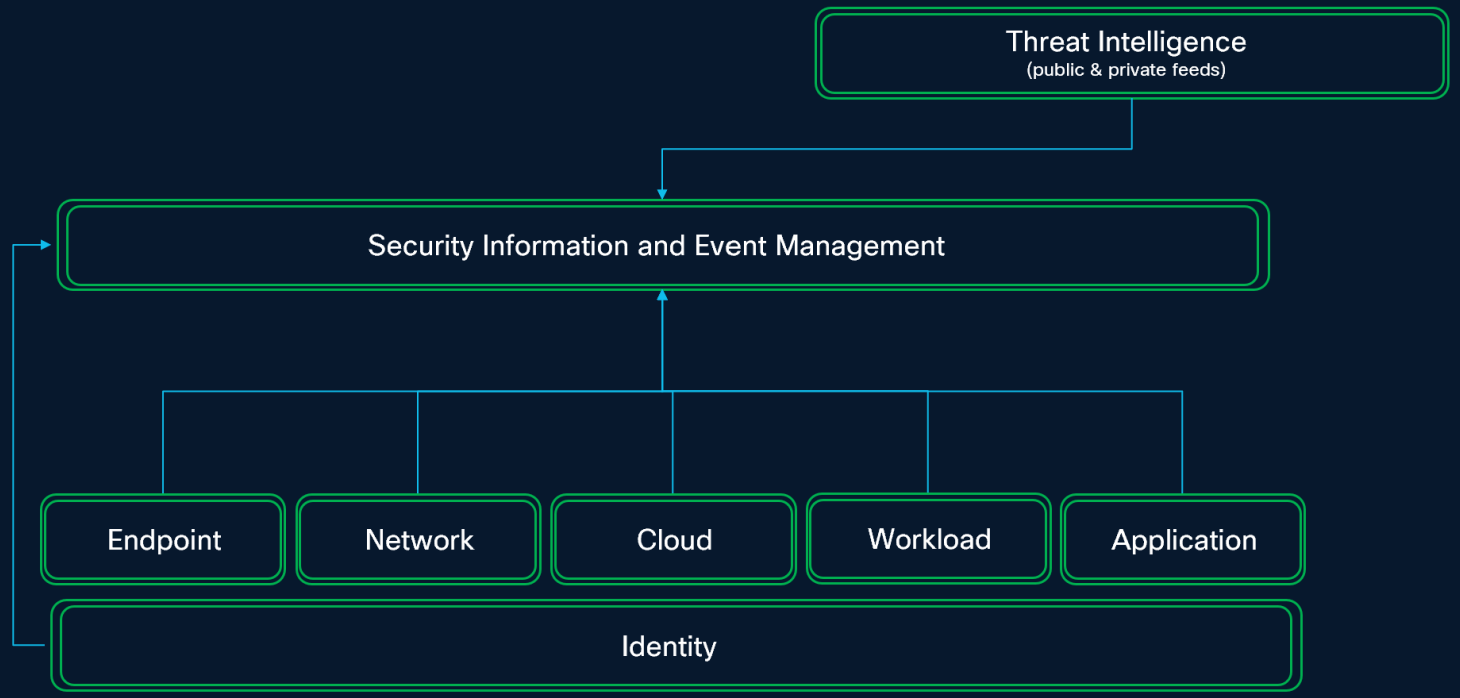
Extended Detection and Response

Business Relevance in the SOC

SOC of Today

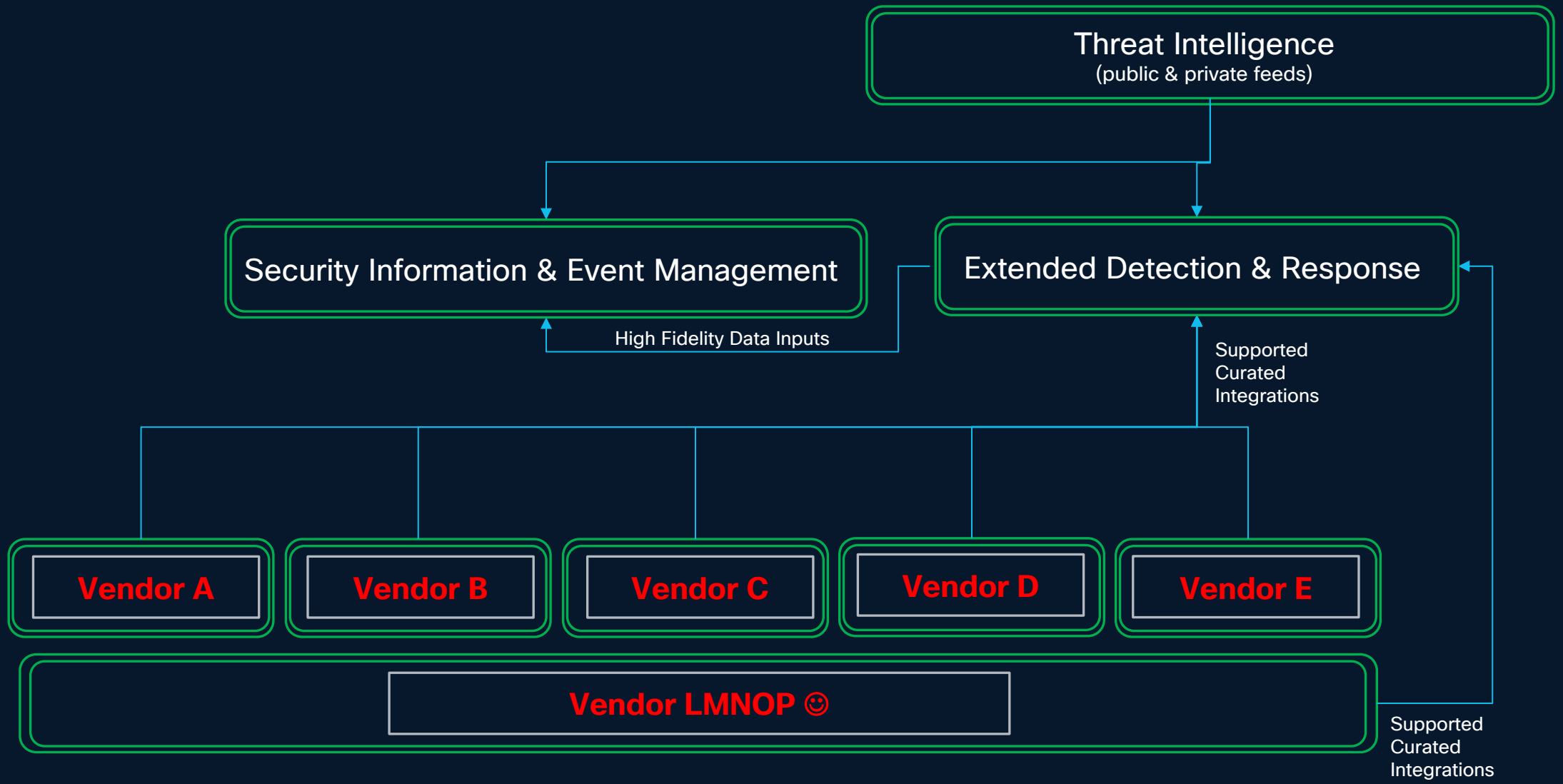


Challenges and Limitations

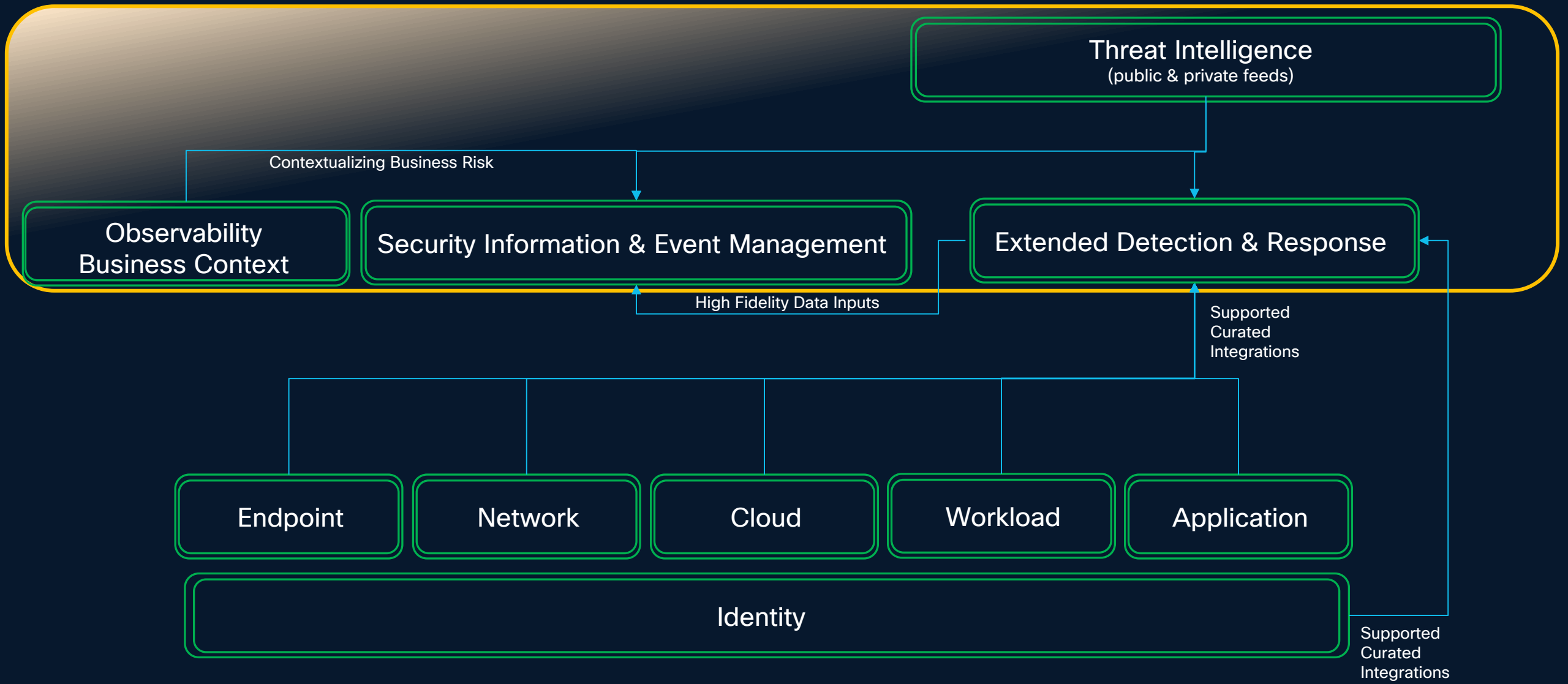


- Expensive to send all raw logs / individual alerts from all sources
- Complex building blocks when integrating technologies
- Limited support with integrations or limited community – lots of finger pointing
- No context in relations to the business and true risk of the event
- Lower overall fidelity outcomes without lots of customization
- Usually late to the party
- Ideal for governance and compliance

SOC of the Future

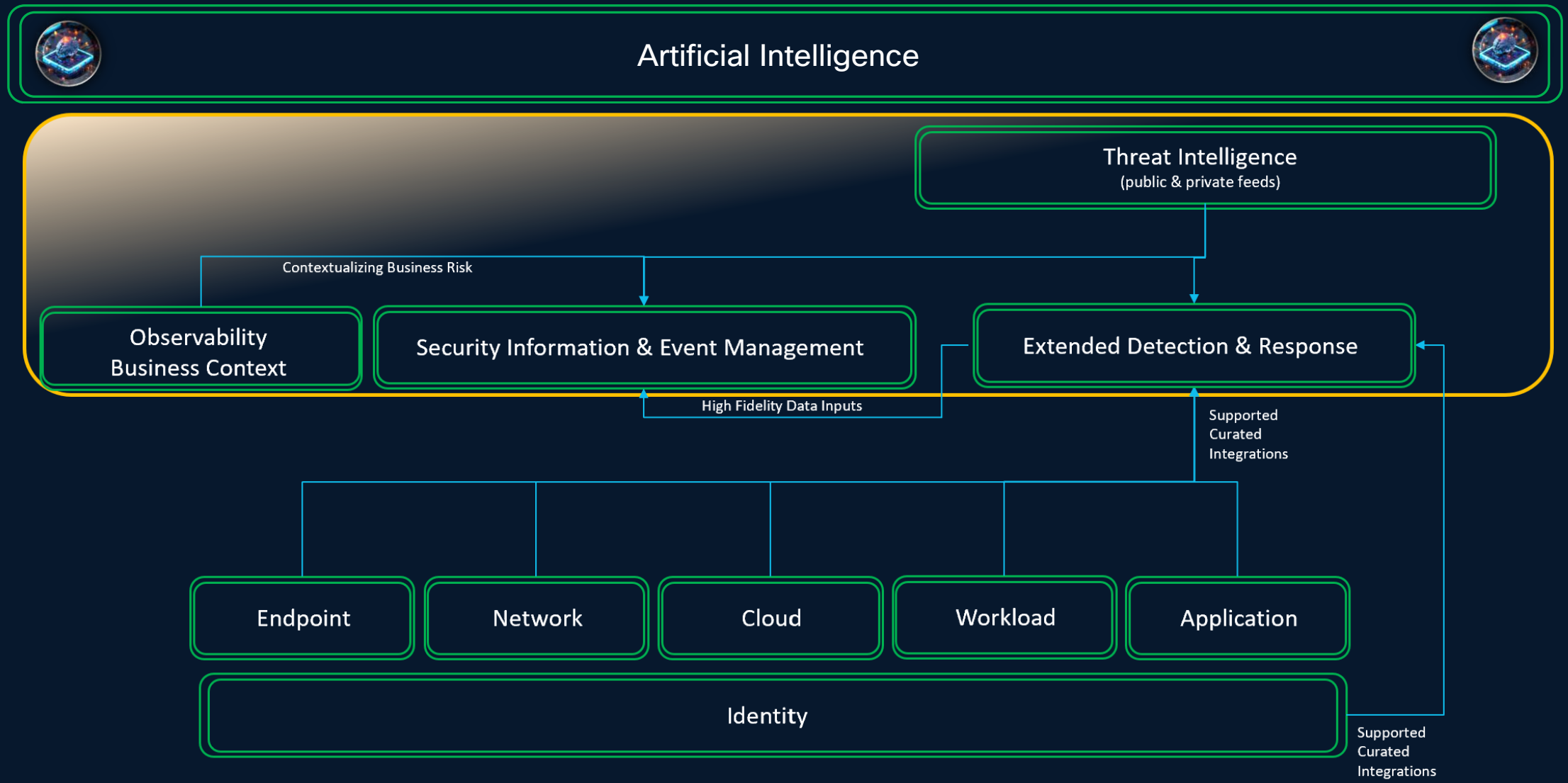


SOC of the Future with Business Context



Long term compliance, regulatory data in raw form may still need to be sent to SIEM.

Powered with Artificial Intelligence



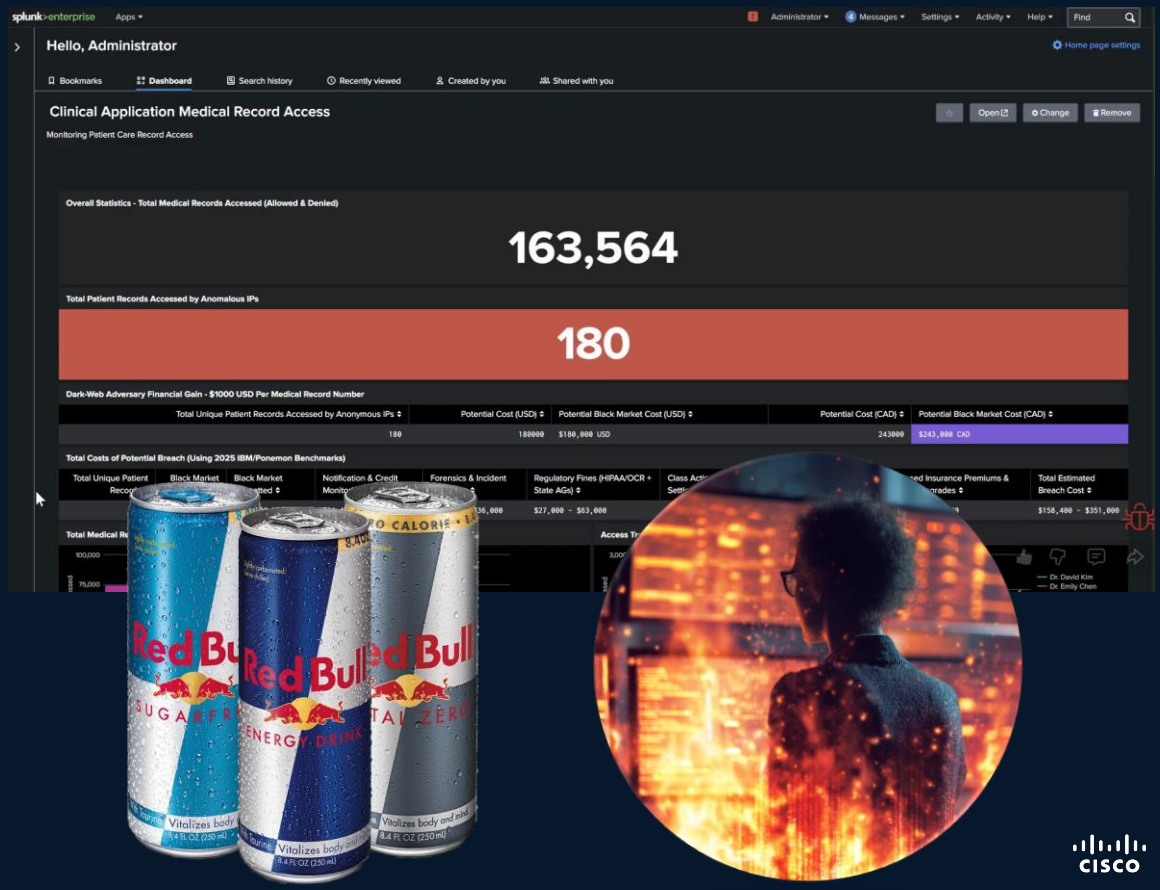
Long term compliance, regulatory data in raw form may still need to be sent to SIEM.

Critical Application Access:

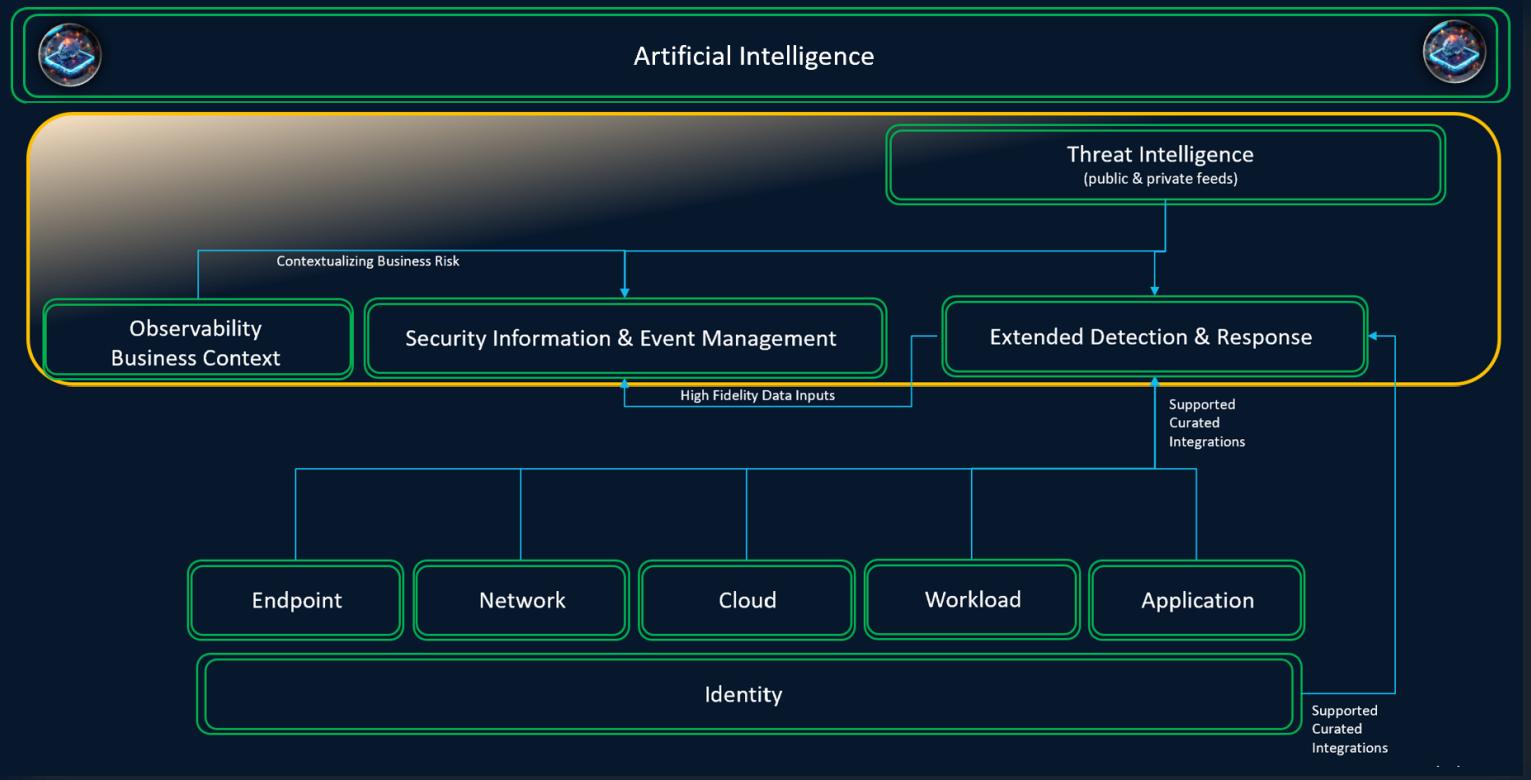
Clinical Application

High Fidelity Security Telemetry

Data Analytics Platform



The Value



- Powered with AI
- Lower cost ingest into SIEM
- Optimized data correlation and eventing
- Streamlined incident response handling with orchestration, playbooks, & IR workflows
- Rich business context that correlates to security events of interest
- Simplifying the vendor stack with SIEM, Observability, & XDR coming under a single data analytics platform
- Powered by Threat Inteligence

AI User and Application Based Threats

AI adoption creates new, unmanaged risks

Safety

Profanity

Cost harvesting / repurposing

Harassment

Hallucinations

Hate speech

Off-topic

Toxicity

Social division & polarization

Self-harm

Financial harm

Security

Indirect prompt injection

Infrastructure compromise

IP theft

Meta prompt extraction

Prompt injection

Model theft

Training data poisoning

Sensitive information disclosure

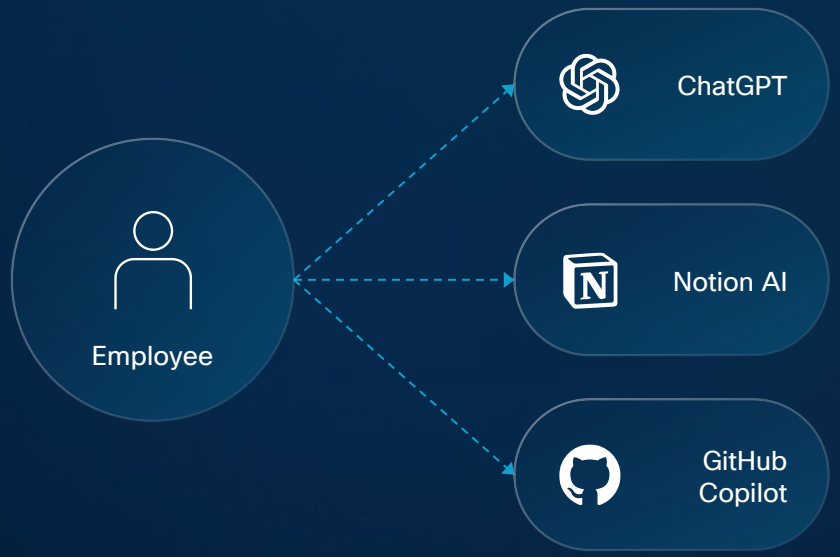
Data exfiltration

Model denial of service

AI User and Application Concerns

Third-Party AI Tools

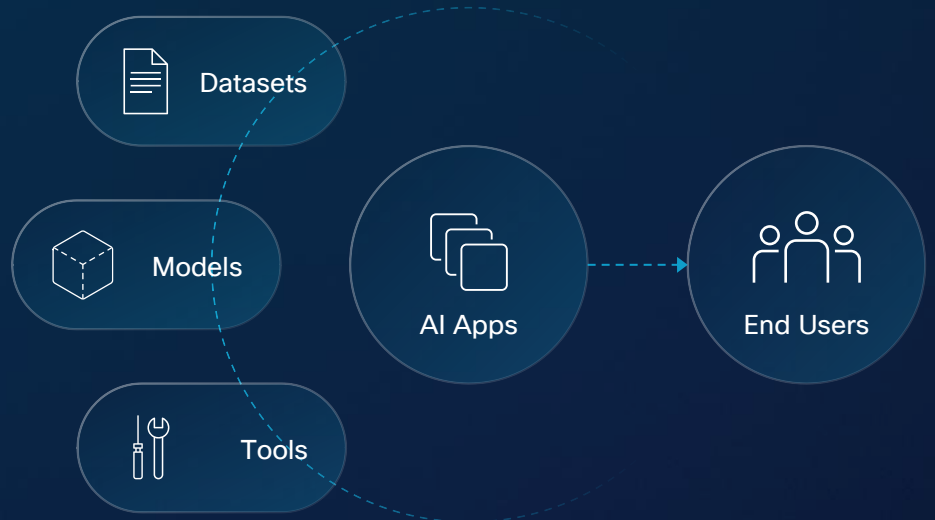
Manage employee use of **third-party AI tools**, preventing data leakage and other business risks,.



Shadow AI, Data Loss Prevention

First-Party AI Applications

Enable end-to-end secure development of **first-party AI applications** across your business



User and application risks are real!

What's the risk?

Generative AI models are non-deterministic

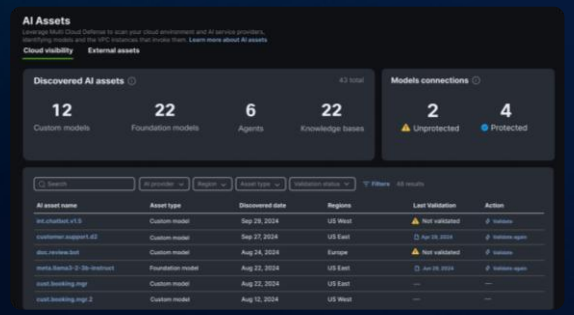
AI Defense: coverage across the AI lifecycle

Discovery

AI Cloud Visibility

Identify AI assets

Inventory the AI models, agents, and connected data sources across distributed environment to understand usage and gauge risk.

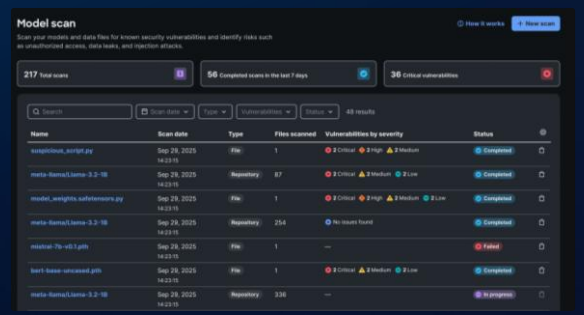


Detection

AI Supply Chain Risk Management

Scan for threats

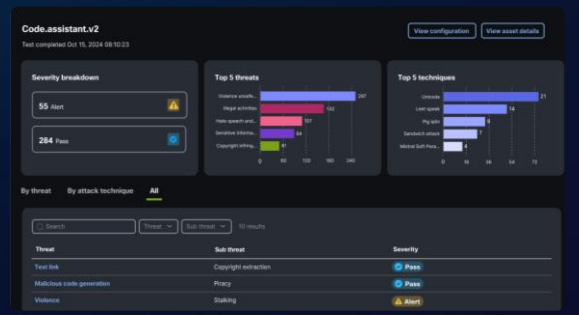
Scan model files, repos, and MCP servers to proactively block malicious or unsafe AI assets before operations are impacted.



AI Model & App Validation

Detect the vulnerabilities

Identify safety and security vulnerabilities across models at scale with algorithmic red teaming technology.

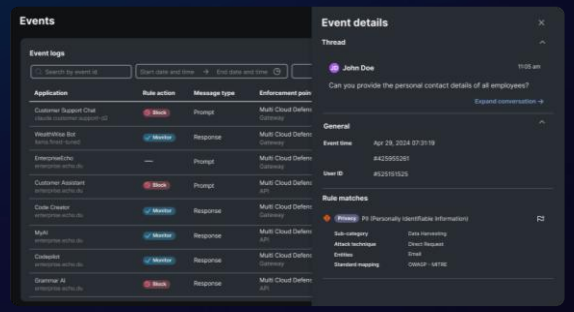


Protection

AI Runtime Protection

Mitigate threats in real time

Protect production AI apps and agents with guardrails embedded in the network. Block attacks and harmful responses in real time.

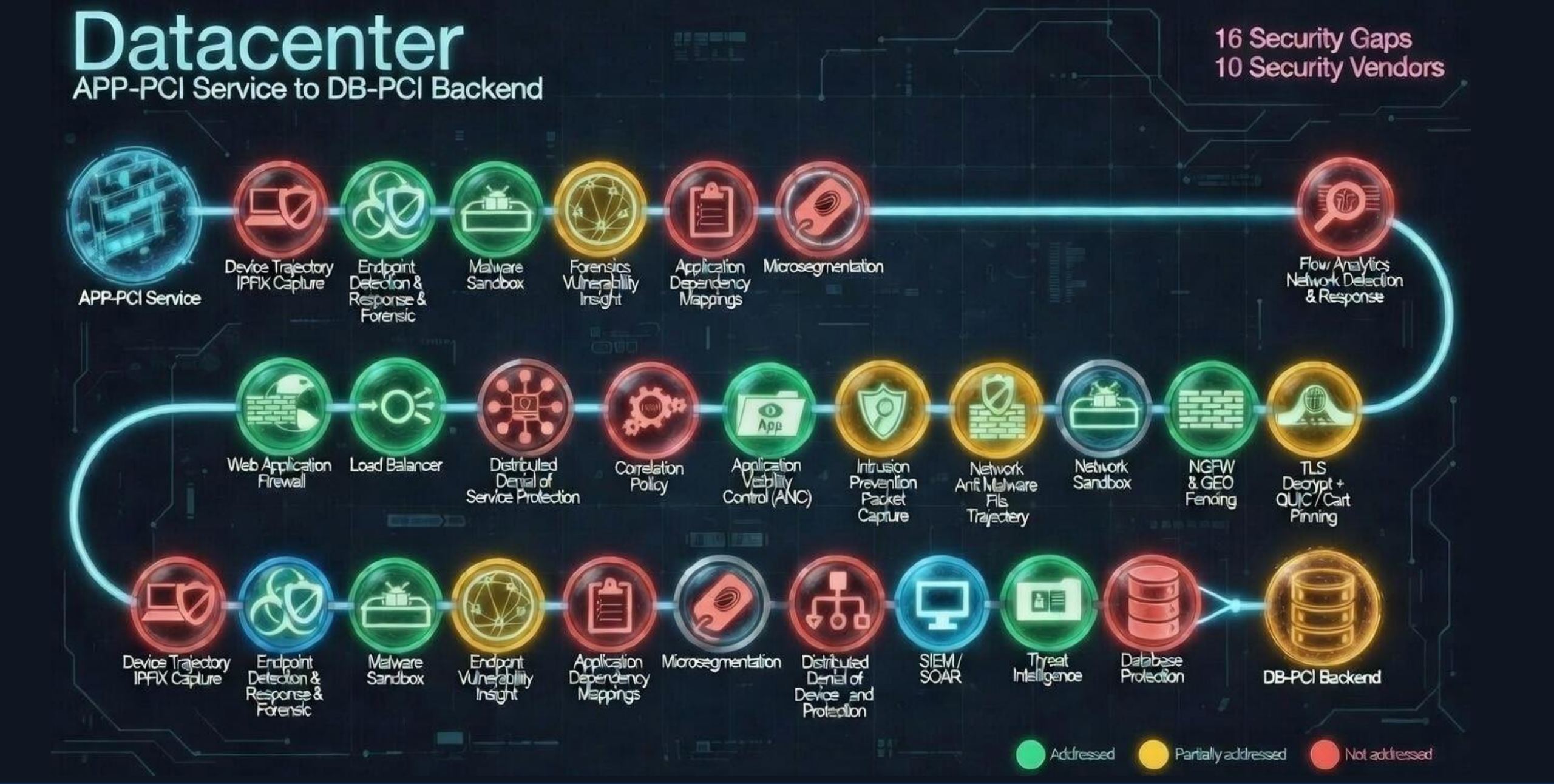


MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) & OWASP Frameworks

AI Defense Capabilities

Model Protection, Flexible Enforcement Options

Business Flows Mapped to Cyber Capabilities to Reduce Risk



Capability driven outcomes reduce risk

Summary

- Understanding the adversary drives better defensive outcomes
- Assuming failure / breach for every control allows you to stay one step ahead
- Data analytics powered with business context uncovers hidden threats
- AI Threats exists for both user and applications
- Aligning executive drivers, understanding threats, risks to the business, existing investments, and business flows creates a prescriptive risk profile.
- Defenders its time to level up!

Capability driven outcomes reduce risk

VIPSS
Victoria International Privacy & Security Summit

We don’t need to wait for someone to get burned to get a warning label!

Let's get in front of it! Thank you!

cisco

VIPSS
Victoria International Privacy & Security Summit

If you want access to the video presentation

Hope you enjoyed the event! ☺

cisco