

# So you got holes in your SOC(k)s

Scott Wofford  
Senior Cybersecurity Solutions Engineer

CCIEEx2 | CISSP  
US Public Sector

Dec 3, 2024



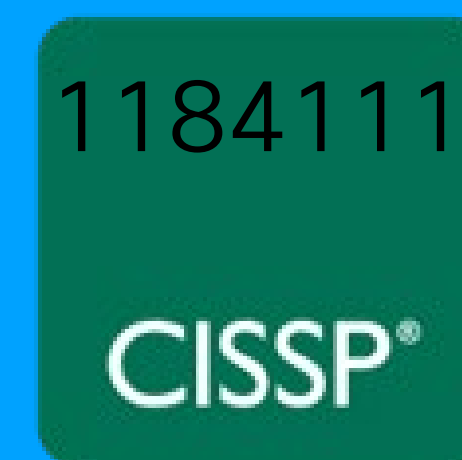
# What we are talking about today

- Whoami
- Security is more than just a thing
- Cisco leading the charge
- Closing thoughts

# About me

Scott Wofford    scwoffor@cisco.com

- SLED Senior SE – Texas, US
- Joined Cisco November 2019
- 20+ Years experience in the IT industry.
- Past roles included Cisco customer, partner, and now Cisco employee.
- Holds an active CCIE Security and Enterprise Infrastructure, CISSP, and various other industry certifications.
- Identity and ISE expert.





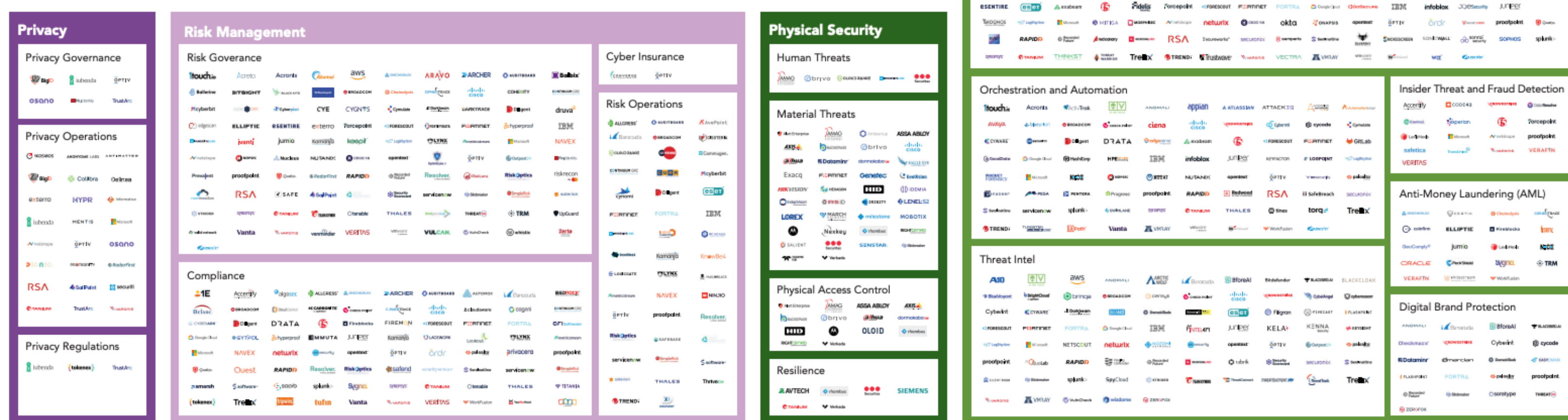
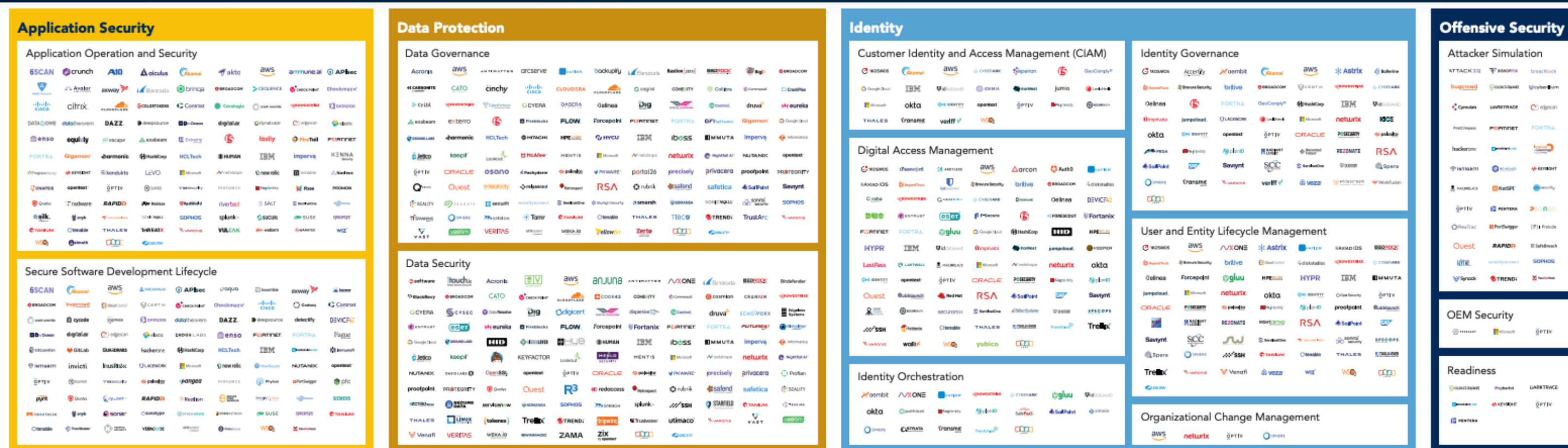


magic  
bullet.®

FAKE

NEWS





Optiv mapped just 450 providers.

Gartner 2024 reports more than 3200 Cybersecurity Vendors

<https://www.optiv.com/sites/default/files/2024-07/Cybersecurity-Landscape-Map-2024.pdf>

<https://digitalisationworld.com/blogs/57542/3200-and-counting-cybersecurity-complexity-is-the-biggest-risk>

# We won't get it right on day one, but...

Continuous Improvement, also known as Kaizen that translates from Japanese as “improvement” (kai – “change” – zen “good”), is ongoing effort to improve existing products, services, or processes by implementing rather smaller than major changes.



## Frequency of Preventable Incidents

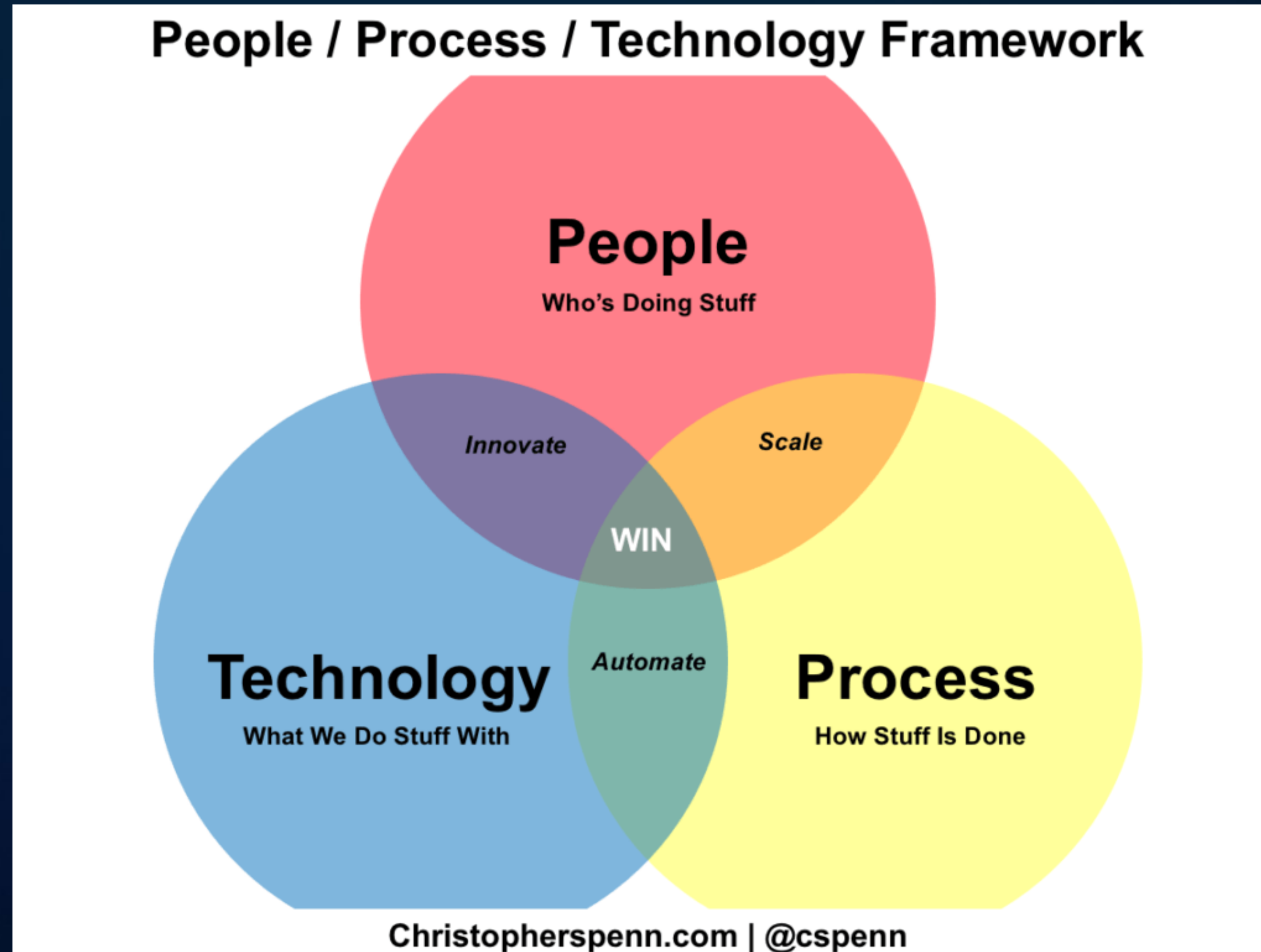
2/3

of security leaders experienced an incident that could have been prevented if security operations were improved.





# FOUNDATIONS





# WE WANT TO WIN

How do we define Success in our SOC

## Why:

What is our company's core focus?

"Why do we do what we do? How does our company define critical assets? What is the value executives place on securing those assets?"

## Measure:

KPIs to measure success

"Do we have a clear definition for measuring ourselves? Can we find success in our losses?"

## Repeat:

Results should be reproducible

"What are we doing to streamline our efforts, so they are efficient and reproducible?"

# GUARDRAILS

## Using Frameworks as a blueprint to Win

### MITRE ATT&CK:

More than just a catalog of TTPs

- \* Training
- \* Response Strategy Development
- \* Security Posture Assessment
- \* Attack Simulation
- \* Threat Detection
- \* And more...

In a nutshell, cyber security teams can now assess their organizations' cyber defenses against the MITRE ATT&CK's body of knowledge – and use this information in decision-making related to developing their security operations center strategy.



# WHY

**“If I had one hour to save the world, I would spend fifty-five minutes defining the problem and only five minutes finding the solution. “**

**– Albert Einstein**

# Why

Can we articulate the need for:

## People:

Do we have the right people to succeed?

“Are we skilled for the appropriate functions?”

“Are we staffed for the expected coverage?”

## Process:

Why are we doing this?

“Can we streamline our workflows?”

“What is the value of a playbook?”

## Technology:

Solutions abound

“Why do we need this or that tool?”

“How does it help meet our objectives?”



# RESTORING FROM BACKUP AFTER A CYBER ATTACK



# MEASURE

**“Measurement is the first step that leads to control and eventually to improvement. If you can’t measure something, you can’t understand it. If you can’t understand it, you can’t control it. If you can’t control it, you can’t improve it.”**

**– H. James Harrington**



# MEASURE

How are we doing? Inquiring minds want to know

## People:

Tracking metrics that matter

“Personal Development”

“Staff workload”

## Process:

Is there room to refine

“How are we evaluating our processes for efficiency?”

“Do we have a plan to test and institute change?”

## Technology:

Does this thing work?

“How well does a widget do it’s job?”

“Is it adding added value to the security stack?”

# MEASURE SOC Performance

MTTD – Mean time to Detect

MTTR – Mean time to Resolution

Incident Escalation Rate

Number of Security Incidents

F(PN)R – False positive and negative rates

Incident Escalation Rate

Incident Containment Rate

Incident Closure Rate



# REPEAT

**“If you always do what you’ve always done, you’ll always get what you’ve always got.”**  
– Henry Ford

# REPEAT

What are we doing to get outcomes we want?

## People:

What works?

“Is the culture setup for success?”

“Are we investing in our people?”

## Process:

Defining success

“Are processes documented?”

“Are they structured for modularity?”

## Technology:

Accelerated Outcomes

“Where can we integrate?”

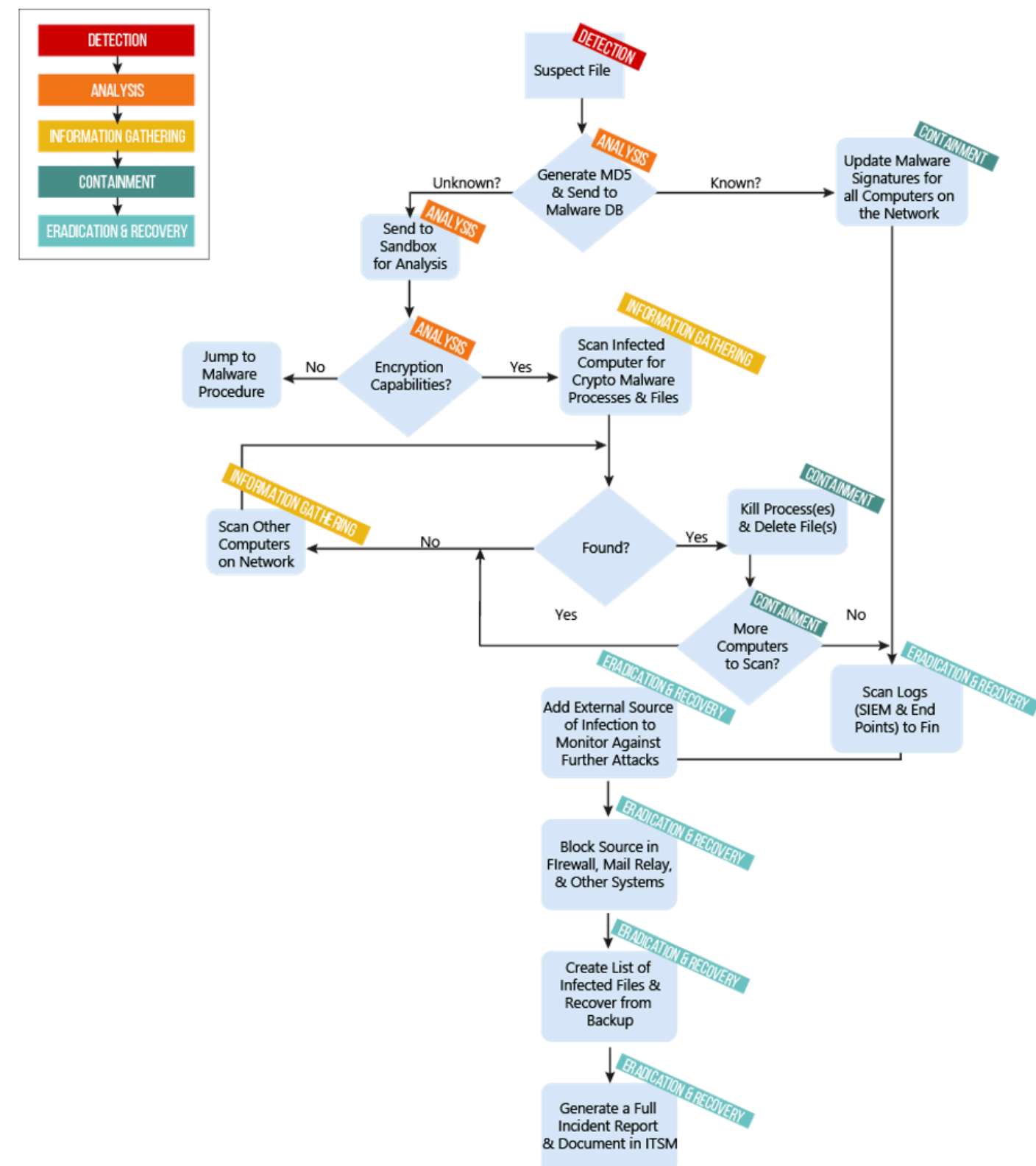
”How do we Automate?”

← Measure →



# Playbooks & Workflows

## RANSOMWARE INFECTION PROTECTION



## CRYPTOJACKING

**Objective:** Automatically detect cryptojacking activity, isolate infected systems, and block cryptojacking domains.

### Tools Required:

- **SIEM:** (e.g., Splunk, QRadar)
- **EDR (Endpoint Detection and Response) Tools**
- **Firewall**
- **SOAR Platform:** (e.g., Palo Alto Cortex XSOAR, Splunk Phantom)
- **Threat Intelligence Platforms:** (e.g., VirusTotal, DomainTools)

### Steps to Implement the Automation:

#### Step 1: Detection

- **Trigger:** Monitor the SIEM and EDR tools for alerts related to cryptojacking indicators (e.g., abnormal CPU usage, unauthorised mining software, outbound connections to known mining pools).
- **Automation Task:** Use predefined correlation rules to detect cryptojacking activity. For example, if the SIEM detects consistent high CPU usage from a specific endpoint along with outbound connections to a mining pool, it triggers the playbook.

#### Step 2: Triage and Analysis

- **Trigger:** Once cryptojacking is detected, automatically extract Indicators of Compromise (IOCs) such as malicious file hashes, domains, and IPs related to cryptojacking.
- **Automation Task:** The SOAR platform automatically enriches the IOCs with threat intelligence from external sources (e.g., VirusTotal, DomainTools) to confirm the cryptojacking activity.

#### Step 3: Containment

- **Trigger:** After confirming cryptojacking, initiate automated containment actions.
- **Automation Task:**
  - **Isolate Infected Systems:** Command the EDR tool to disconnect the infected endpoints from the network to prevent further cryptojacking activity.
  - **Block Domains:** Update firewall rules to block outbound traffic to known cryptojacking domains and mining pools.



How is  
Cisco + Splunk is  
helping you stitch up your  
holes?





Threat actors do not discriminate based on an organization's size or vertical.



# Driving security modernization

across detection, investigation, and response as a top priority to achieve digital resilience.



of organizations claim improving efficacy and efficiency of SecOps is a top 5 priority.

Source: [ESG SOC Trends Report 2023](#)



# Cisco Delivers

The right partners matter!

## People:

World-class experts

“Experts across multiple domains”

## Process:

Partners in process

“Customized security operations for the SOC and TDIR”

”Well articulated and clearly defined”

## Technology:

Solutions not just widgets

“Architected and engineered to work together and drive success”

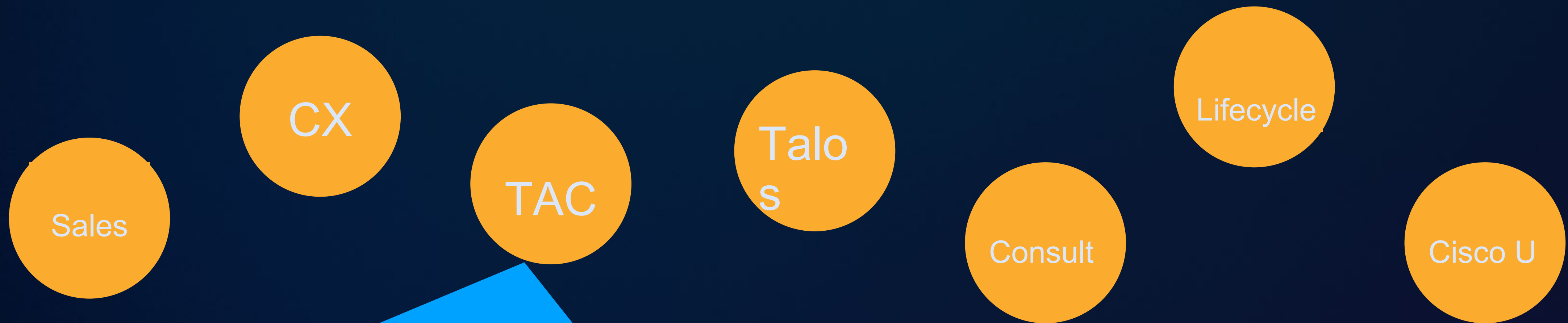


# People



# People & Process

The right partners matter!



We have 3 main priorities going forward in TAC.

1. Provide personalized support
2. Proactive and preventative support
3. Develop future ready skills for our engineers.

We have initiatives that support all 3 that include fundamental focus areas like

'Radical Ownership'  
Technology alignment  
AI and Automation everywhere



Scale and  
persistence of  
threats vary

Driving the need  
for a tailored cyber  
defense strategy.





# Product

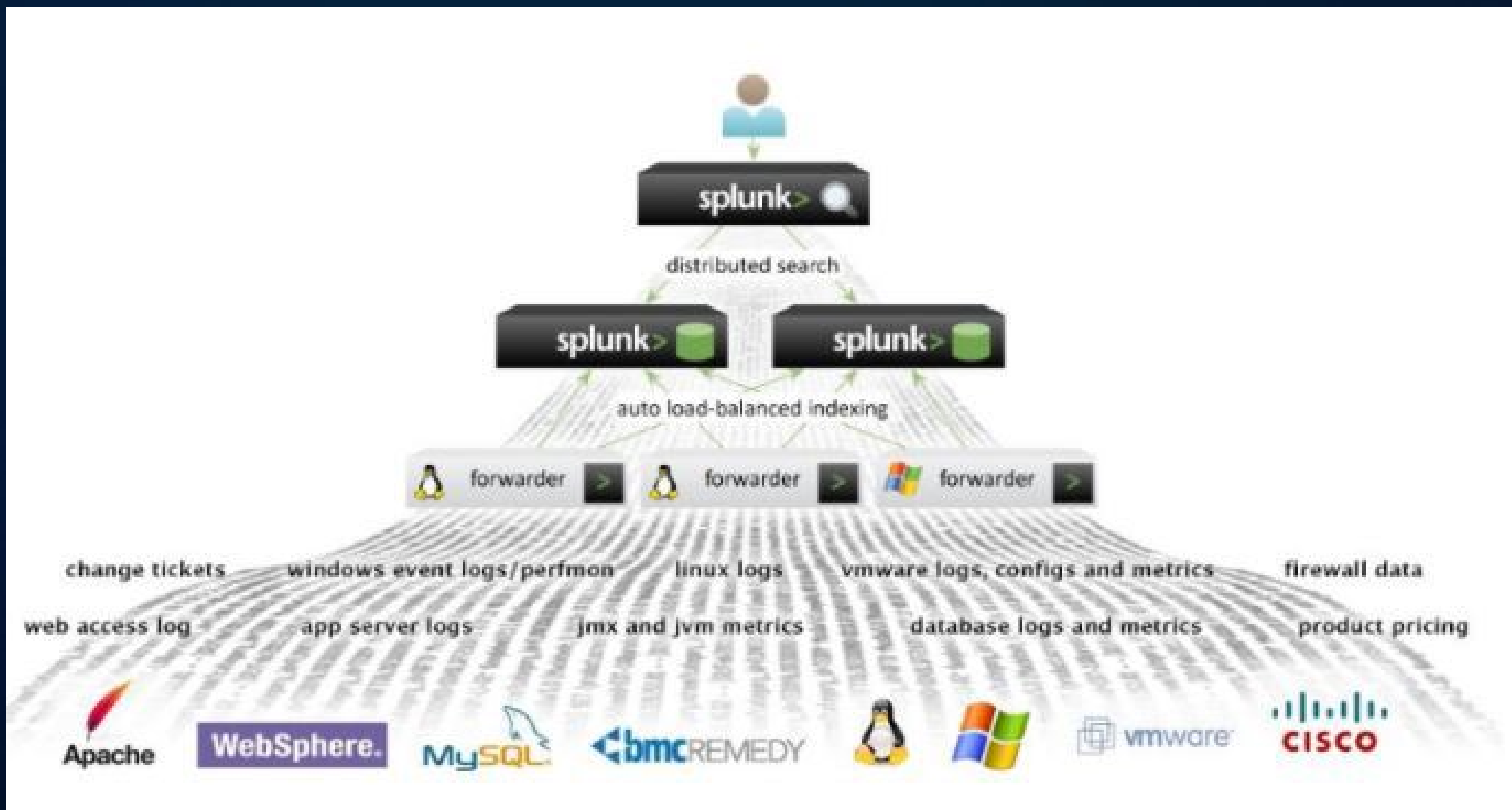
Yes, tools generate a lot of data

The image displays a comprehensive grid of 24 panels, each representing a different cybersecurity or IT domain. Each panel is color-coded and contains a title, a sub-title, and a collection of company logos. The domains are as follows:

- Application Security** (Yellow): Application Operation and Security, Secure Software Development Lifecycle.
- Data Protection** (Orange): Data Governance, Data Security.
- Identity** (Blue): Customer Identity and Access Management (CIAM), Identity Governance, Digital Access Management, User and Entity Lifecycle Management, Identity Orchestration, Organizational Change Management.
- Offensive Security** (Dark Blue): Attacker Simulation, OEM Security, Readiness.
- Infrastructure Security** (Light Blue): Cloud Security, Network Security, OT and ICS, Endpoint Security, IoT.
- Operations** (Green): Analytics, Incident Response, Threat Detection and Response, Orchestration and Automation, Insider Threat and Fraud Detection, Anti-Money Laundering (AML), Digital Brand Protection.
- Privacy** (Purple): Privacy Governance, Privacy Operations, Privacy Regulations.
- Risk Management** (Light Purple): Risk Governance, Risk Operations, Compliance, Cyber Insurance.
- Physical Security** (Dark Green): Human Threats, Material Threats, Physical Access Control, Resilience.

# Splunk Core

Let's get organized!





# Splunk Reporting & Dashboards

## Defender 365 Overview



### Incident Summary



severity	New	InProgress	Resolved	Total
high	1345	3	9	1357
medium	607	10	35	652
low	748	738	833	2319
informational	3007	218	809	4034
	5707	969	1686	8362

### Incident Timeline - 30d



### Incident Disposition Stats

True Positives	False Positives	Not Specified
752	17	7,593
9.0%	0.2%	90.8%

### Incident Assignments

assignedTo	New	InProgress	Resolved	Total
Automation	0	864	727	1591
	0	0	3	3
	1	0	2	3
null	5688	109	968	6765
	5689	973	1700	8362

### MITRE ATT&CK Techniques by Entity Type





# Splunk Security Essentials

## Consultant in a box...

The screenshot displays the Splunk Security Essentials web interface. At the top, there is a navigation bar with the Splunk logo, 'enterprise' branding, and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this is a secondary navigation bar with 'Home', 'Security Content', 'Analytics Advisor', 'Security Operations', 'Data', 'Advanced', 'Documentation', and 'Configuration'. The main content area is titled 'Security Content' and includes a search bar, a 'Learn how to use this page' button, and filter options for 'Journey', 'Security Use Case', 'Category', 'Data Sources', and 'Featured'. Below the filters, there are more specific filters for 'ATT&CK Tactic', 'ATT&CK Technique', 'ATT&CK Threat Groups', 'CIS', and 'NIST'. The main content area is titled 'Stage 1: Collection' and contains a grid of search results. Each result card includes a title, a brief description, and a 'Featured' badge. The results are as follows:

Search Title	Description	Tags
Access to In-scope Resources	Visibility into who is accessing in-scope resources is key to your GDPR efforts. Splunk allows easy analysis of that information.	Featured, Searches Included
Access to In-Scope Unencrypted Resources	Unencrypted communications leaves you vulnerable to a data breach -- when users access PII data, ensure that all connections are encrypted.	Featured, Searches Included
Authentication Against a New Domain Controller	A common indicator for lateral movement is when a user starts logging into new domain controllers.	Featured, Searches Included, Lateral Movement, Remote Services
Basic Brute Force Detection	Uses a simple threshold for Windows Security Logs to alert if there are a large number of failed logins, and at least one successful login from the same source.	Featured, Searches Included, Credential Access
Basic Malware Outbreak	Looks for the same malware occurring on multiple systems in a short period of time.	Featured, Searches Included, Initial Access, Execution, Privilege Escalation
Basic Scanning	Looks for hosts that reach out to more than 500 hosts, or more than 500 ports in a short period of time.	
Basic TOR Traffic Detection	The anonymity of TOR makes it the perfect place to hide C&C, exfiltration, or reconnaissance purposes.	
Credentials In File Detected	Adversaries may dump credentials into local files using OS Credential Dumping or credentials might have	
Endpoint Uncleaned Malware Detection	Detect a system with a malware detection that was not properly cleaned, so they escape high risk	
Flight Risk Web Browsing	This search implements several heuristics to look for indications that a user is a flight risk from Web	

# Product & Process

Different approaches, optimized for different things

Extensibility  
Data Sources,  
Integrations

## XDR

- Curated data
- Limited duration
- Targeted automations

## SIEM & SOAR

- Any source, at scale
- Extended storage
- Flexible workflows

Customizability  
Detections, Investigation, Response

# ...and solving different problems

## XDR:

Great at notifying you  
of an incident

“PowerShell created an internal  
network connection never seen  
before. This might be ransomware!!!”

## SIEM:

Great at answering  
complex questions

“View prioritized alerts based on risk  
from our U.K. subsidiary.”

## SOAR:

Great at automating workflows  
& response actions

“Initiate a password reset for all  
U.K. employees.”

“Quarantine the affected endpoint  
and take a snapshot of all our data  
center servers.”



# Creating a more efficient and responsive threat detection, investigation, and response capability

Splunk + Cisco

## XDR:

Foundational  
Detection &  
Response



Real-time attack  
chain detection for  
the most common  
attacks



Best course  
of action  
& guided  
response



Expanded  
Retention



Risk based  
detection



Proactive  
threat hunting



Automation &  
orchestration



SOC  
playbook



Lifecycle automation  
and optimization

## SIEM:

Broadening  
Insights

## SOAR:

Unlimited  
Automation

Unified TDIR:  
Maximize SOC  
Efficiency

SOC Journey

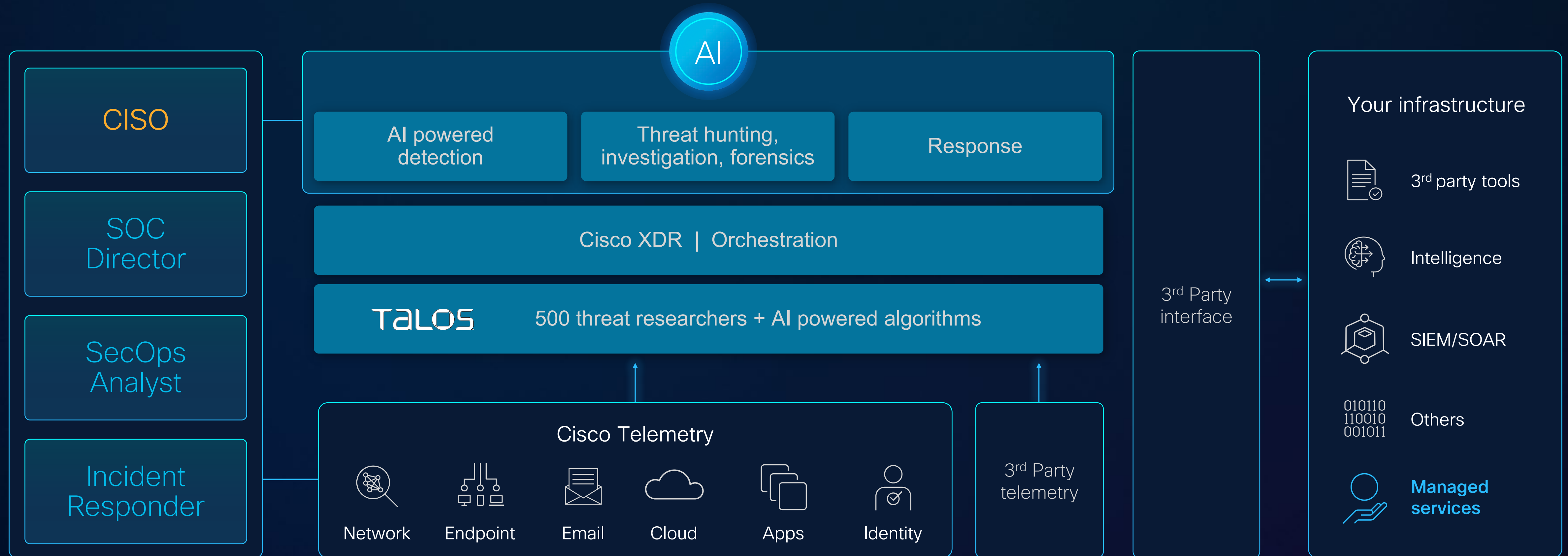
People  
+  
Process  
+  
Technology  
=





We can meet you  
wherever you are  
on this journey

# Start with the fastest, easiest solution with an AI-first XDR

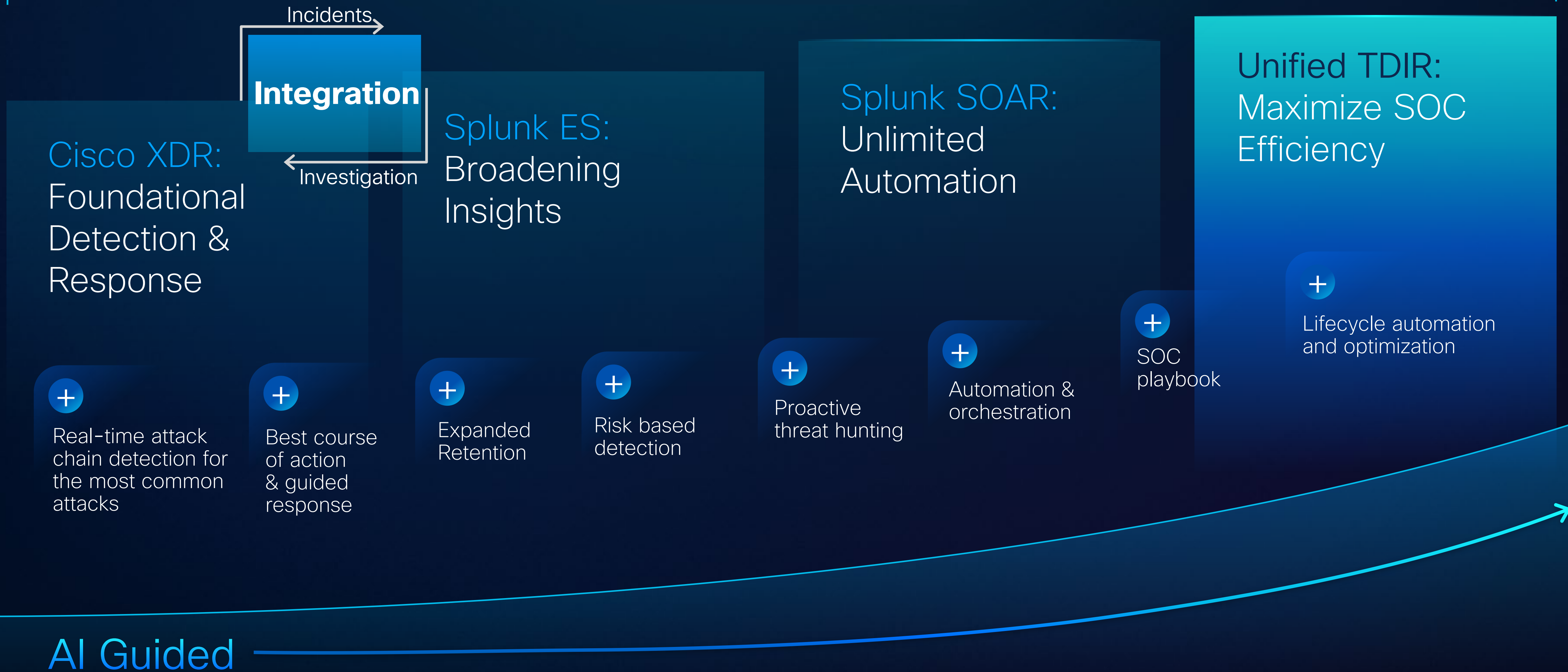


Real-time attack chain detection for the most common attacks with curated integration and response guidance



# Investment protection for Cisco XDR. Even better threat signal for Splunk ES.

## Splunk + Cisco



## How adoption of **AI** in SOC operations impacts SOC's performance:

- Reduction in mean time to remediation
- Significant decrease in response times
- Enhanced visibility into the scope of incidents and affected systems
- Broadened detection and response capabilities
- Expanded technical security proficiency
- Streamlined and unified threat responses



# Enabling powerful security outcomes for our customers



<15min

Execute a  
phishing  
investigation

90%

reduction  
in alert  
volumes.

5x

faster detection  
& response to  
threats

# Cisco XDR + Splunk

AI driven | Platform powered | Extensible



# To close...

**Kaizen – Always be looking to hone and refine**

## Be intentional

- People – Cultivate a culture where people are invested
- Process – Continue to evaluate and adjust processes
- Technology – Invest in complimentary technology

## Measure

- Identify metrics that matter and have a passion to win



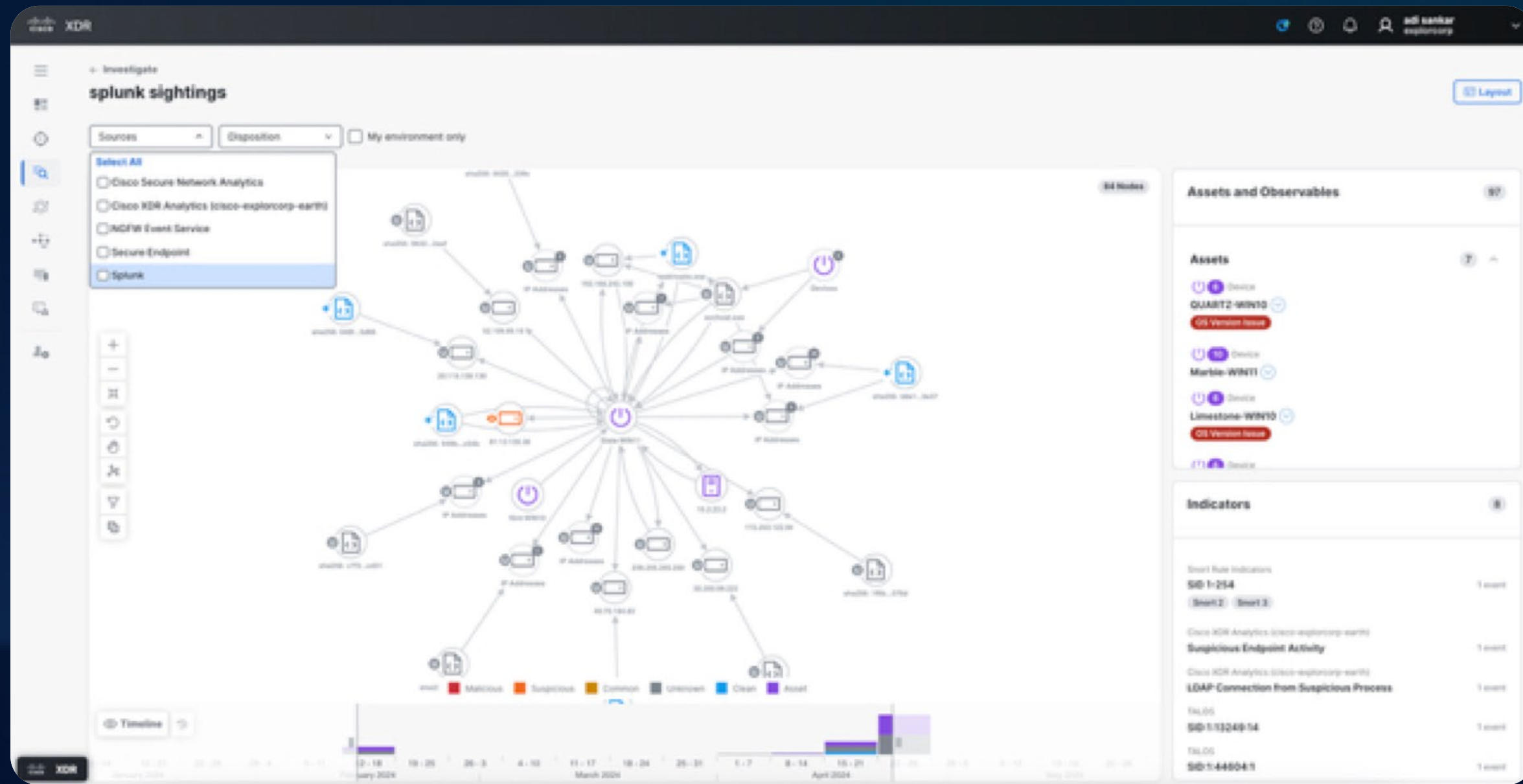
# Appendix



Use case

# Expand visibility across domains

FUTURE



Seamless collaboration for threat identification, action, and investigations

Leverage verdicts from Splunk for correlated verdicts on indicators of compromise

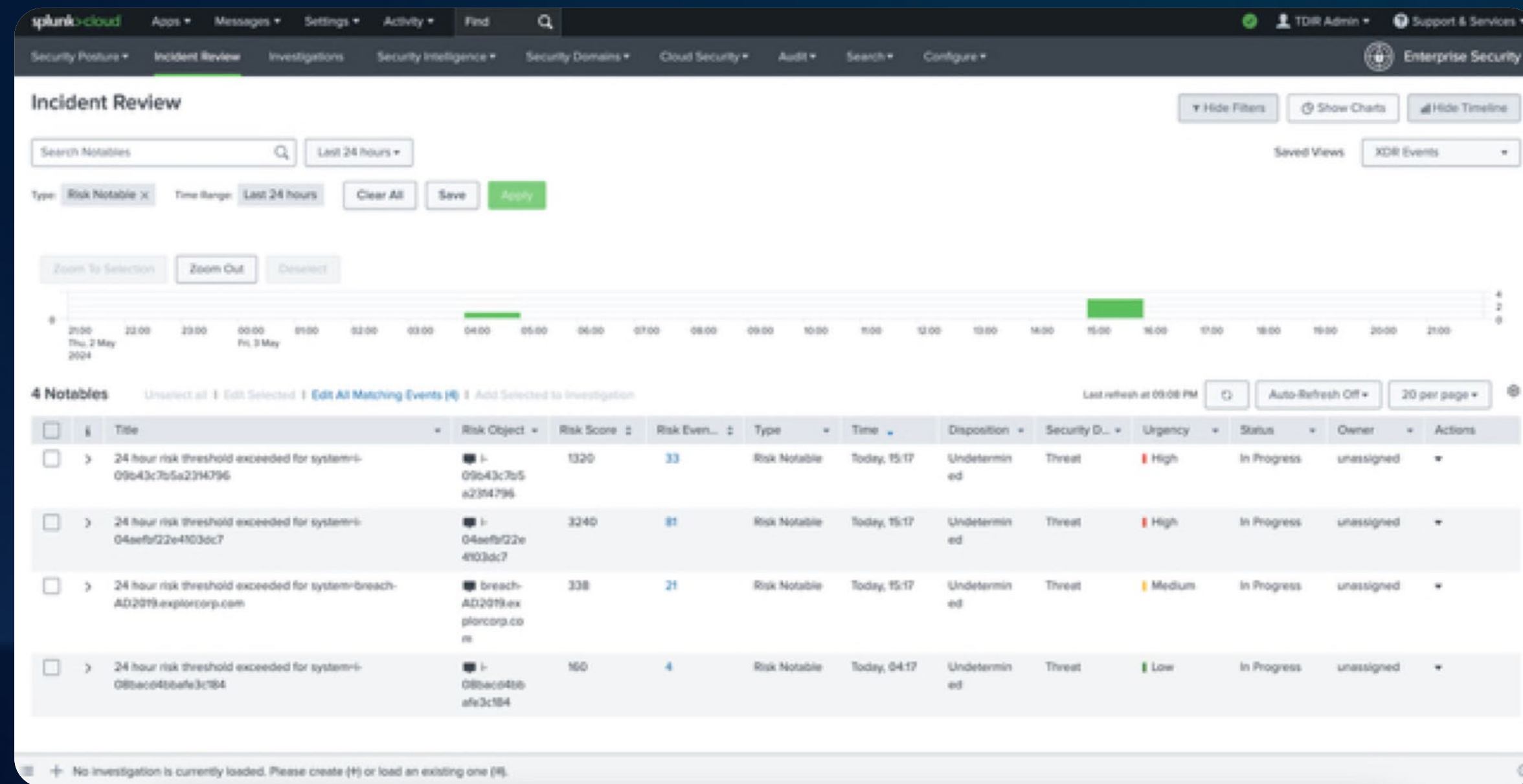
**Integrating Cisco XDR with Splunk ES for Enhanced Security Analysis**

Use case

# Deliver higher fidelity alerts for investigation and analysis

FUTURE

Facilitate efficient analysis and mitigation of security threats with context from multiple sources



Promote incidents detected by Cisco XDR to Splunk ES, allowing SOC analysts to view and analyze incidents

**Integrating Cisco XDR with Splunk ES for Enhanced Security Analysis**