CISCO Engage | Tech Day Charlotte

# Transforming Security Operations to Punch Above Your Weight Class

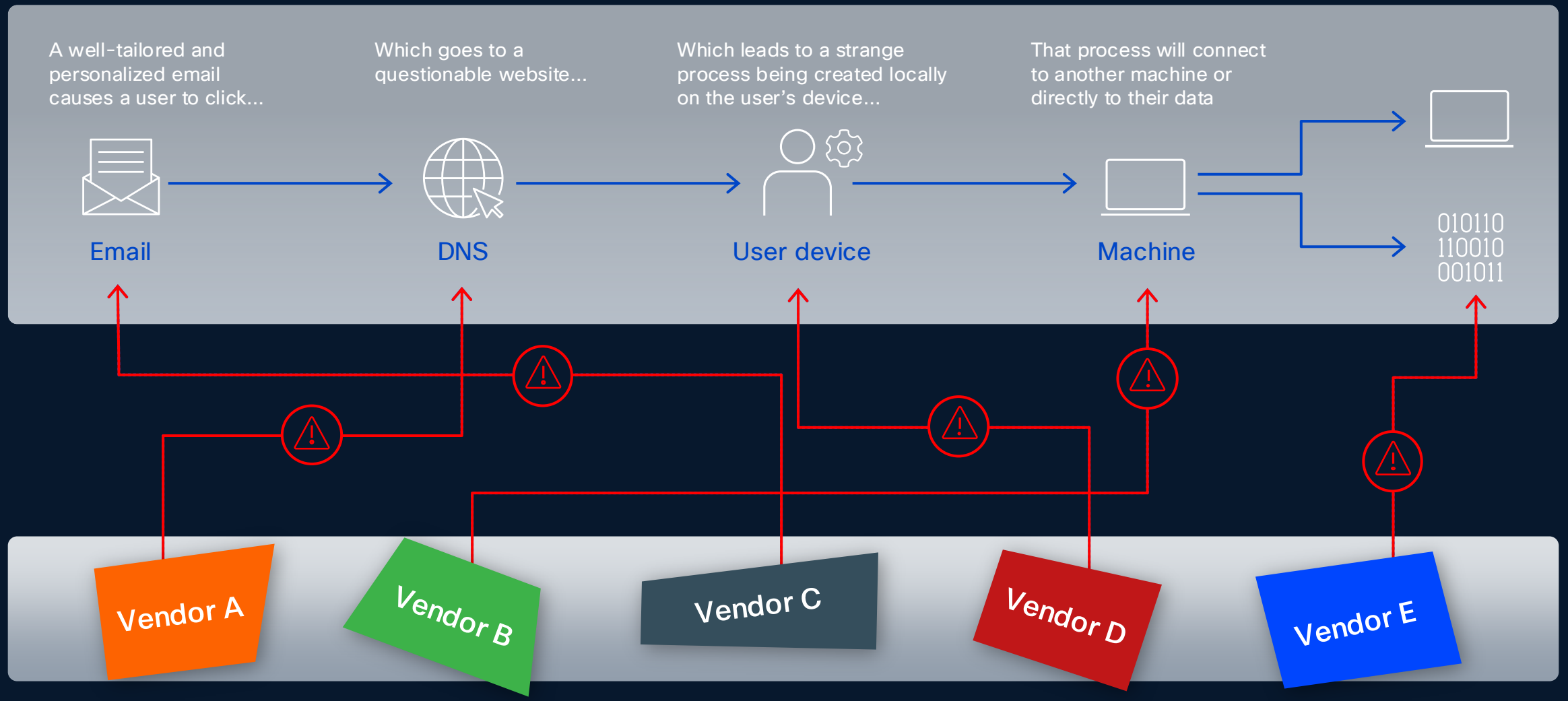
## Stronger Together: Elevate Your Security Game with Cisco and Splunk Integration

Jamey Heary
Chief Security Architect, DSE

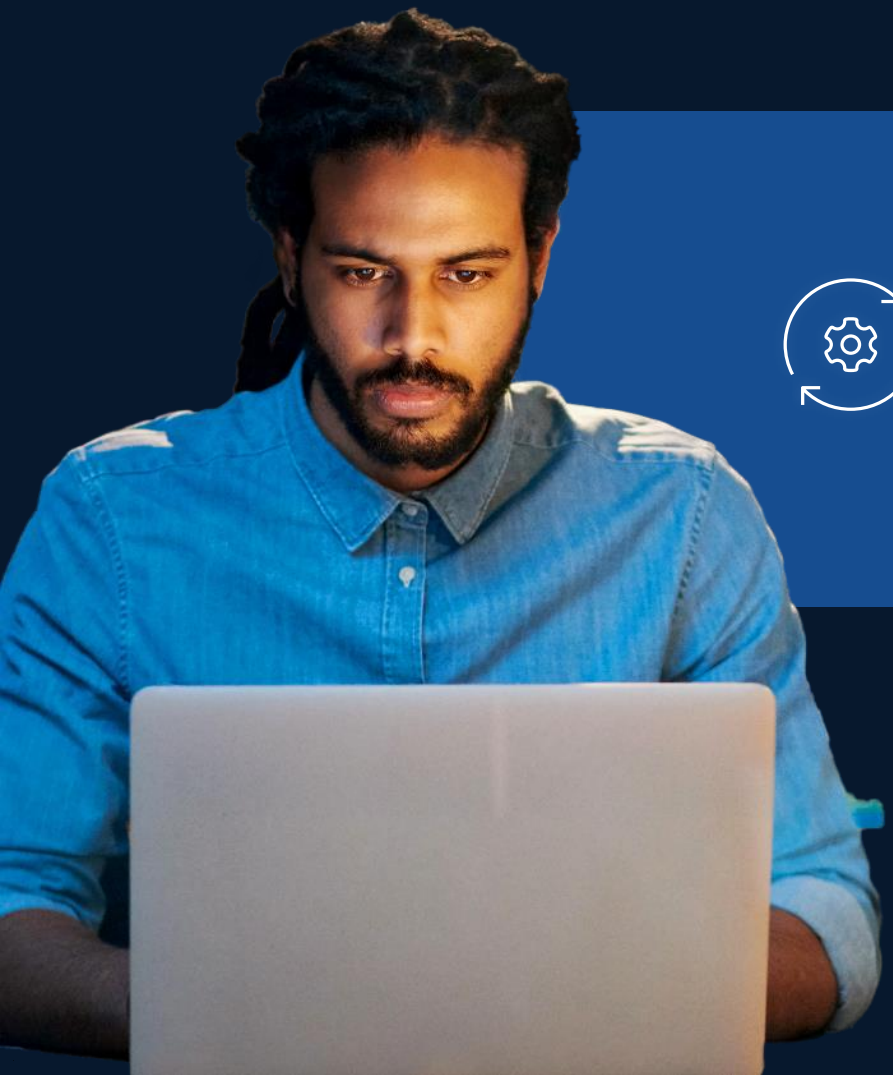
March 31, 2026

# The Problem

# Ransomware Campaigns are Multi-Vector



# Your Challenges



Limited Staff vs 24/7 threats

Network blind spots

Alert Fatigue Tool Crawl

Manual investigation delays

Security is a problem of plenty

# What Security Operations Wants

"I want to have a correlated view of alerts across my environment."

"I need my security tools to help me work with speed, accuracy, and confidence."

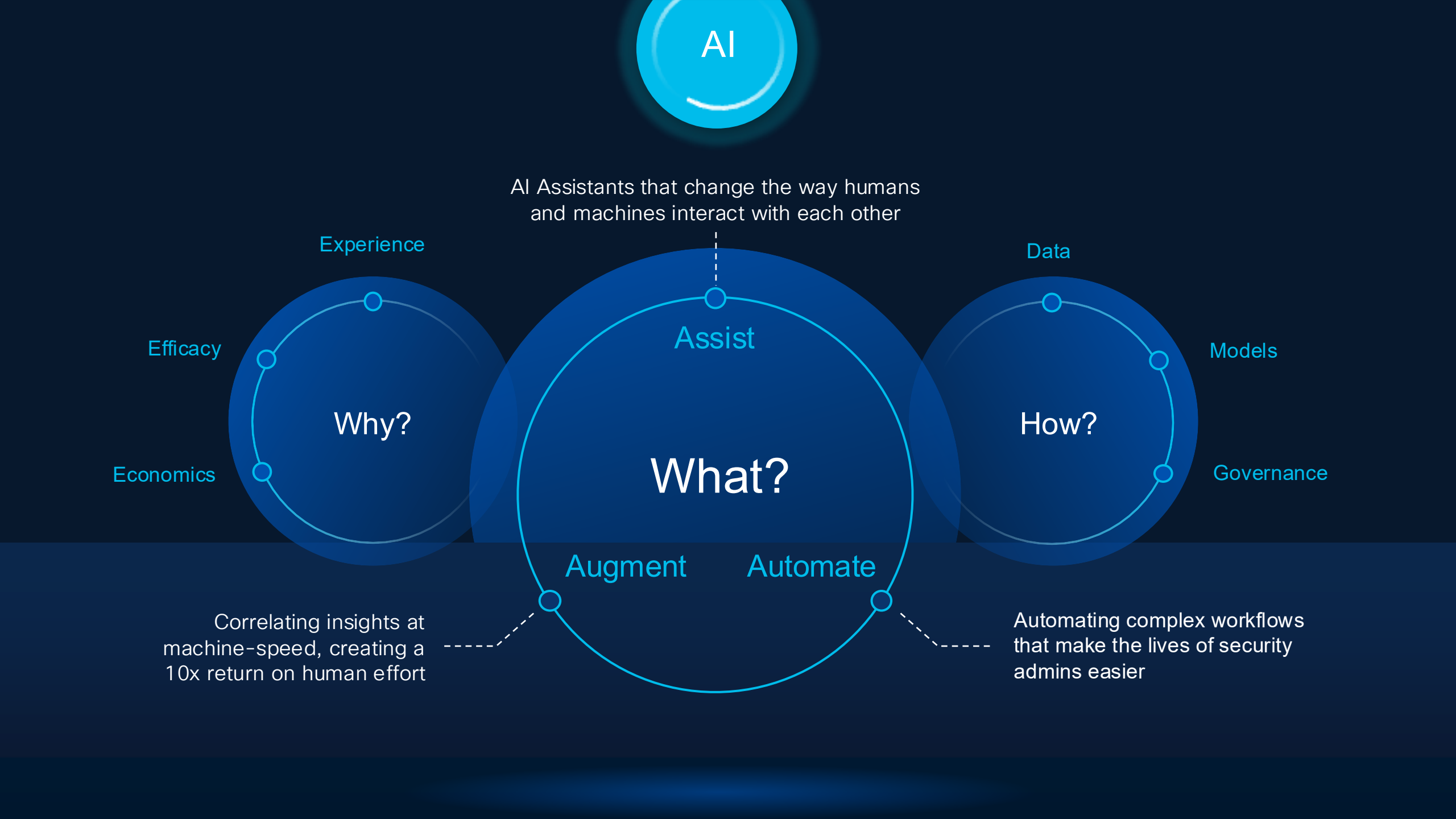
"I want my team to remediate threats with guidance and automated playbooks."



cisco

# Centralization with a unified SOC platform

# Using AI: Fighting for an Unfair Advantage


AI
AI Assistants that change the way humans and machines interact with each other
Experience
Efficacy
Economics
Why?
Assist
What?
Augment
Automate
Data
Models
Governance
How?
Correlating insights at machine-speed, creating a 10x return on human effort
Automating complex workflows that make the lives of security admins easier

# We Are Leveraging AI Across The Portfolio

Assist

Augment

Automate

## AI Assistant Experience

Give your admins superpowers.
Simplify management, improve outcomes.

## AI Powered Detection

Correlate 550B security events at machine-speed.

## Autonomous Actions

Learn from human-to-machine interactions to automate complex playbooks.

Cisco Security Cloud

Breach Protection

User Protection

Cloud Protection

Firewall Foundation



cisco

# AI-driven Security Operations

Unified Threat Detection, Investigation & Response (TDIR)

# Journey to the self-driving SOC

## Foundational AI

AI used to detect & prioritize incidents

## AI Assists

AI provides insights & recommendations, but humans make all decisions.

AI flags a suspicious login pattern and recommends an investigation path.

## AI Augments

Human in the loop, AI automates actions

AI automatically escalates high-fidelity threats and drafts response actions for human review

## Autonomous SOC

AI detects, investigates, and mitigates threats end-to-end

AI acts without human involvement, except in edge cases.

# XDR: Instincts and Fundamentals in the Ring

# Our open XDR integrates with other security tools

Cisco XDR has curated integrations with the top best-of breed security vendors

## Cloud Telemetry

Amazon Web Services, Google Cloud Platform, Microsoft Azure, Oracle Cloud Infrastructure

Cisco Talos: Unrivaled collection of actionable intelligence for known and emerging threats

## Endpoint Telemetry

Cisco Secure Endpoint, CrowdStrike, Cybereason, Microsoft Defender, Palo Alto Networks, SentinelOne, Trend Micro

Identifies tactics, techniques, and procedures (TTPs) used


## Firewall Telemetry

Cisco Secure Firewall Threat Defense, Cisco Meraki MX, Check Point, Fortinet, Palo Alto Networks

## Network Telemetry

Cisco Secure Network Analytics, Darktrace, ExtraHop

## Apps/Email Telemetry

Cisco Email Threat Defense, Microsoft 365, Proofpoint

Prioritizing threats based on impact to the business

# Telemetry data source importance

The top six data sources that customers believe are essential for XDR are:
Endpoint, Network, Firewall, Identity, Email, and DNS

Essential

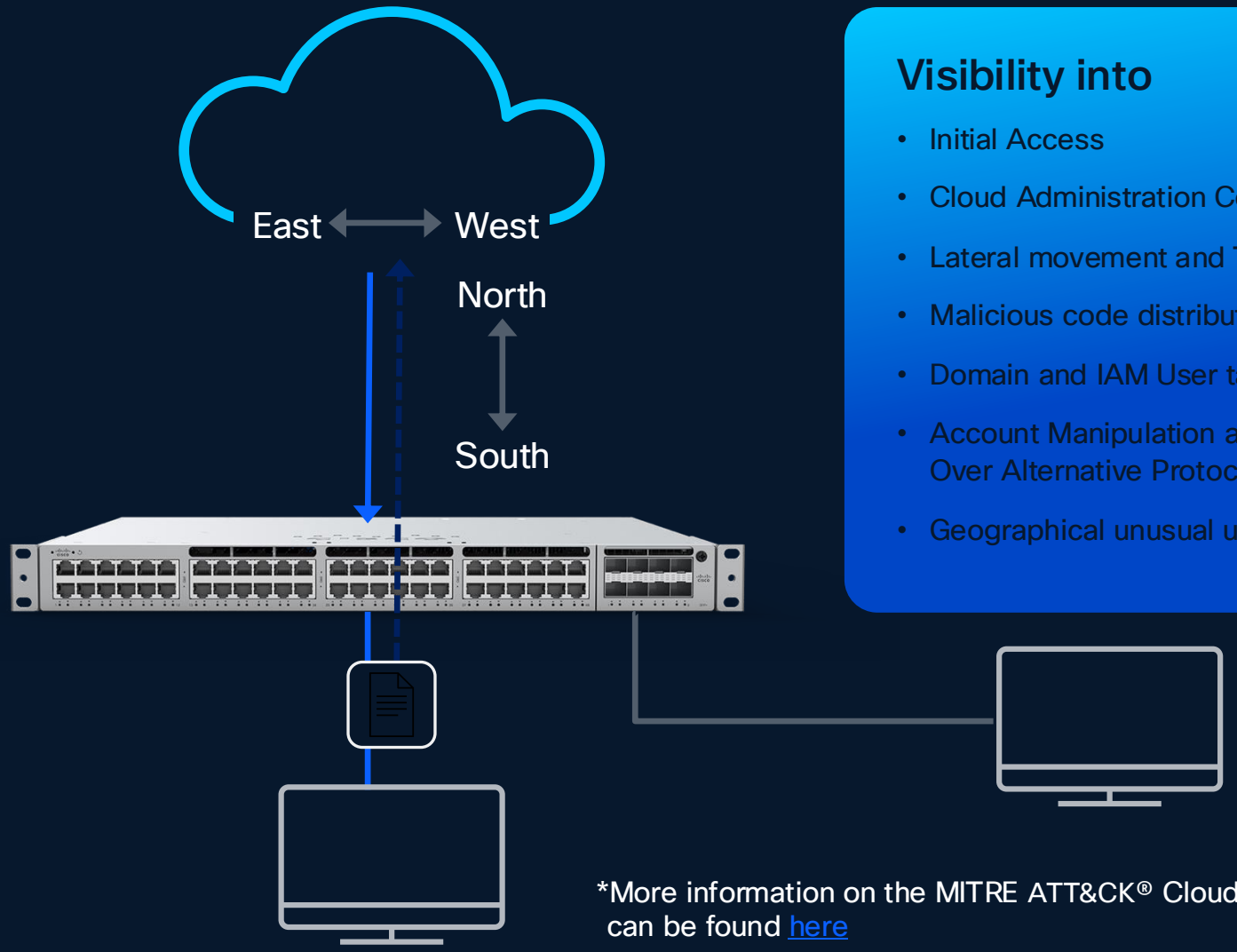
| | Count | Share |
|---|---|---|
| Endpoint | 255 | 85.0% |
| Network | 226 | 75.3% |
| Firewall | 207 | 69.0% |
| Identity | 191 | 63.7% |
| Email | 179 | 59.7% |
| DNS | 140 | 46.7% |
| Public Cloud | 137 | 45.7% |
| Non-Security Sources | 36 | 12.0% |

Cisco SOC of the future

# The value with built-in cloud native NDR

## Visibility into

- Indicators of compromise
- Malicious outbound/inbound behavior
- Command and control / heartbeat tracking
- More and more traffic is northbound due to cloud services like SaaS, PaaS, IaaS, Kubernetes, etc.



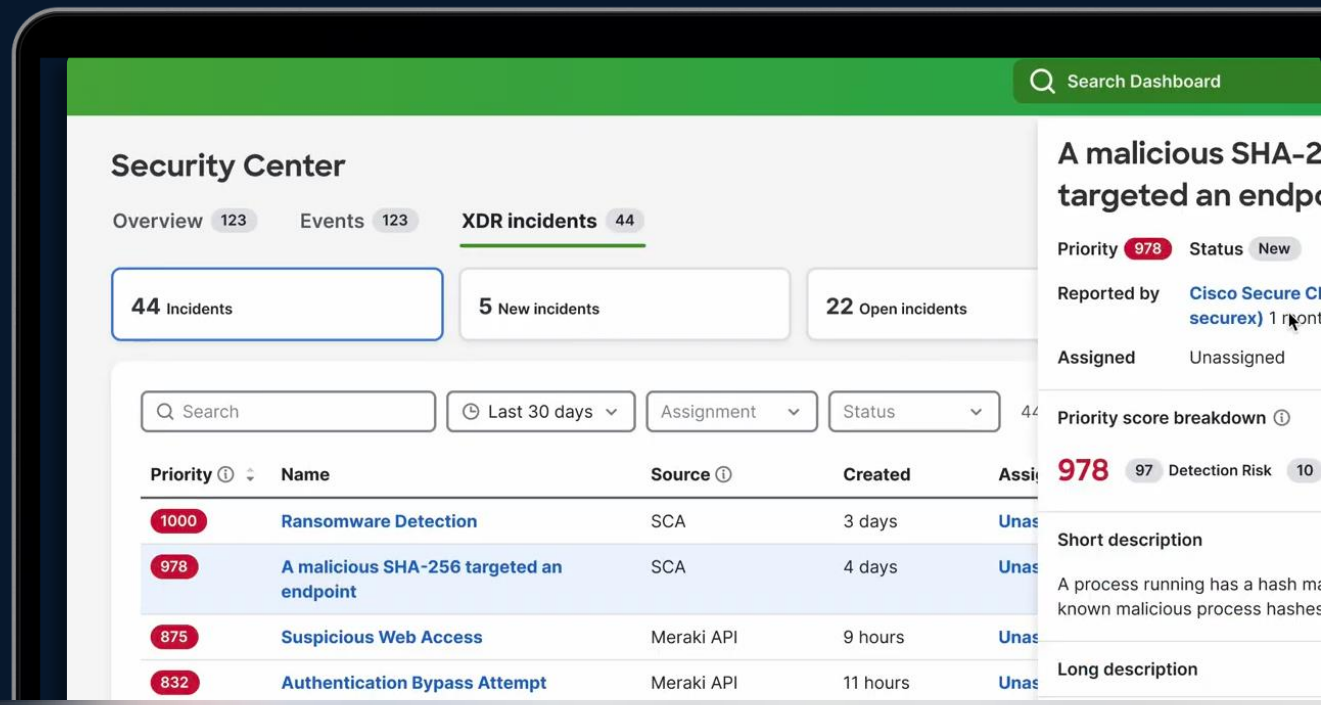

## Visibility into

- Initial Access
- Cloud Administration Command
- Lateral movement and Transfer data
- Malicious code distribution and execution
- Domain and IAM User takeover
- Account Manipulation and Exfiltration Over Alternative Protocol
- Geographical unusual usage

*More information on the MITRE ATT&CK® Cloud Coverage can be found here

# Cisco XDR

## Innovating to detect and stop common attacks




Optimized for lean teams

Speed to value

Deeply integrated with the network

## Every Meraki MX becomes a sensor

In under 60 seconds

# Introducing Cisco XDR 2.0

## Clear verdict. Decisive action. AI speed.

### Instant Attack Verification

Multi-agent, agentic AI to quickly confirm threats, enabling decisive, automated response

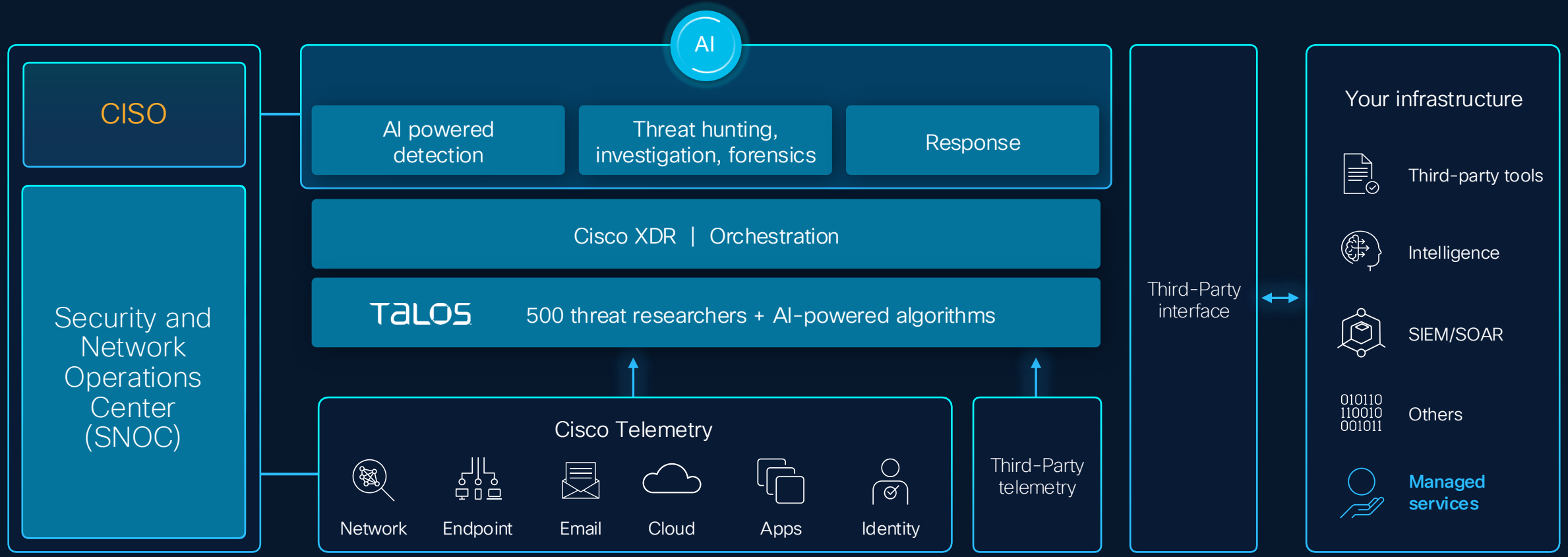
### Automated Forensics

Market leading forensics from every endpoint in minutes.

### Attack Storyboard

Incident comprehension in under 30 seconds with an intuitive visual representation of attack chains and natural language.

# Simplify security operations with AI-driven Cisco XDR




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

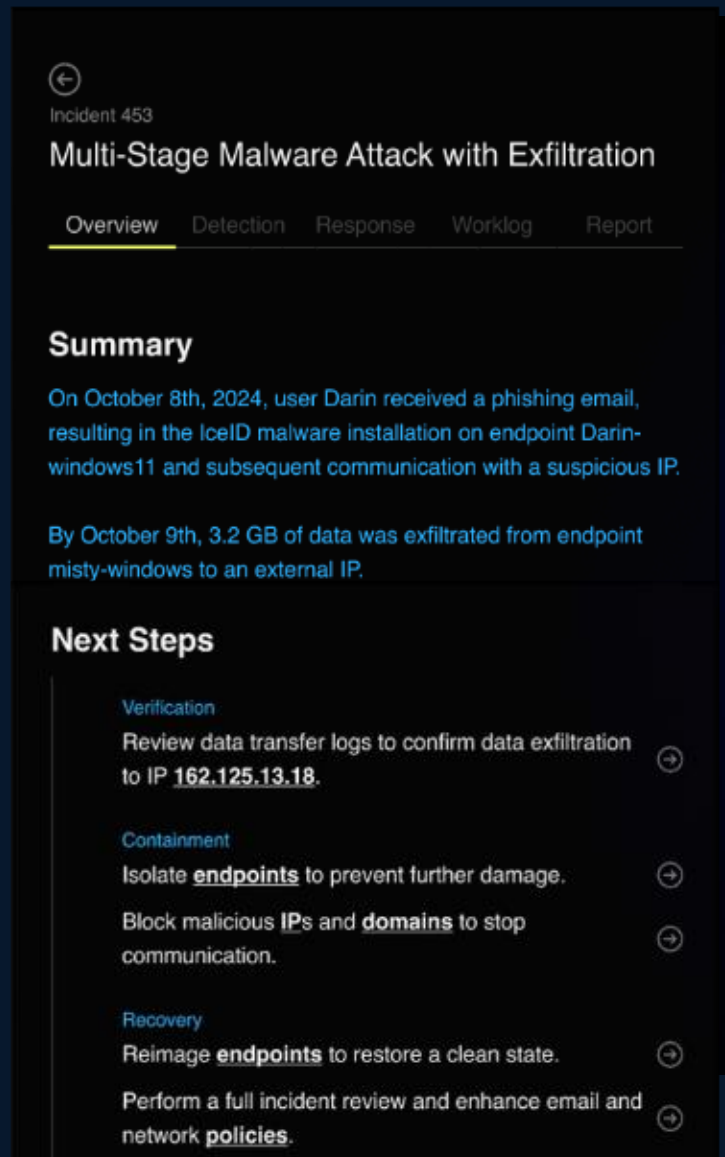
# Instant Attack Verification with a Clear Verdict

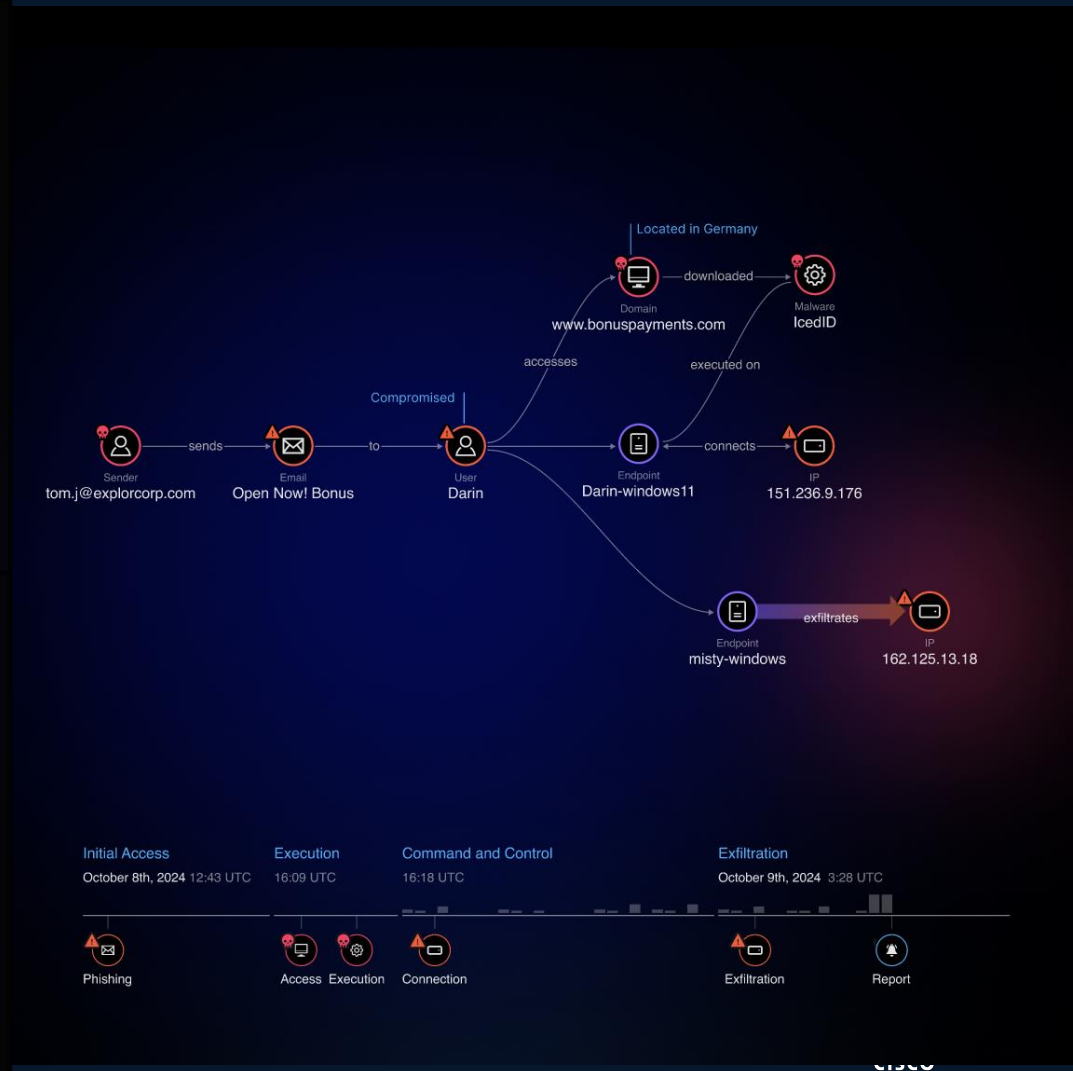
Clear verdict. Decisive action. AI speed.

Each alert is analyzed by AI agents to eliminate false positives

Multiple AI agents launch investigation plan to verify real attack with a clear verdict

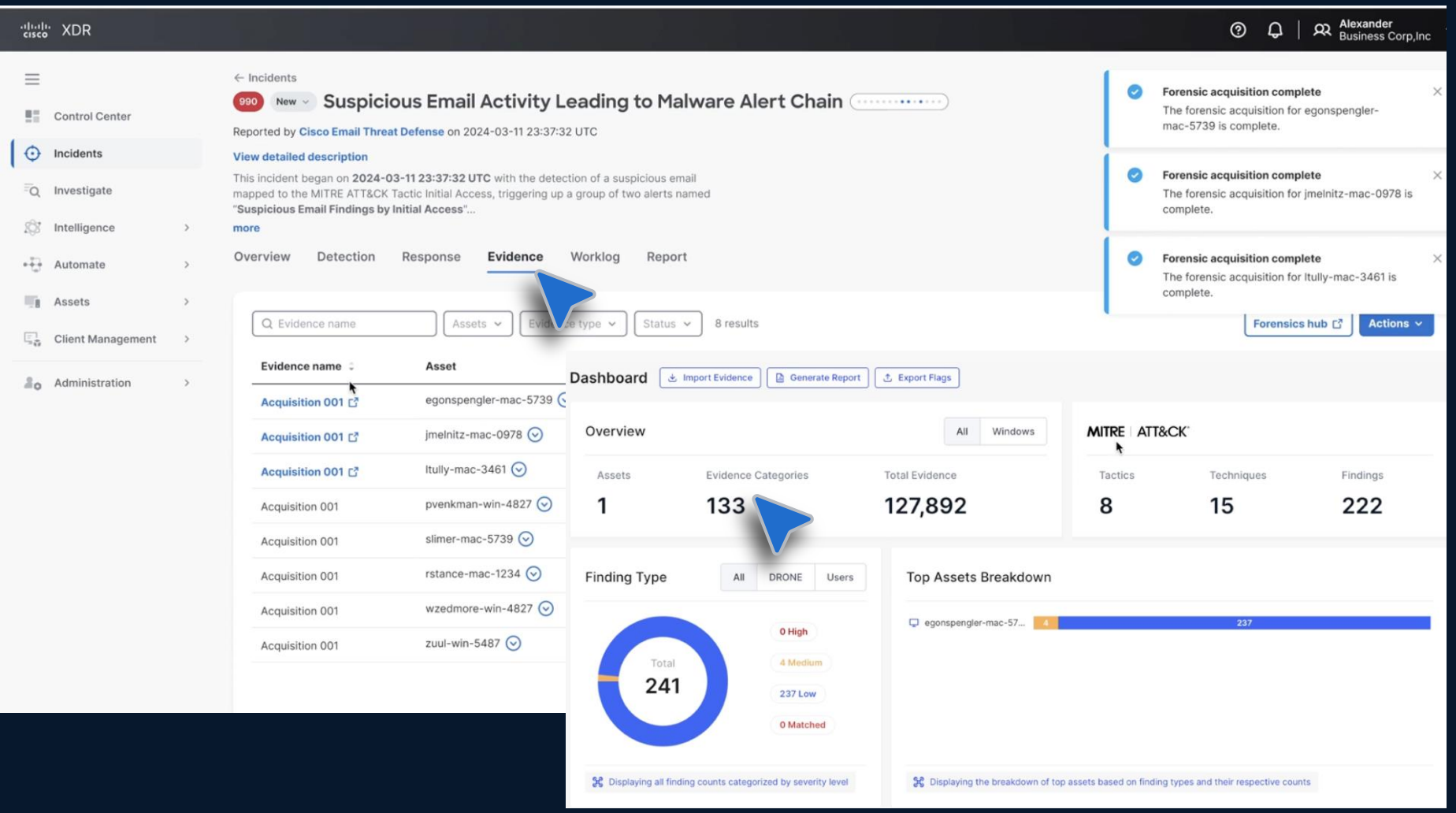
Trigger a decisive response through playbooks in XDR/ SOAR



# Automated Forensics to Gather Evidence Instantly

Clear verdict. Decisive action. AI speed.



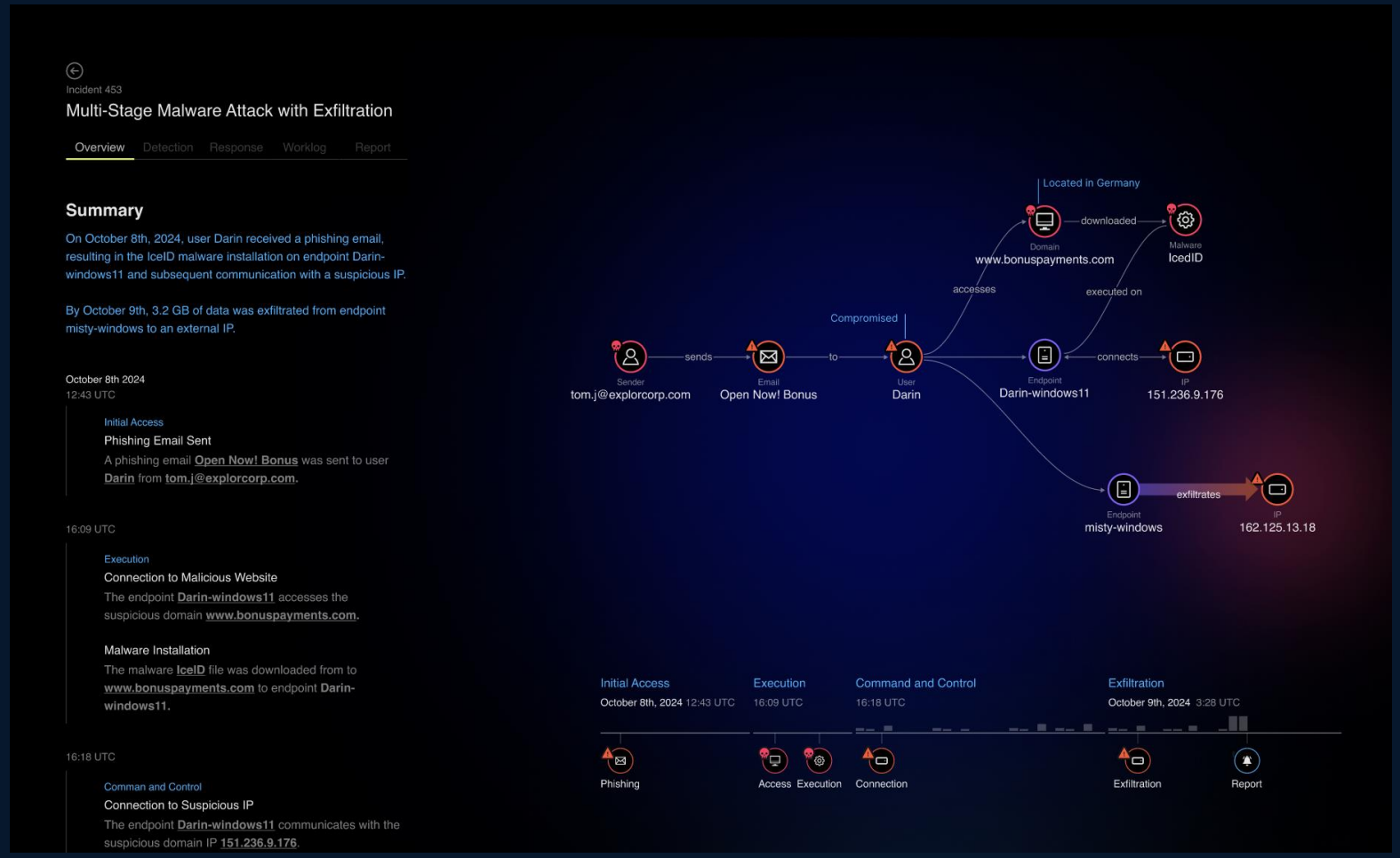

Trigger forensics before you know that you need it

100s of evidence components are captured even from compromised device

Evidence builds confidence to take decisive next steps

# Attack Storyboard to Comprehend an Incident in 30 Sec

Clear verdict. Decisive action. AI speed.




Turn complex attacks into visual narratives with explanation summary

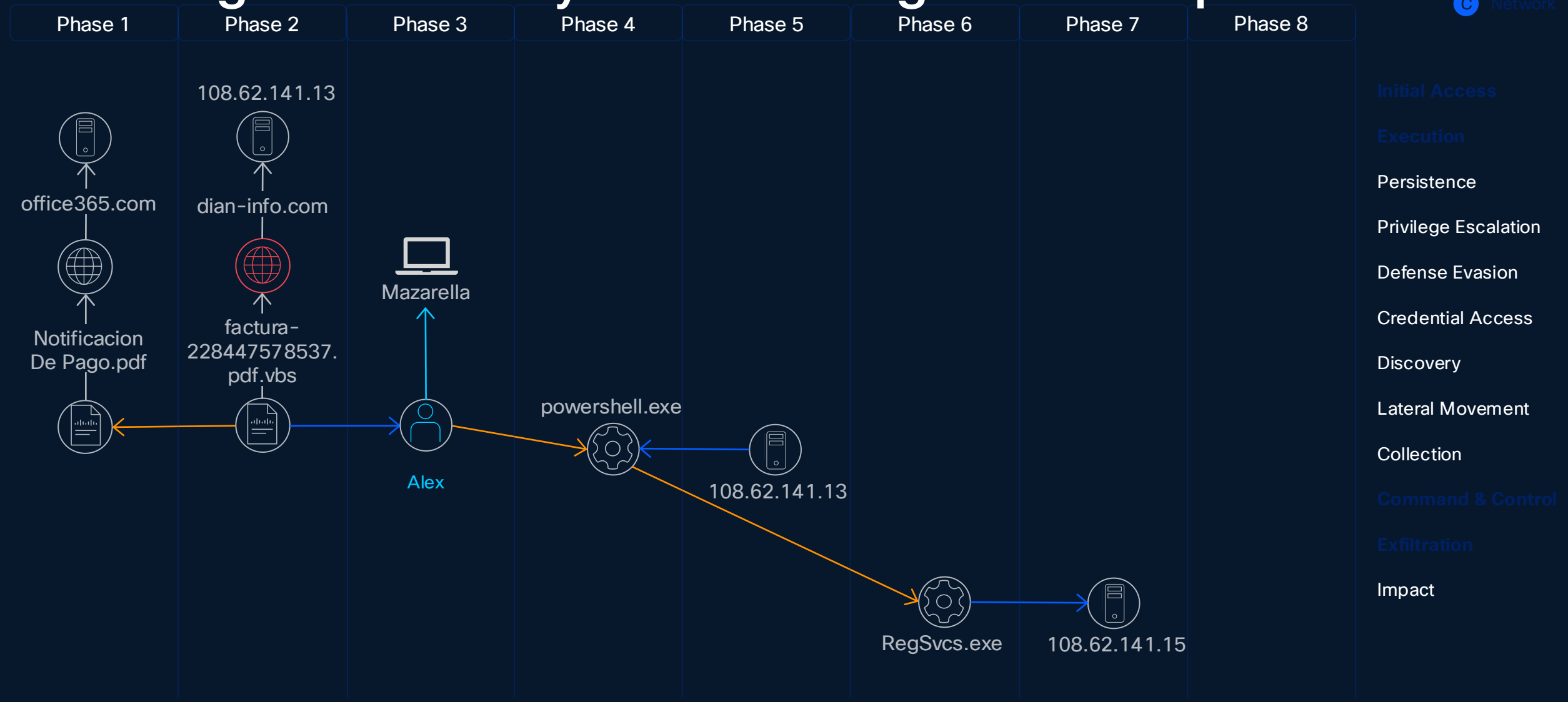
Attack graph mapped MITRE tactics

Unified workflow from investigation to remediation with no context switching

# Finding persistence & more

Demo

# Strength of visibility – Uncovering attack sequences



AI-generated

## Suspicious Endpoint and User Activity Detected

Critical

The incident is likely confirmed, with an **85% probability**

The incident highlights **critical security issues with** the device **mazzarella.ad.ciscrypt.info**, including **AsyncRAT activity and suspect data loss**, suggesting **potential compromise and urgent need for investigation**.

### Summary

Starting **March 27, 2025** XDR Network identified **Potentially Harmful Hidden File Extension - Multiple File Extensions** involving **mazzarella.ad.ciscrypt.info** and **108.62.141.13** with 2 findings.

Cisco Secure Endpoint detected **W32.WScriptExecuteFakeExtension.ioc** involving the User **alexw** and **mazzarella.ad.ciscrypt.info** with 1 finding.

Additionally, Cisco Secure Endpoint reported **PowerShell DownloadString** involving **alexw** and **mazzarella.ad.ciscrypt.info** with 2 findings.

There were further findings involving the same endpoint including XDR Endpoint reporting **Unusual Encoding on Command Line - Suspicious Endpoint Activity** and **Content Download Using Powershell - Suspicious Endpoint Activity**, both with findings involving **108.62.141.13**, **108.62.141.15**, **alexw**, and **mazzarella.ad.ciscrypt.info**.

Cisco Secure Endpoint also detected **AsyncRAT activity** and **AsyncRAT Mutex** on the same endpoint followed by **high priority intrusion detection alert** from Meraki Firewall triggered by device **mazzarella** communication with IP **108.62.141.15**.

Additionally, the same day included a detection of an **Excessively long PowerShell command**, and a **Long Lasting Network Connection from a System Binary** detected by XDR Endpoint and Cisco Secure Endpoint, involving **108.62.141.15**, **alexw**, and **mazzarella.ad.ciscrypt.info**.

### Impact

High **Impact**

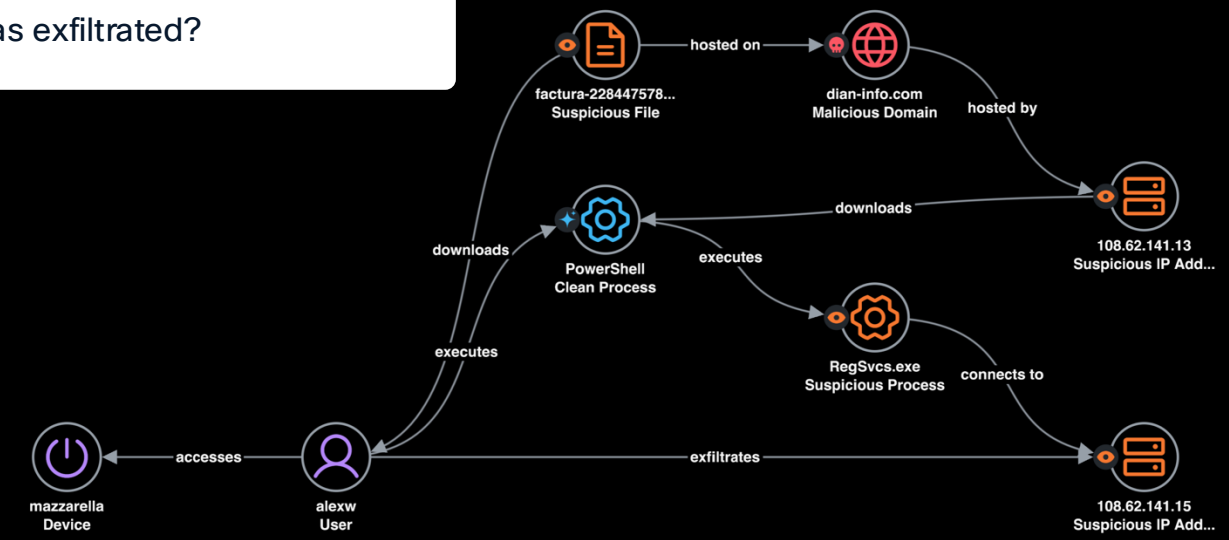
4.07 GB of data was uploaded from mazzerella to external hosts, risking sensitive information exposure. The breach, involving AsyncRAT and PowerShell, bypassed security controls, allowing malware and unauthorized data transfers.

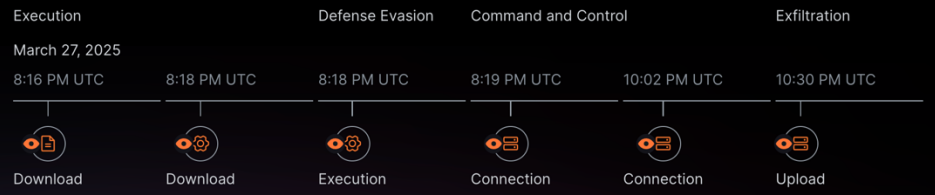
### Recommendations 5

Four questions:

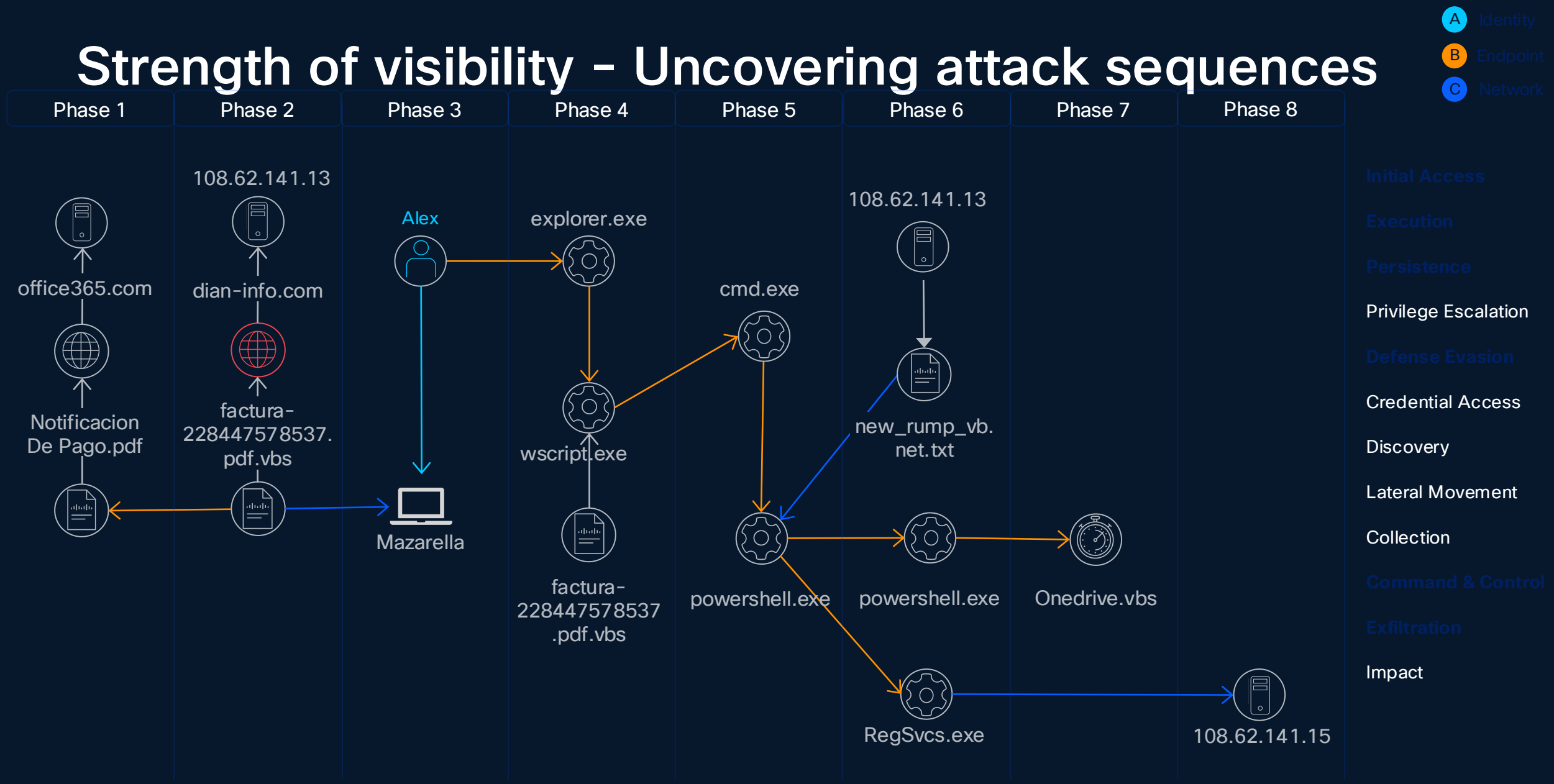
- ✓ What was the initial access?
- ✓ Which Systems are infected?
- Does the attacker still have access?
- What was exfiltrated?

Return to legacy view



# Strength of visibility – Uncovering attack sequences



AI-generated

## Suspicious Endpoint and User Activity Detected

Critical

The incident is likely confirmed, with an **85% probability**

The incident highlights **critical security issues with** the device **mazzarella.ad.ciscrypt.info**, including **AsyncRAT activity and suspect data loss**, suggesting **potential compromise and urgent need for investigation**.

### Summary

Starting **March 27, 2025** XDR Network identified **Potentially Harmful Hidden File Extension - Multiple File Extensions** involving **mazzarella.ad.ciscrypt.info** and **108.62.141.13** with 2 findings.

Cisco Secure Endpoint detected **W32.WScriptExecuteFakeExtension.ioc** involving the User **alexw** and **mazzarella.ad.ciscrypt.info** with 1 finding.

Additionally, Cisco Secure Endpoint reported **PowerShell DownloadString** involving **alexw** and **mazzarella.ad.ciscrypt.info** with 2 findings.

There were further findings involving the same endpoint including XDR Endpoint reporting **Unusual Encoding on Command Line - Suspicious Endpoint Activity** and **Content Download Using Powershell - Suspicious Endpoint Activity**, both with findings involving **108.62.141.13**, **108.62.141.15**, **alexw**, and **mazzarella.ad.ciscrypt.info**.

Cisco Secure Endpoint also detected **AsyncRAT activity** and **AsyncRAT Mutex** on the same endpoint followed by **high priority intrusion detection alert** from Meraki Firewall triggered by device **mazzarella** communication with IP **108.62.141.15**.

Additionally, the same day included a detection of an **Excessively long PowerShell command**, and a **Long Lasting Network Connection from a System Binary** detected by XDR Endpoint and Cisco Secure Endpoint, involving **108.62.141.15**, **alexw**, and **mazzarella.ad.ciscrypt.info**.

### Impact

High **Impact**

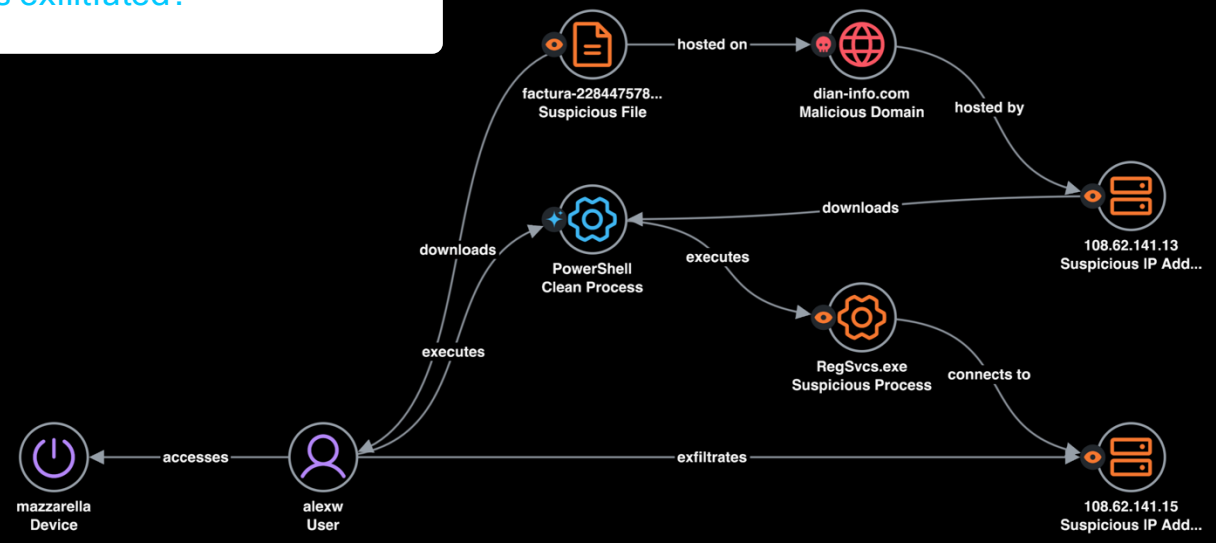
4.07 GB of data was uploaded from mazzerella to external hosts, risking sensitive information exposure. The breach, involving AsyncRAT and PowerShell, bypassed security controls, allowing malware and unauthorized data transfers.

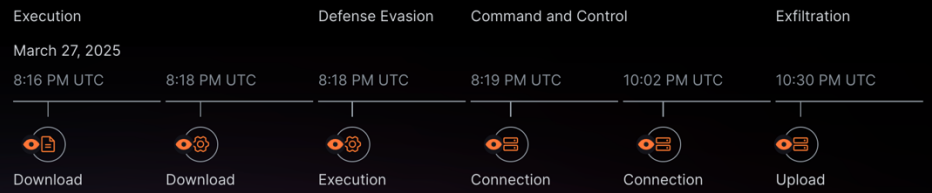
### Recommendations 5

Four questions:

- ✓ What was the initial access?
- ✓ Which Systems are infected?
- ✓ Does the attacker still have access?
- ✓ What was exfiltrated?

Return to legacy view






cisco

# The Cisco XDR difference

Clear verdict. Decisive action. AI speed.

## Agentic AI paired with human intelligence

Create clarity and increase confidence in every decision with Agentic AI

## Network + Endpoint at the core

Detect the most advanced attacks since Cisco XDR is powered by network insights

## Open and unified approach to XDR

Get unified visibility via broad integrations with Cisco security solutions and third-party tools

## Security Operations Simplified

Detect sooner

Prioritize by impact

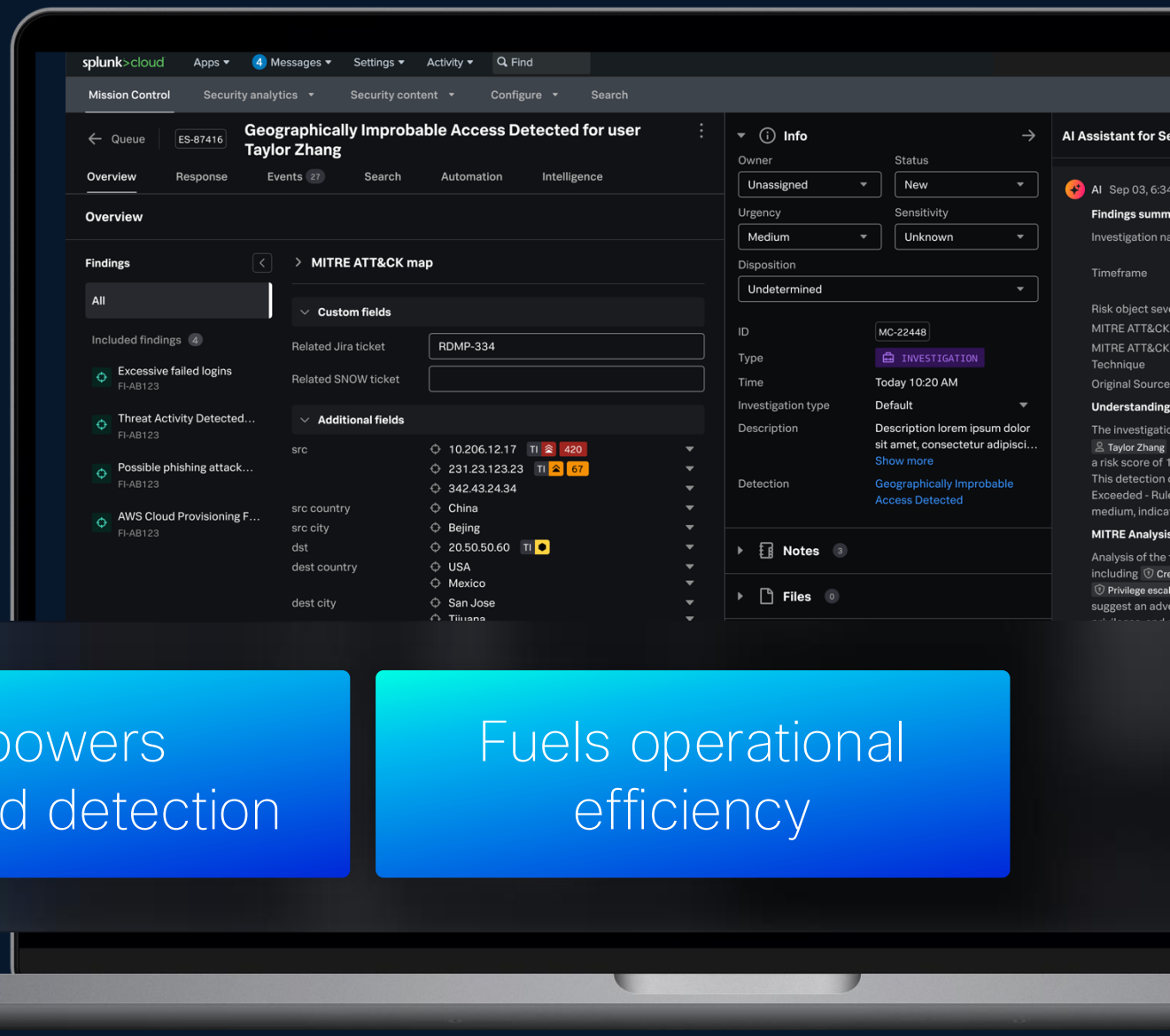
Speed up investigations

Accelerate response

# Splunk ES: Using Insights to Exploit Every Advantage

# Splunk Enterprise Security

## Market-leading SIEM with AI-powered capabilities




Unmatched visibility

Empowers advanced detection

Fuels operational efficiency

# Effective security operations require

## Visibility

Of the Attack Surface

Telemetry & Logs

+

## Knowledge

Knowing what to look for

Threat Intel, Indicators, Detections, Context

+

## Action

Ability to take Action

Policies, Blocking, Patching, Remediating

Cisco Security Cloud Technical Add-on: +25K downloads

Cisco Talos: 2,000 new samples analyzed every minute

SOAR ecosystem: +300 connectors with +2,800 automated actions



cisco

# Power the SOC of the future

**Data Management and Federation**

## Search, Analyze and Manage Data Wherever it Resides

Effectively manage complex data management needs. Seamlessly access data stored across different data stores for search and analytics.

**Transform Threat Detection**

## Tackle an Expanding Threat Landscape

Author and engineer detections to support a range of detection methodologies and effectively implement detection as code.

**Reduce Risk Exposure**

## Reduce Your Exposure to Risk and Compliance Gaps

Unleash continuous asset discovery to enhance compliance posture and close gaps in security controls.

**Simplify SecOps with AI**

## Simplify the Analyst Experience with AI

Augment your SOC team with AI to help analysts with routine yet error-prone tasks such as writing investigative summaries.

**Unify TDIR**

## Unify TDIR with Automated Workflows

Coordinate and collaborate across the TDIR lifecycle with automated workflows using custom SOAR playbooks.

# Cisco integrations made seamless

The Cisco Security Cloud app enables easier integration of your Cisco data sources within Splunk

Single application that packages all Cisco Security integrations in a single offering based on “gold standard” best practices

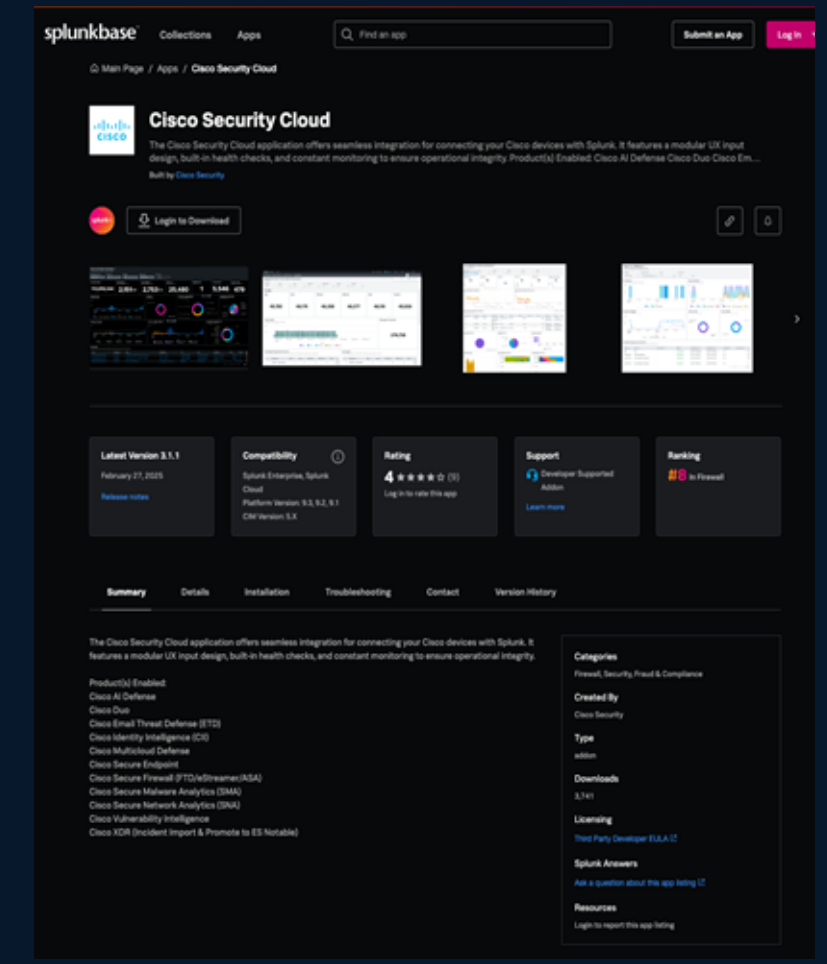
Replaces the older individual Cisco TA's and Apps that are now archived

Available Today:

- AI Defense
- Secure Network analytics
- XDR (Incident Reporting)
- Email Threat Defense
- Multi Cloud Defense
- Secure Firewall (FTD, Estreamer, ASA)
- Malware Analytics
- Secure Endpoint
- Kenna Vulnerability Intelligence
- Identity Intelligence
- Duo

Next Up:

- Secure Workload
- Isovalent (Hypershield)
- Crosswork Cloud



# Splunk Security delivering a comprehensive approach

World class detection approach for the SOC of the future

Pre-built detections
- 1,700+ Curated Detections by Splunk Threat Research
- 225+ Analytic Stories
- 75+ Automation Playbooks

**Rule-based detections**
- Event-based Detections
- Findings-based Detections
- Adaptive Response Actions
- Automation Rules and SOAR Playbooks

**Dynamic detections**
- ML-based Detections
- Real-time Behavioral Analytics
- Risk-Based Alerting

**Custom detections**
- Fully customizable built-in detections
- Full flexibility to create custom detections
- Machine Learning Toolkit

Automatic threat intelligence enrichment
(Threat Intelligence Management, Talos Threat Intelligence, 3rd Party)

Integration with cybersecurity frameworks
(Threat Topology Visualization, MITRE ATT&CK, NIST CSF 2.0, Cyber Kill Chain®)

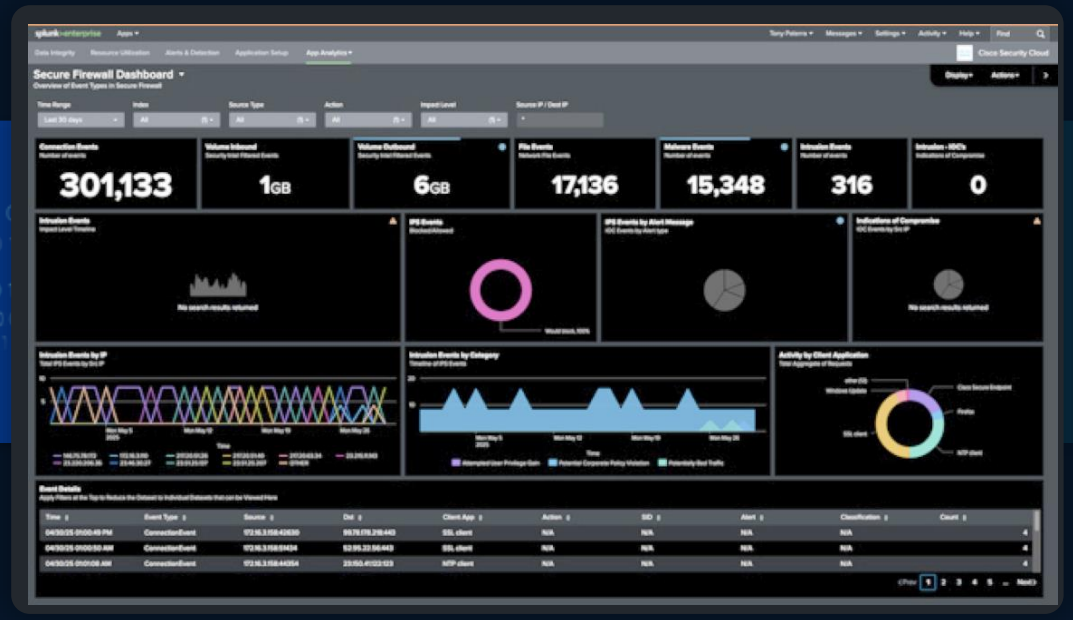
Detection authoring and management
(Automatic Detection Versioning, Open-Source Tools)

NEW

# Security Insight, on Us

## Free Cisco firewall logs to Splunk*

AVAILABLE since August 2025




New detections | Automated response

*Ingest up to 5GB/device/day requires Firewall Threat Defense subscription and Splunk license

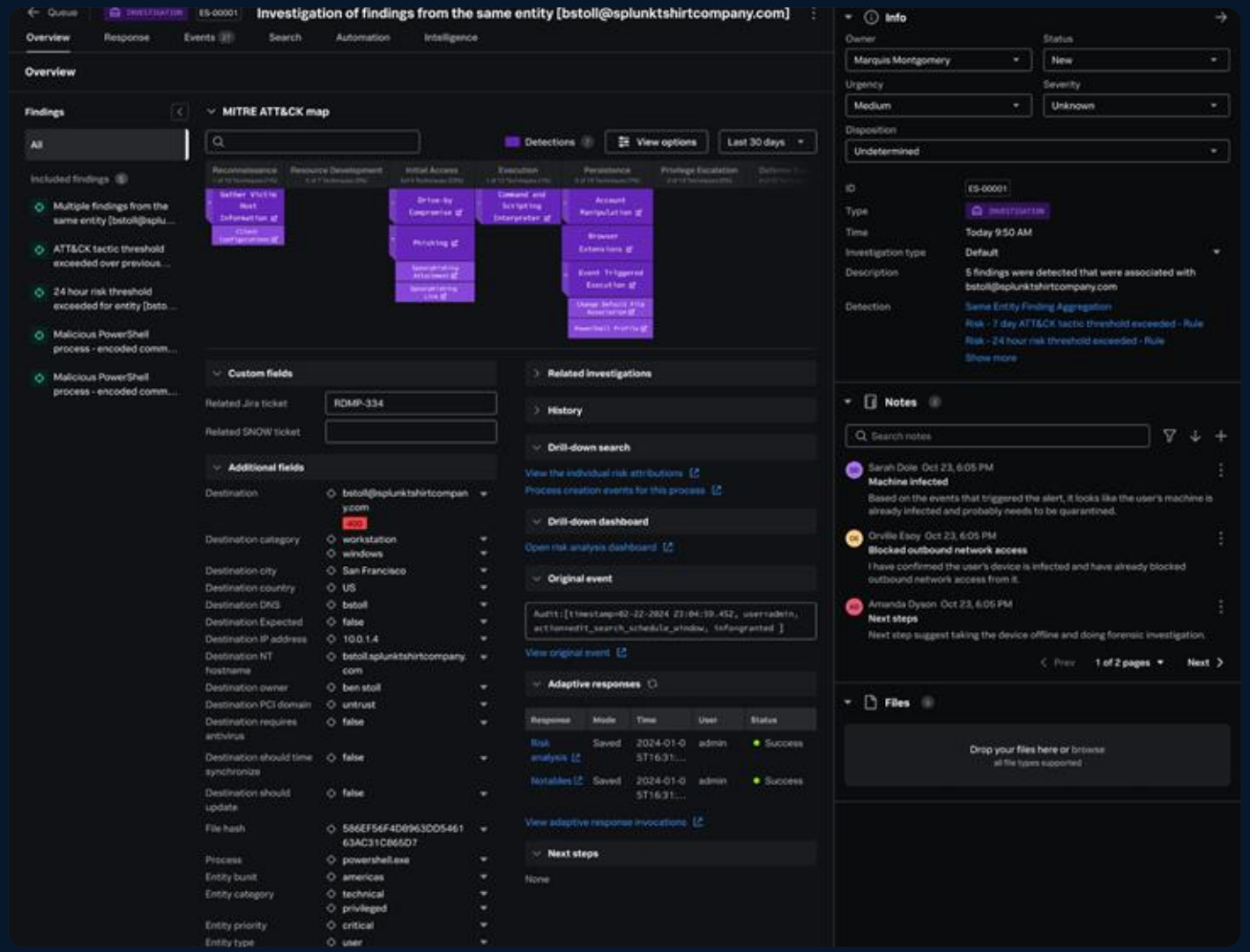


cisco

# Enterprise Security 8.0

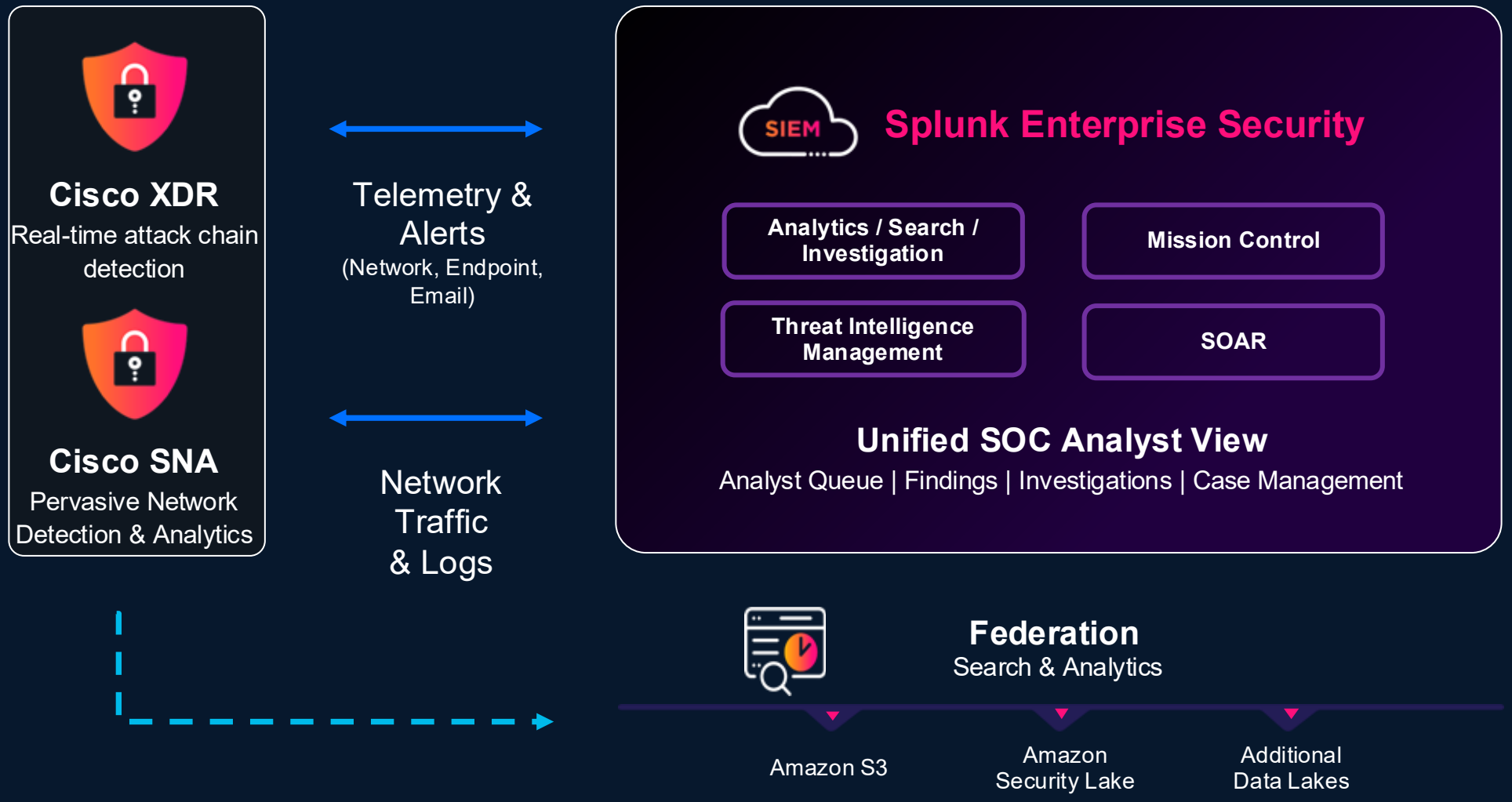
The Market-Leading SIEM to Power the SOC of the Future

- Improved case management capabilities
- Native Splunk® SOAR integration
- Enhanced detection engineering capabilities
- Simplified terminology for security analytics



# Unifying Threat Detection, Investigation and Response

Splunk Enterprise Security: The Core of the Unified TDIR Experience



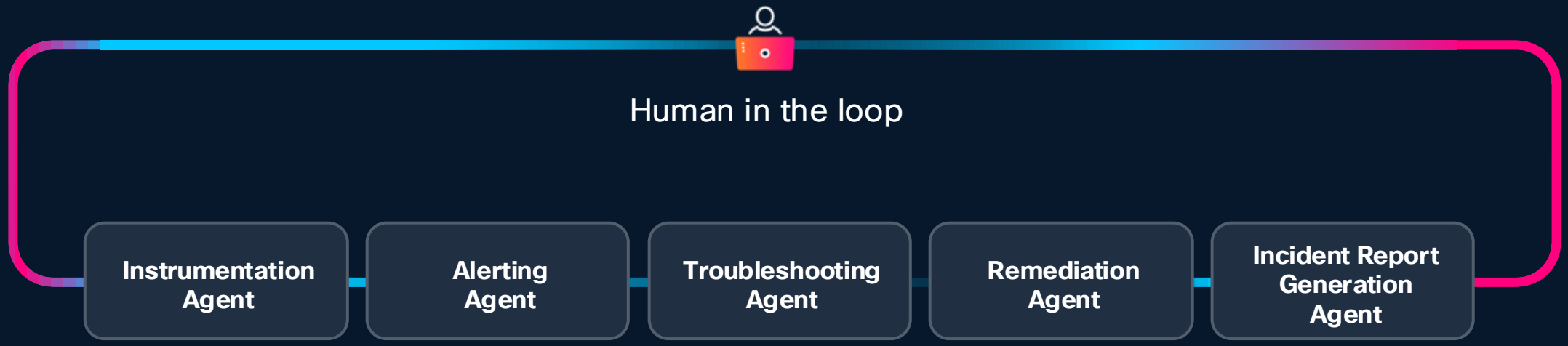
# Modern Observability must evolve

Fix and prevent with AI agents

Observe AI agents and infrastructure

GenUI for human and agent workflows

# Fix and prevent with AI agents



# Why MCP Matters

*Model Context Protocol — The Universal Connector for AI*

THE CHALLENGE

Every AI model today requires custom integrations for each data source, tool, and enterprise system, creating M×N complexity that doesn't scale.

THE MCP ANSWER

A single open protocol that standardizes how AI models connect to any data source or tool, turning M×N into M+N.

## Universal Interoperability

One protocol connects any LLM to any enterprise tool, API, or data source — no custom adapters.

## Composable Architecture

Modular MCP servers snap together, enabling multi-agent workflows across heterogeneous stacks.

## Security & Governance

Centralized auth, audit, and policy enforcement at the protocol layer — enterprise-grade by design.

## Accelerated Deployment

Pre-built connectors slash integration time from weeks to hours, reducing TCO for AI initiatives.



cisco

# MCP Architecture

*How Model Context Protocol connects agents, tools, resources, and platforms*




`tools/list` Startup: executor discovers all tools across servers

`tools/call` Runtime: agent requests a tool → routed by name

`resources/read` Pre-meeting: DataGatherer pulls structured context

cisco

# Agentic SOC “Art of the possible” Demo

# Cisco Splunk and Cisco Security

# Splunk and Cisco drive actionable insights

Splunk + Cisco Talos = Unmatched outcomes


**4PB+** data ingested daily

**800B+** Security events daily

**1B** Endpoints

**625B** Web requests analyzed daily

Stop billions of attacks

Ensure resilient networks and applications

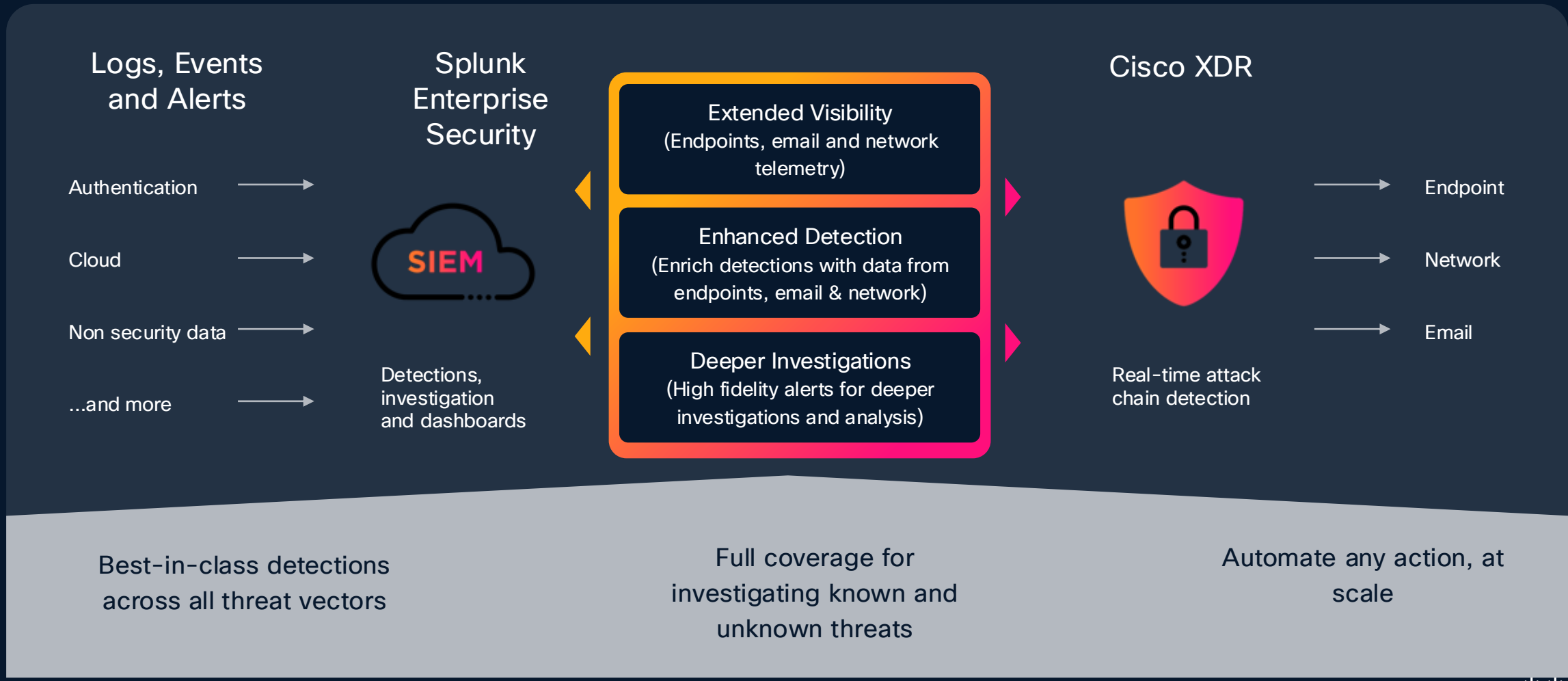
**But what does this mean in practice?**



cisco

# Expand detection surface and context

## Cisco XDR integration with Splunk ES



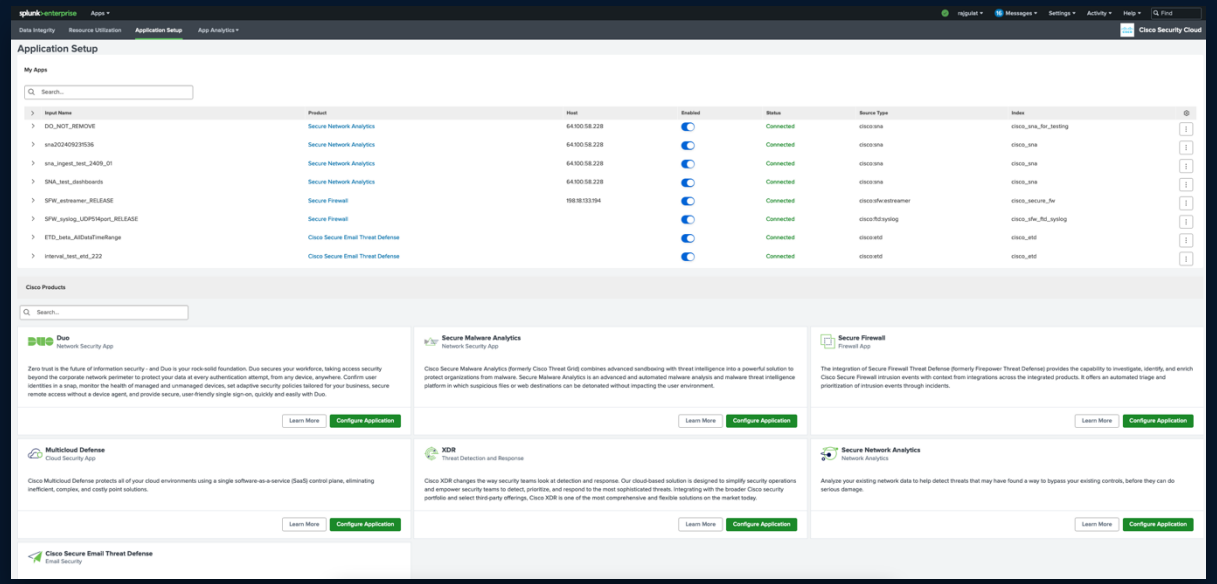

Best-in-class detections across all threat vectors

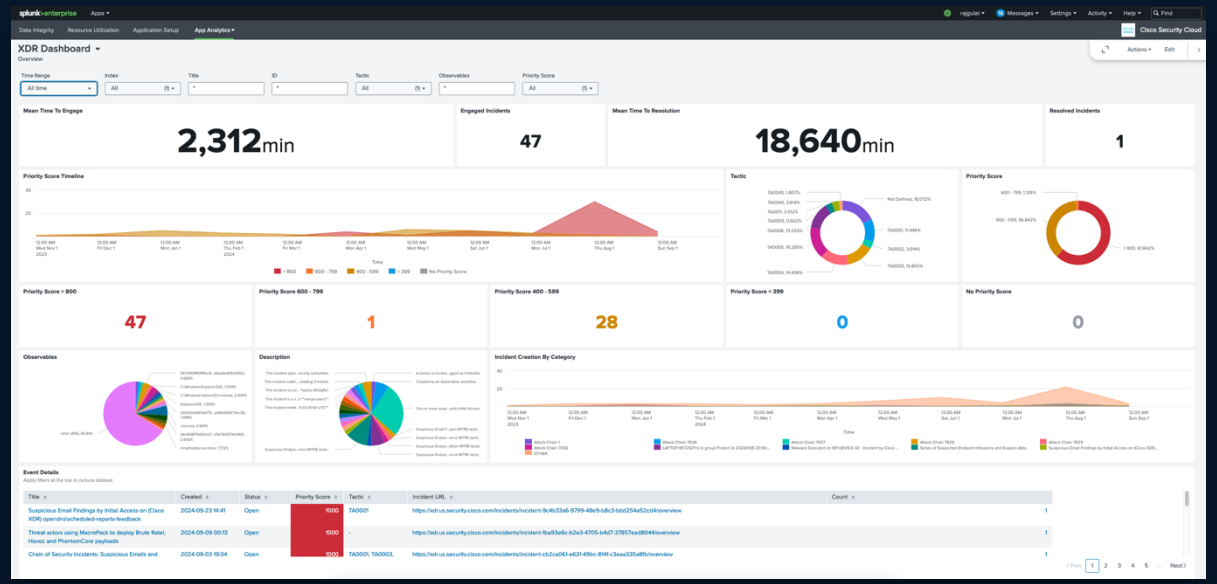
Full coverage for investigating known and unknown threats

Automate any action, at scale

# Cisco XDR and Splunk

- **Splunk App:** Cisco Security Cloud
  - Incident Import (pull model)
  - Optional: promote incidents to Notable/Finding (Enterprise Security required)
- **XDR Integration: Splunk Cloud** and **Splunk Enterprise**
  - **Automation Workflows:** a Splunk (Cloud or Enterprise) target is automatically created for out-of-box and custom workflows.
  - **Playbooks:** system workflow included in the Cisco Managed Incident Playbook (recovery phase) can be used to close and export (push model) an incident.
  - **Exchange:** send an Incident (or other XDR data) to Splunk (push model), as well as perform advanced on-demand or scheduled searches.
  - **Atomic Actions:** search and retrieve in Splunk can be used as building blocks in workflows for threat hunting.
  - **Enrichment:** Cisco XDR investigations query Splunk for events based on selected observables (NEW).



# Better together:  SOC of the Future

## Market leading SIEM + Innovative XDR

- Federated data management
- Advanced threat detections
- AI-accelerated investigations
- Automated response

EMBEDDED AI

CONTENT AND THREAT RESEARCH


User/Cloud/ Breach/


Networking


Third-party tools


Talos


Clouds


Devices


Data centers


Applications



cisco

# Thank you