CISCO Engage | Tech Day

Clear Verdict. Decisive Action. AI Speed.

Cisco XDR + Splunk

Elliot Riegner
Splunk Senior Solution Engineer

Matt Gockel
Cisco Security Solution Engineer

Agenda

1. SOC Challenges
2. SOC Maturity Model
3. XDR AI Analytics & Forensics
4. One Cisco for Unified TDIR
5. Splunk ITSI
6. Q&A

SOC Challenges

Security Operations Challenges

Constant threats and a growing attack surface add complexity

Lack of Analyst Bandwidth

Velocity of Credential Phishing and Malware

Limited Visibility and Context

cisco

What SecOps 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

SOC Maturity Model

Common SOC Duties

Tier 1 (Triage):

- Phishing campaigns
- Phishing file analysis
- IP/domain analysis
- Mobile device wipes
- Email investigations
- 3rd party vulnerability reports – threat hunt
- Escalate to T2

Tier 2 (Sr/Lead):

- IDS/IPS alerts
- Rogue users
- DNS Sinkholing domains
- IP/VPN blocks
- DDoS
- Escalate to CTI/CTA/CTD/IR
- Email pulls
- Account disables/wipes
- Pull forensic package

Shift Lead (Sr/T3):

- Create and Monitor dashboards
- Train new hires
- Make sure everyone is doing their work
- Jump into incidents ad hoc
- Manage the SOC queue
- Interface with vendors

Unified TDIR: XDR w/Splunk

Easy Button

XDR

- Easy button
- Foundational TDIR
- Out of box workflows and basic investigation
- Integrated SOAR
- Fewer 3rd Party integrations than Splunk
- Complete Forensics
- Agentic AI Investigations
- <1 year storage

Increasing Maturity & Sophistication

XDR w/ Splunk Core Platform

- Everything in XDR
  - Over 1k OOTB integrations
  - Splunk Dashboards
  - Investigation (SPL)
  - Federated Search
  - On-prem or cloud
  - FedGov Certification requirements (FIPS/CC/IL5+)

Splunk Enterprise Security (ES)

- Case Management
- Detection Engineering
- Risk Based Alerting
- Ad-hoc investigations
- PCI /SOX HIPAA

Splunk Enterprise Security w/ XDR Detections

- Deep Threat Hunting
- Bespoke workflows
- Advanced automation capabilities
- XDR pre-built detections
- Cisco XDR Forensics
- Agentic AI Investigations

Mature SOC

Splunk ES Premier w/ XDR Detections

- Everything in ES & XDR plus:
  - Insider Threat / UEBA
  - Asset Risk Intelligence
  - SnapAttack detections
  - Attack Analyzer

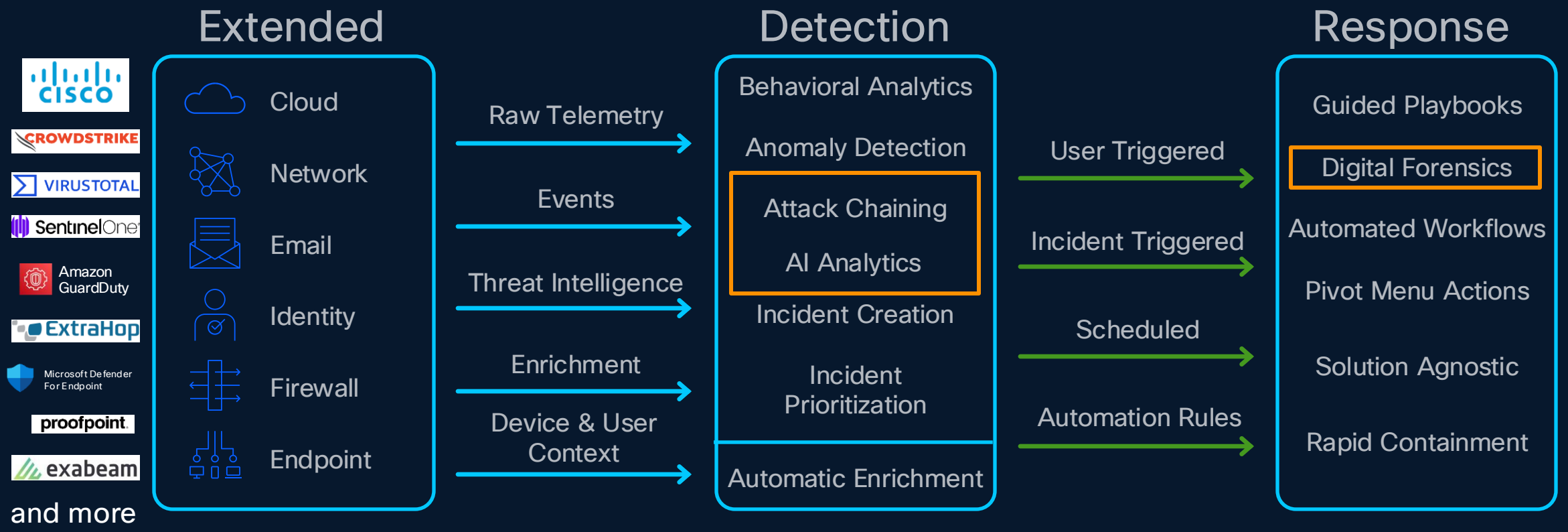
XDR UI	**XDR UI w/ Splunk dashboards**	**Splunk UI**	**Enterprise Security UI w/ XDR Pivots**
XDR Storage	**XDR & Splunk Storage**	**Splunk Storage**	**Splunk & XDR Storage**

Additive features and functionality starting with XDR, adding Splunk Core then layering in Enterprise Security advanced security use cases

cisco

XDR AI Analytics & Forensics

Cisco XDR High Level Architecture



Multi-vector telemetry ingest network, cloud, endpoint, email, and more from Cisco and 3rd party

Cross domain alert detections and attack chaining with automated incident prioritization and enrichment

Automated or user triggered responses to block observables using any integrated technology

LLM Multi-Agent System for Automated Investigation

Highly specialized agents:

- GenAI/AI model + domain specific knowledge
- Divide and conquer

Orchestration agent

- Coordinate across agents

Summarization agent

- Produce summary of the incident

Planner agent

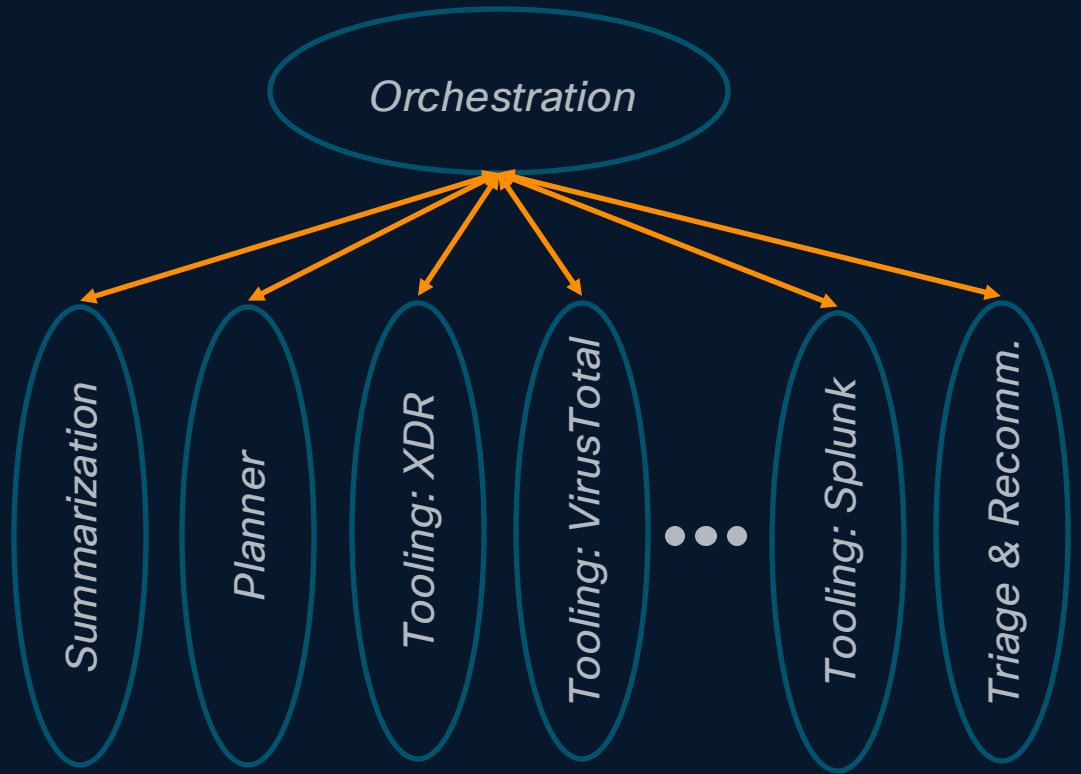
- Generate a list of tasks to do

Tooling agent per task

- *Execution* agent
- *Interpretation* agent

Triage & Recommendation agent

Agent Architecture

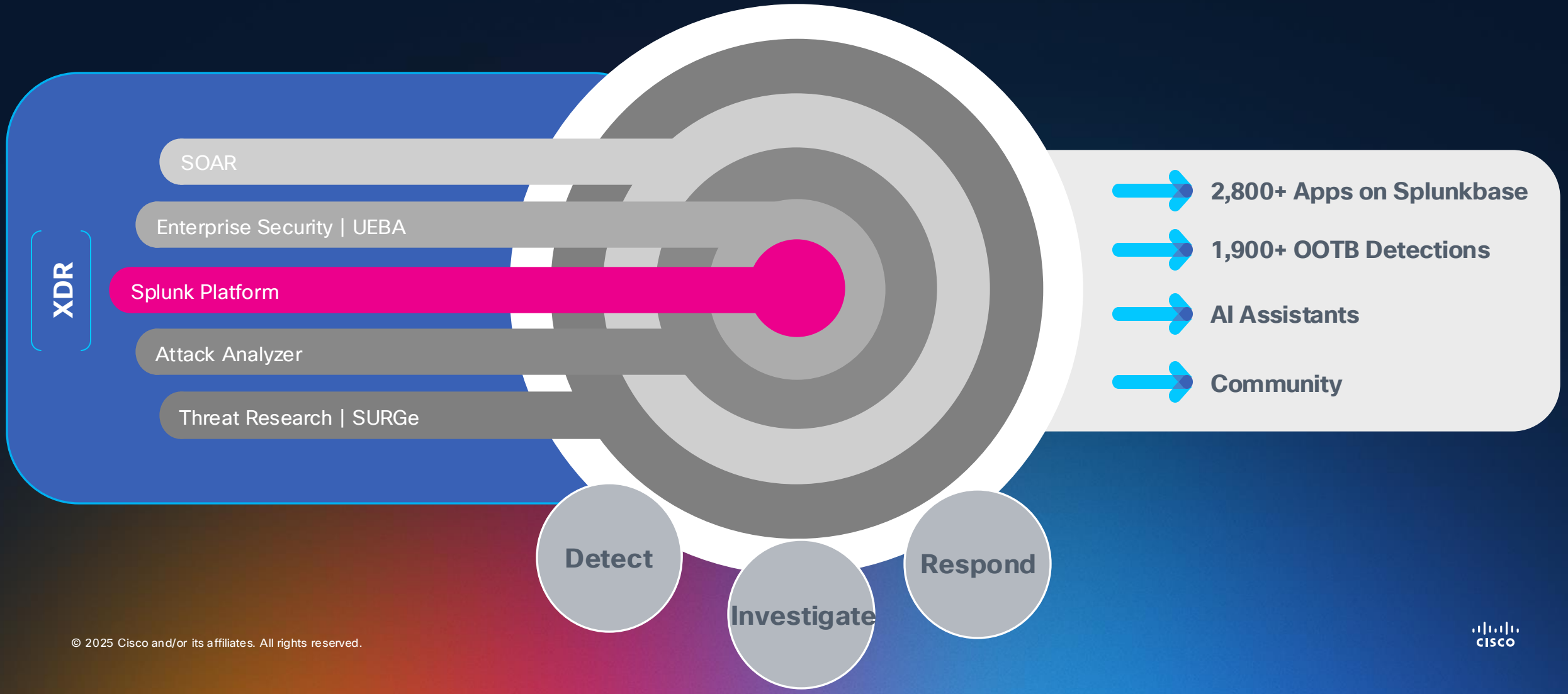


** tooling agents under development (except VT)*

XDR AI Analytics & Forensics Demo

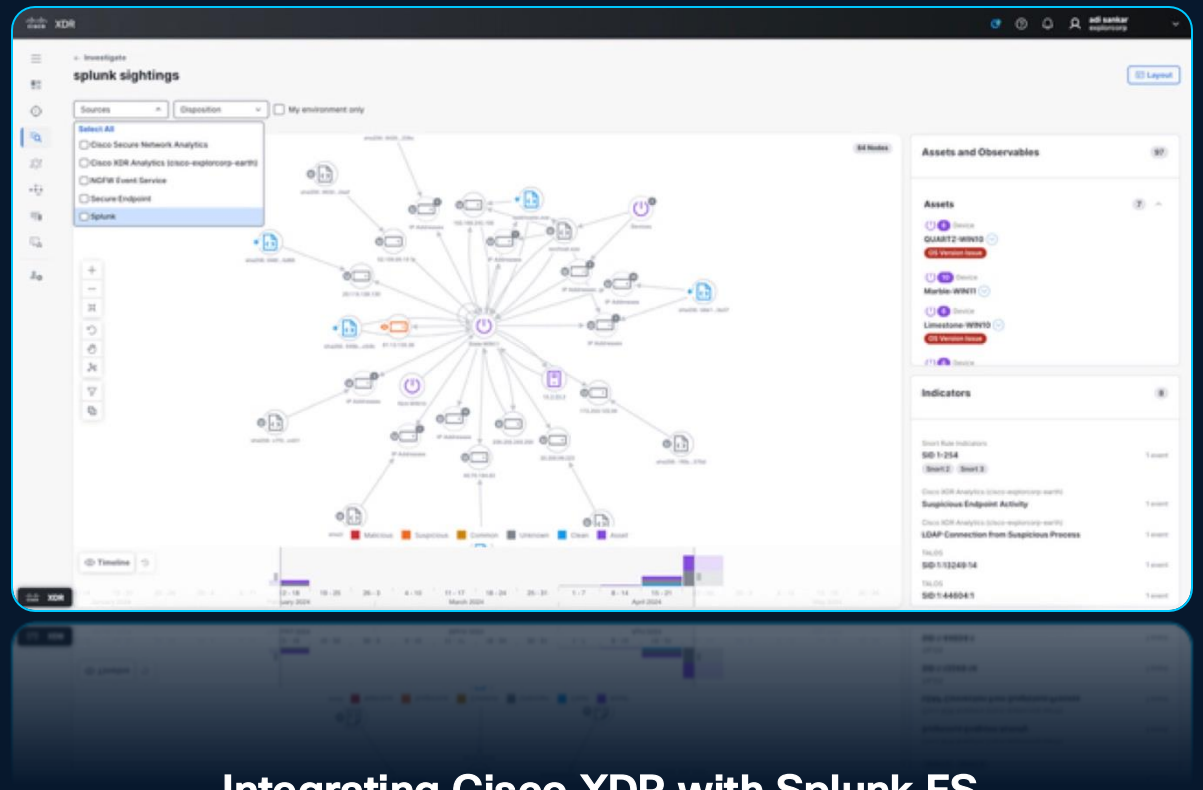
One Cisco for Unified TDIR

One Cisco Security Portfolio



Use case

Expand visibility across domains

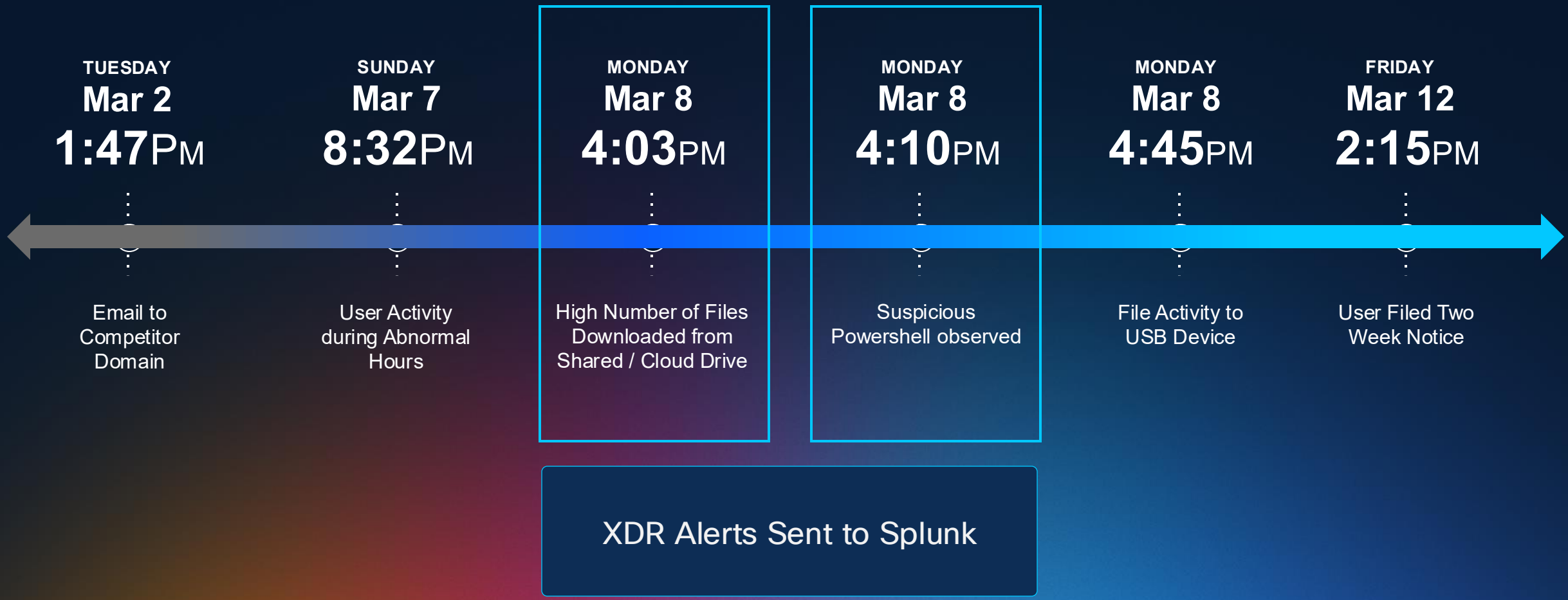


Integrating Cisco XDR with Splunk ES for Enhanced Security Analysis

Seamless collaboration for threat identification, action, and investigations

Leverage verdicts from Splunk for correlated verdicts on indicators of compromise

Better Together Alerting



Better Together Alerting

TUESDAY Mar 2 1:47PM	SUNDAY Mar 7 8:32PM	MONDAY Mar 8 4:03PM	MONDAY Mar 8 4:10PM	MONDAY Mar 8 4:45PM	FRIDAY Mar 12 2:15PM
Email to Competitor Domain	User Activity during Abnormal Hours	High Number of Files Downloaded from Shared / Cloud Drive	Suspicious Powershell observed	File Activity to USB Device	User Filed Two Week Notice
0 pts	**0 pts**	**40 pts**	**20 pts**	**30 pts**	**60 pts**

Aggregated user risk score **>100**

Risk Notable

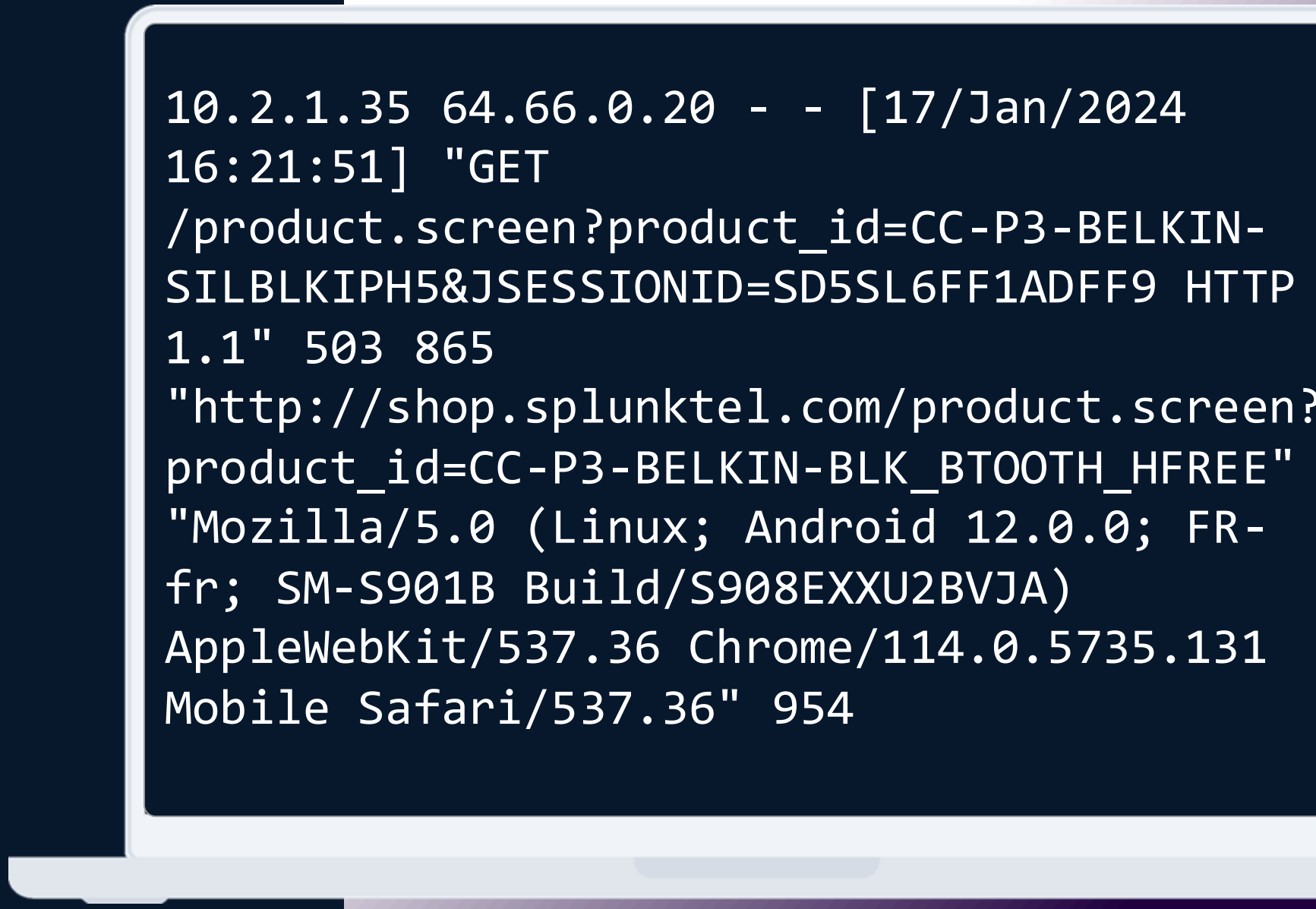
Generate alert for any user or system that exceeds a **risk score of 100 in a 30-day period**

ALERT

With one click, view all of the risk events that contributed to the alert

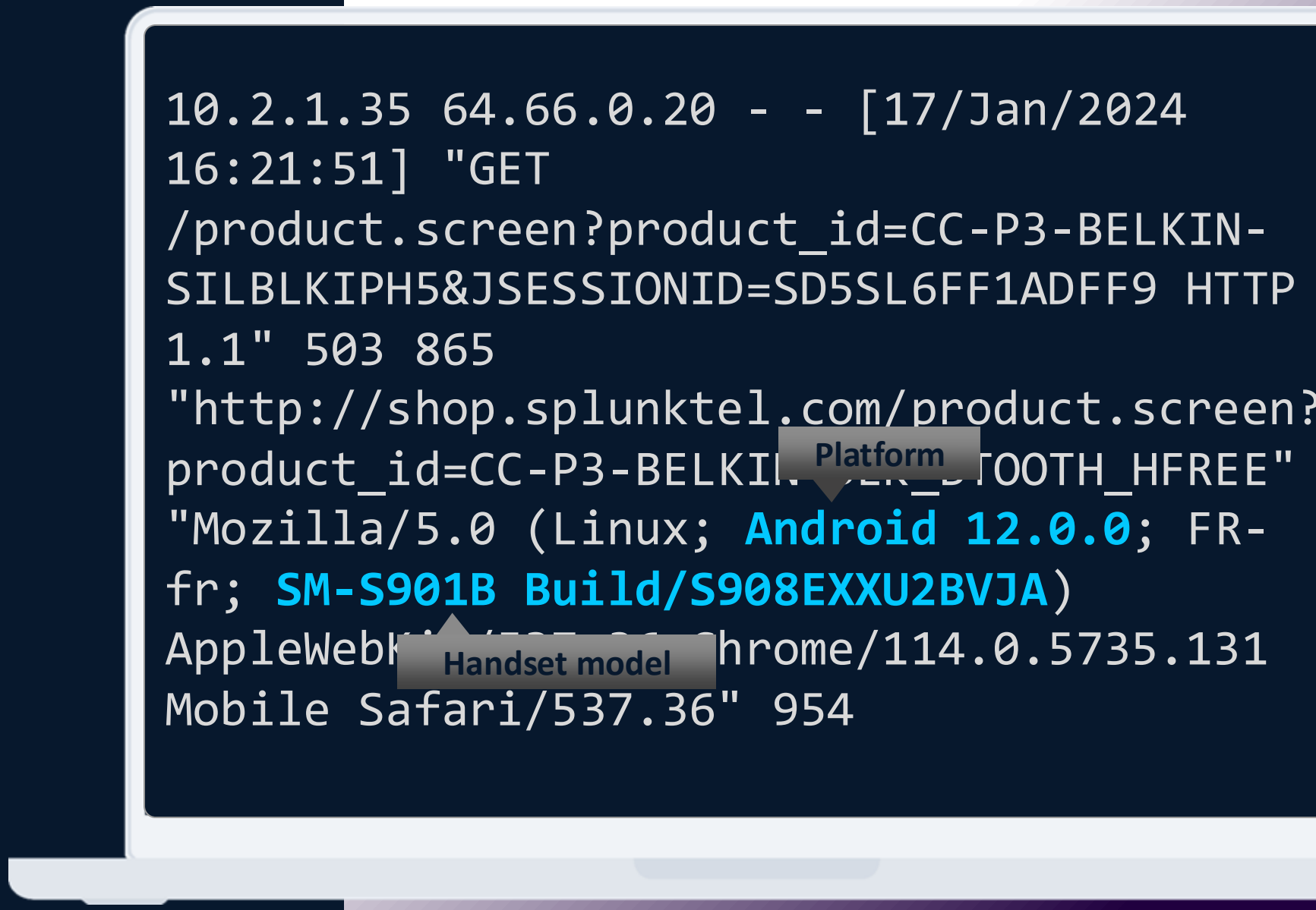
Splunk ITSI

Data Reuse



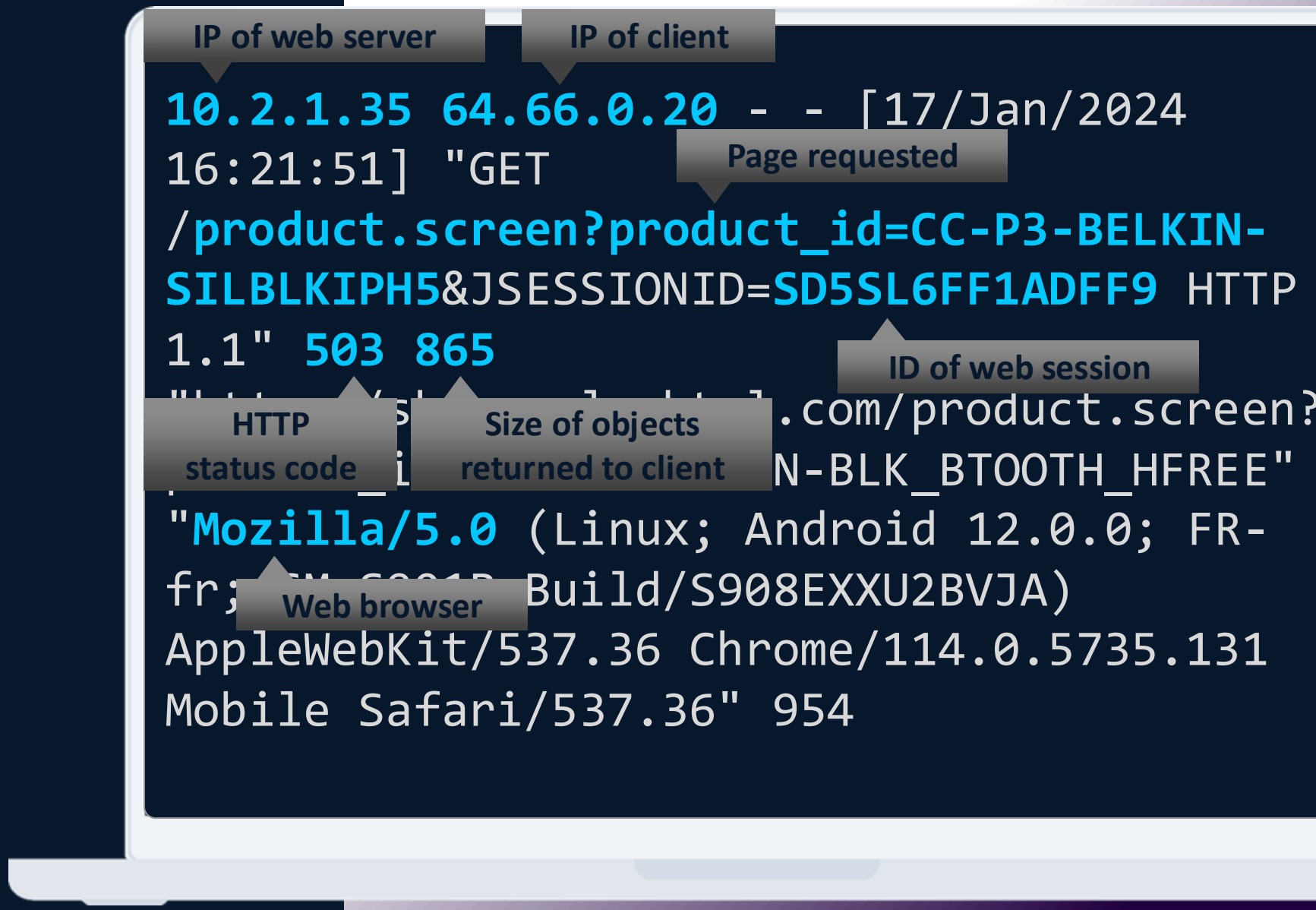
DevOps Use Case

Which mobile handsets should I test the most before releasing my new app?



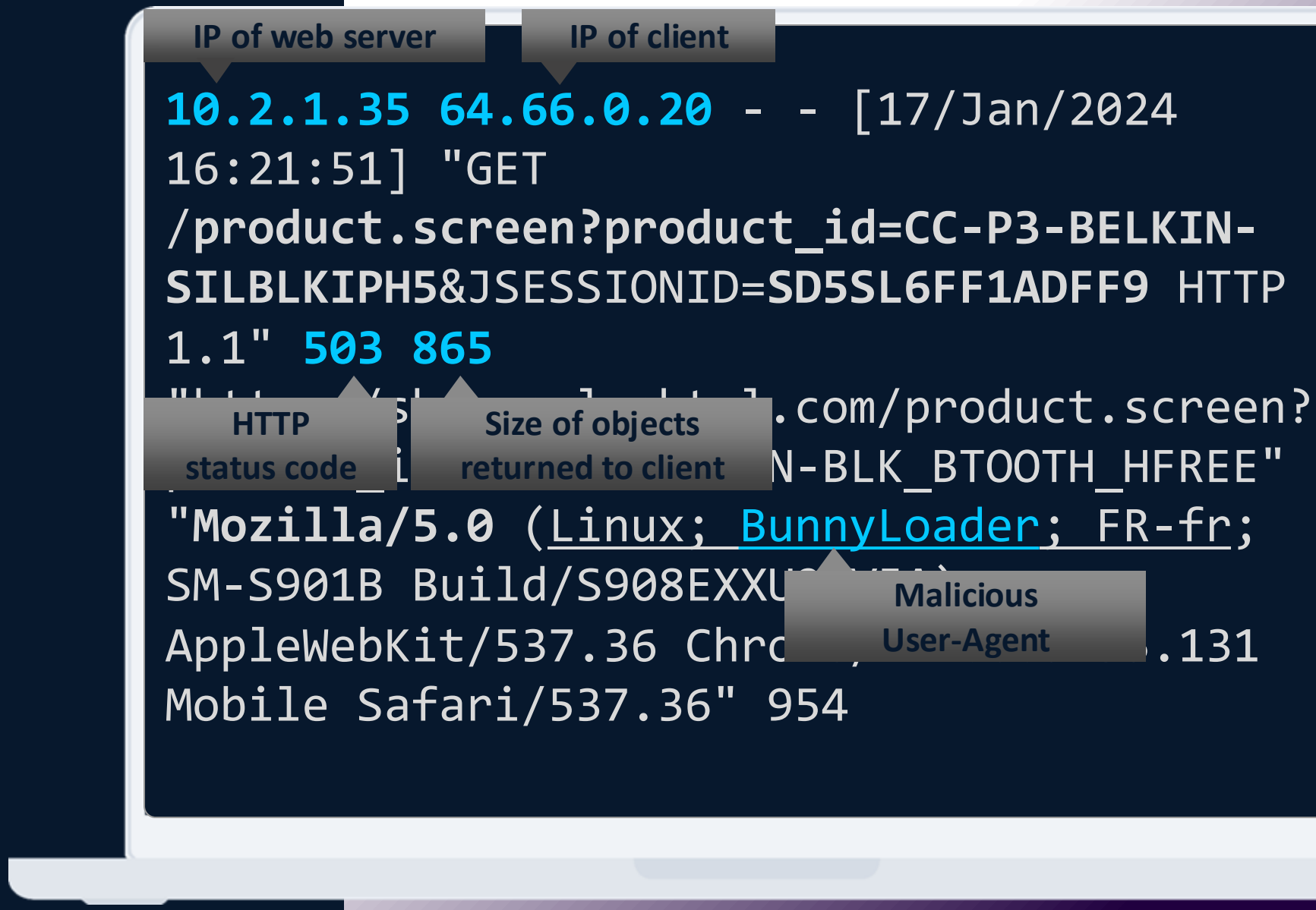
IT Ops Use Case

Which web pages are generating the most errors?



Security Use Case

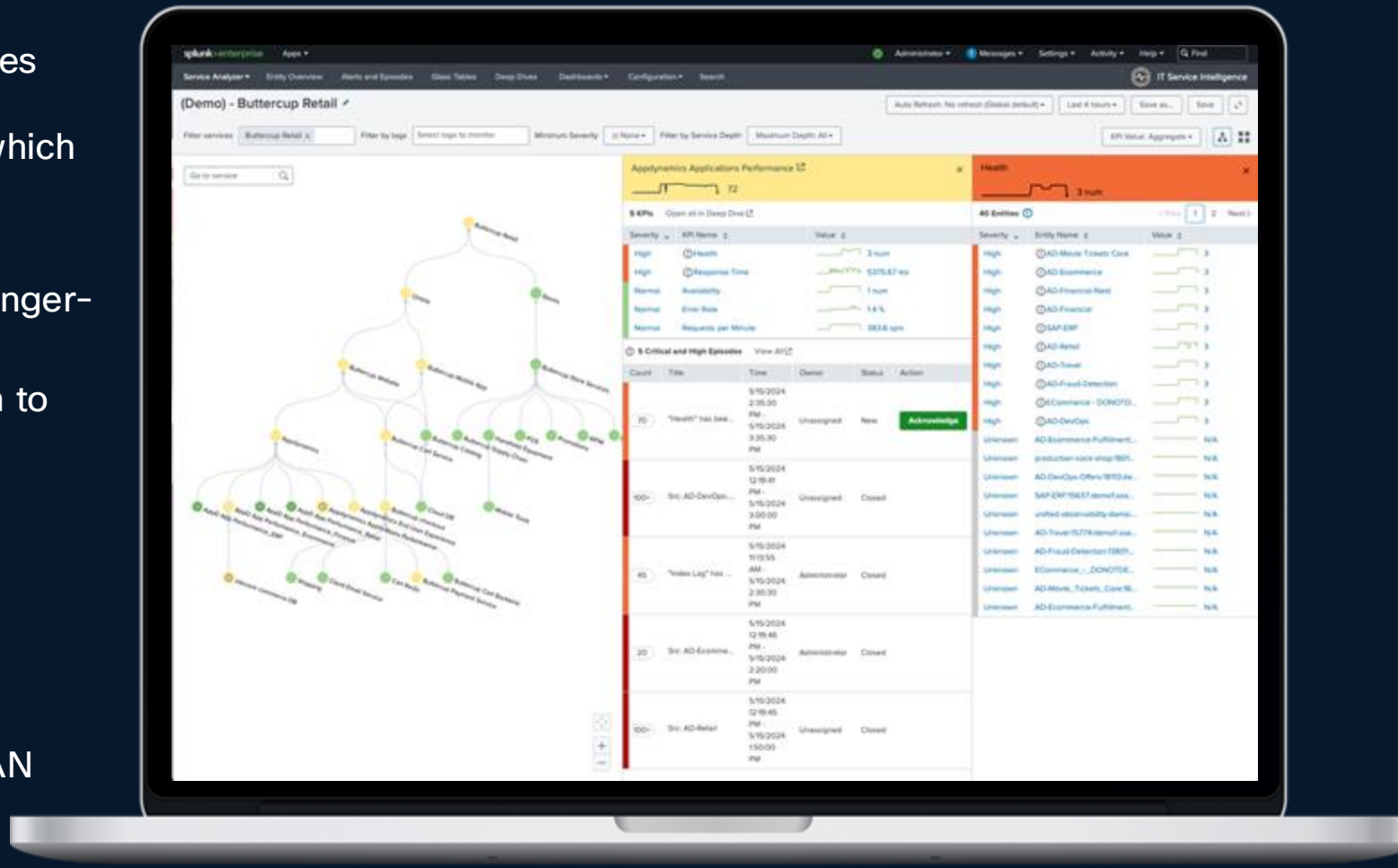
Do we have any malicious user-agents interacting with the network?



Bringing Security and IT Together with Business Context

Data Reuse

- Mapping alerts to business services helps teams understand which incidents matter most – not just which are loudest
- ITSI Bridges IT and Security to determine root cause and avoid finger-pointing to accelerate MTTX
- Shared language for collaboration to align IT Operations and SecOps around the same truth



Developing Next

- Integration of additional Cisco networking portfolio (ACI, SD-WAN manage etc.)