Power the SOC of the Future

Splunk Security

splunk> a CISCO company

Alex Pilger

Partner Technical Manager (CISSP, GCSA)

apilger@splunk.com

splunk>

Expanding attack surface

Siloed tools, teams, data, and workflows

Stalled innovation

Compliance mandates

Sophisticated threat actors

Growing attack volumes

Talent and skills shortages

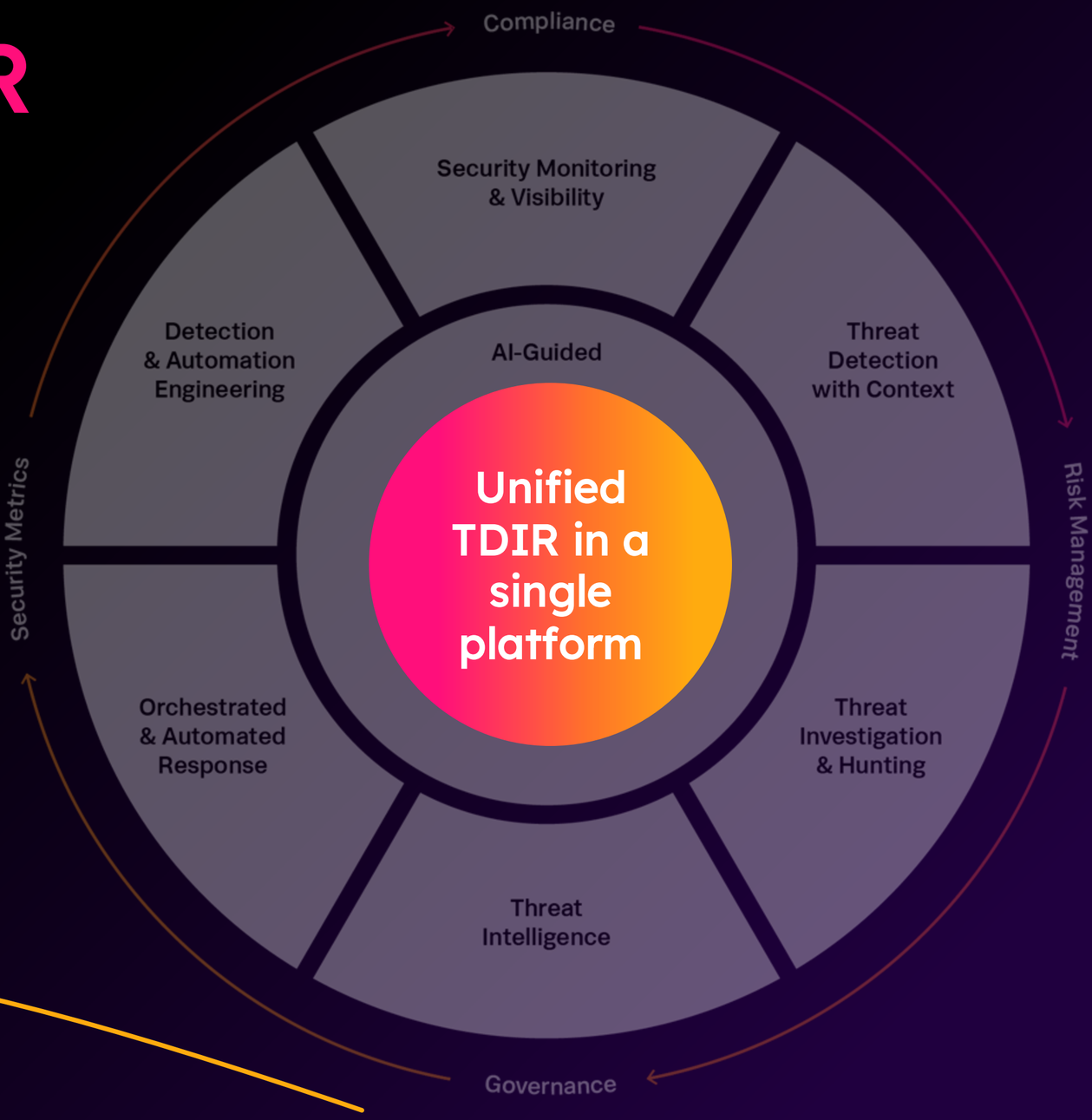

It's Time to
Reimagine
the SOC

The SOC
of the future

- ❑ Complete visibility
- ❑ Context and collaboration
- ❑ Clear path to resolution

With Unified TDIR at the core

- ❑ Tool consolidation
- ❑ Workflow efficiency
- ❑ Data management



Splunk's unified TDIR platform approach

Flexible Deployment Models

True Multi Vendor

Unified Analyst Experience
Workflows | Case Management | Collaboration

Threat Detection ⟷ Investigation ⟷ Response

Static | Dynamic (ML) | Pre-Built | Custom | Authoring

Risk-Based Alerting | Threat Hunting | Integrated Analytics

Enrichment | Automation | Orchestration | Playbooks

GenAI for SecOps
Summarization | Natural Language Search | Reporting

Common Services
Assets & Identities | Threat Intelligence | Risk

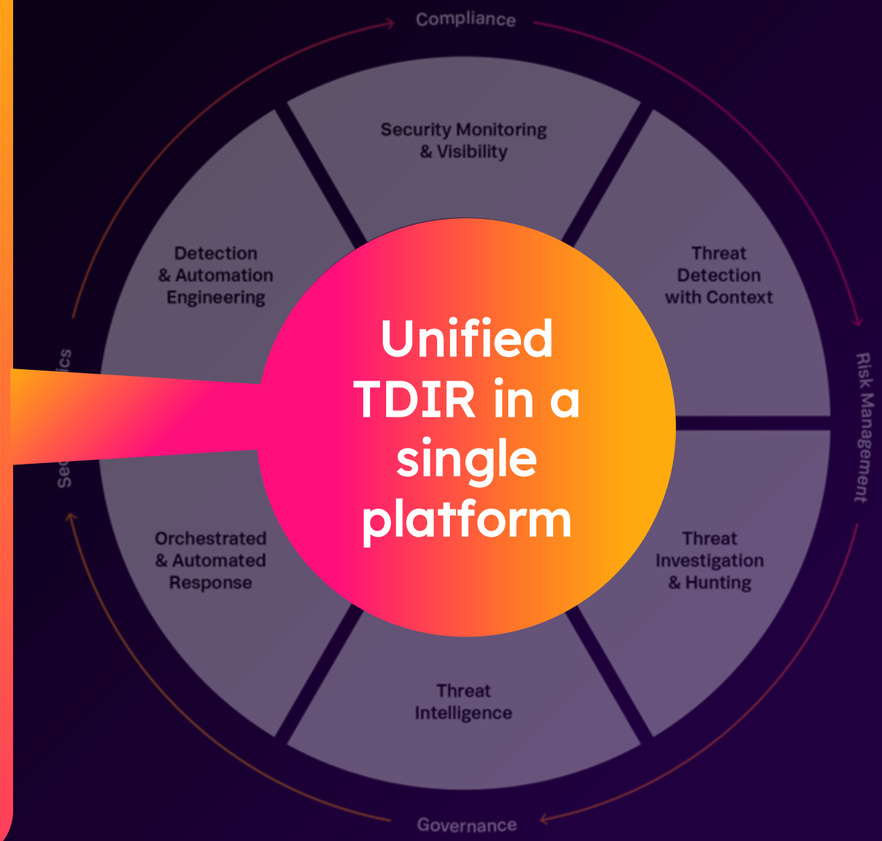
Data Management & Federation
Filter | Mask | Route | Access

Logs

Events

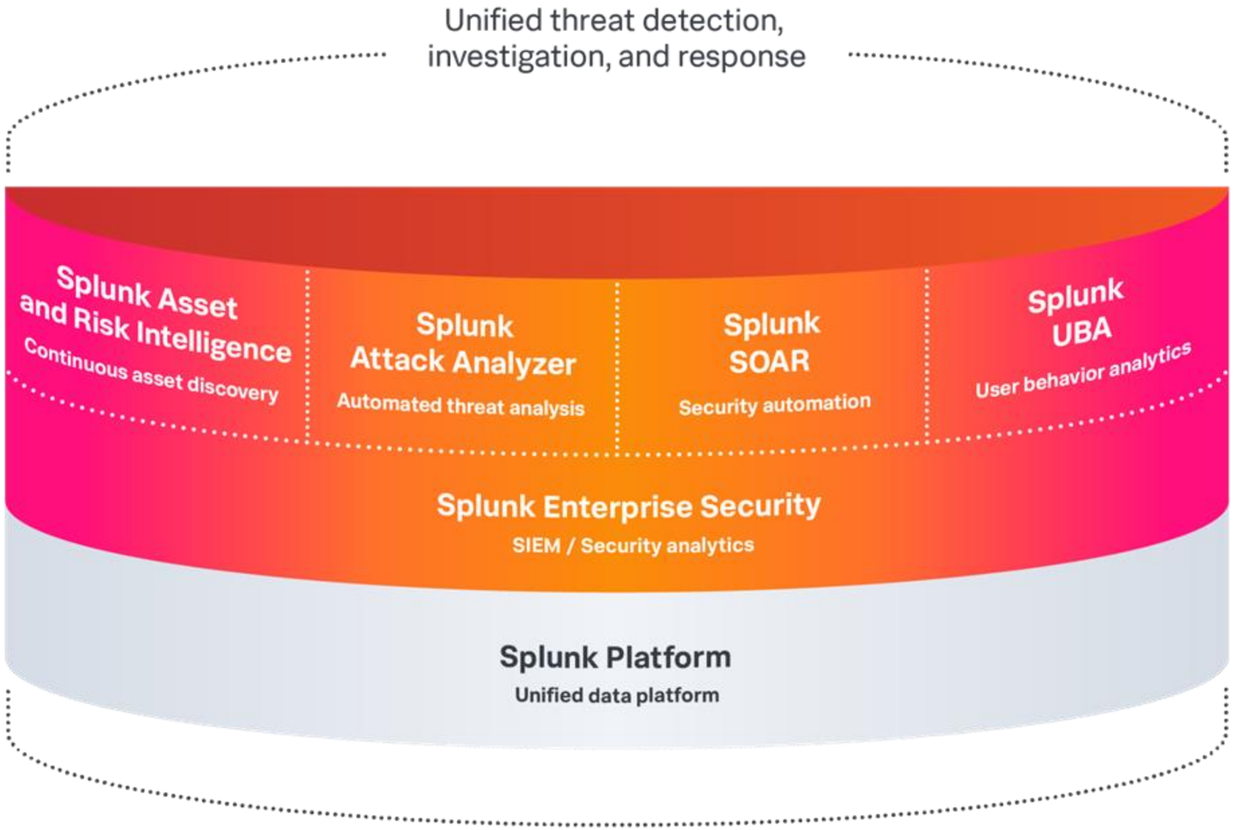
Alerts

Telemetry



Splunk Security

Powering the SOC of the future with the leading TDIR solution



Third-party tools

Cisco User/ Cloud/ Breach/XDR

Talos

Networking

IT/OT

Applications

Clouds

Data centers

Splunk Enterprise Security

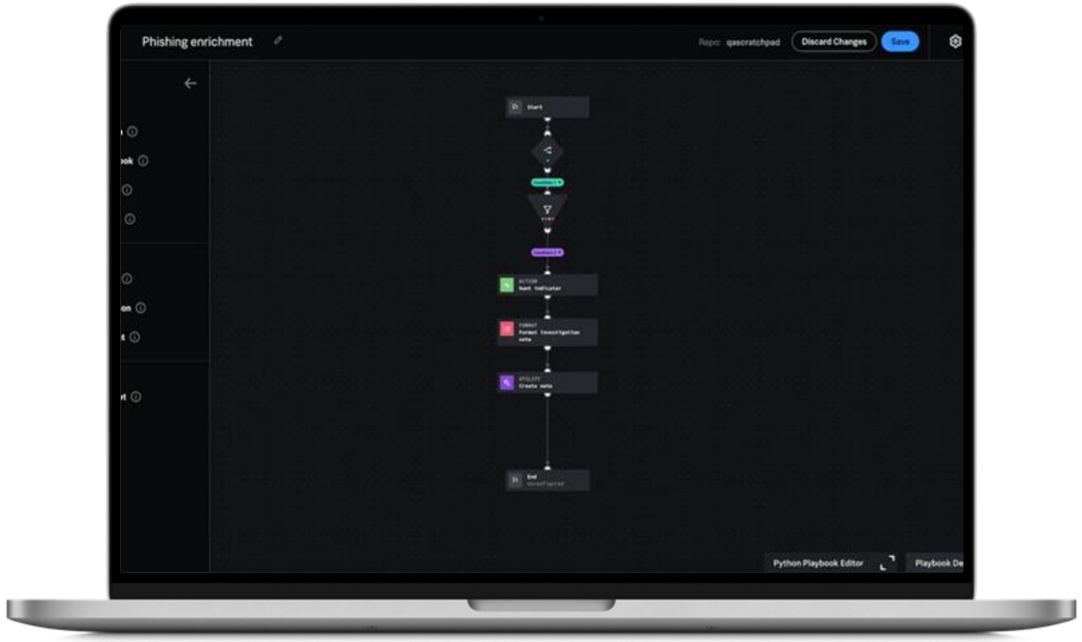
Industry-defining security analytics solution trusted by SOCs globally

- Unify threat detection, investigation and response using a modern work surface.
- Gain comprehensive visibility searching and analyzing any data at scale.
- Get insights into risk with customizable dashboards, visualizations, and reports.
- Prioritize with context using risk-based alerting to focus on imminent threats.
- Detect threats faster with over 1,700+ pre-built detections.
- Effectively detect anomalies and unknown threats with AI/ML.
- Build what you need with custom apps and powerful integrations.

Splunk SOAR

Work smarter by automating repetitive tasks, respond to security incidents in seconds, and increase analyst productivity.

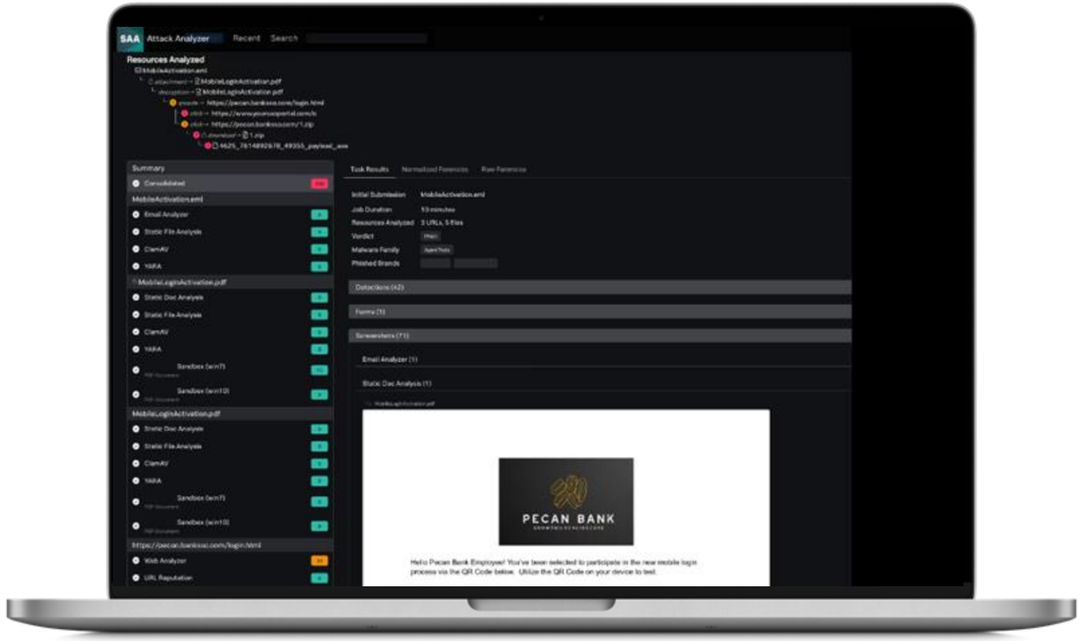
- Enhance team productivity with automation for speed and efficiency.
- Take prioritized actions to act on the most pressing threats.
- Respond with threat context for common threats automatically.
- Automate with ease using pre-built playbooks, integrations, or build customized playbooks.
- Get more out of your security stack by orchestrating workflows across teams and tools.
- Foster collaborative investigations for a cohesive investigative process.
- Actionize your data by integrating SOAR with Splunk ES and Splunk Attack Analyzer.



Splunk Attack Analyzer

Automatic analysis of active threats for contextual insights to accelerate investigations & resolution

- Take the manual work out of threat analysis and integrate into SOC workflows seamlessly.
- Ensure a baseline standard of investigation with consistent, comprehensive, and high-quality threat analysis.
- Interact seamlessly with malicious content in a dedicated, unattributable environment.
- Achieve intelligent automation for end-to-end threat analysis and response with easy integration with Splunk SOAR.
- Enhance the analyst experience by reducing the toil of threat analysis and free up valuable time.



Director, Global Security Operations, Splunk

Splunk Asset and Risk Intelligence (ARI)

Continuous asset and identity intelligence

- Gain comprehensive asset visibility to reduce risk exposure.
- Accelerate security investigation with accurate asset context.
- Identify compliance gaps in security controls.
- Seamless integration and deployment with Splunk Enterprise Security.
- Get more out of your security stack by orchestrating workflows across teams and tools.
- Bridge the IT and Security gap with seamless ServiceNow CMDB integration.

Integrations to protect your entire digital footprint

Threat intelligence

Enhance defense against known and unknown threats

Splunk + Cisco Talos

Security alerts and context

Accelerate detection, investigation and response

Splunk + Cisco Security Cloud App

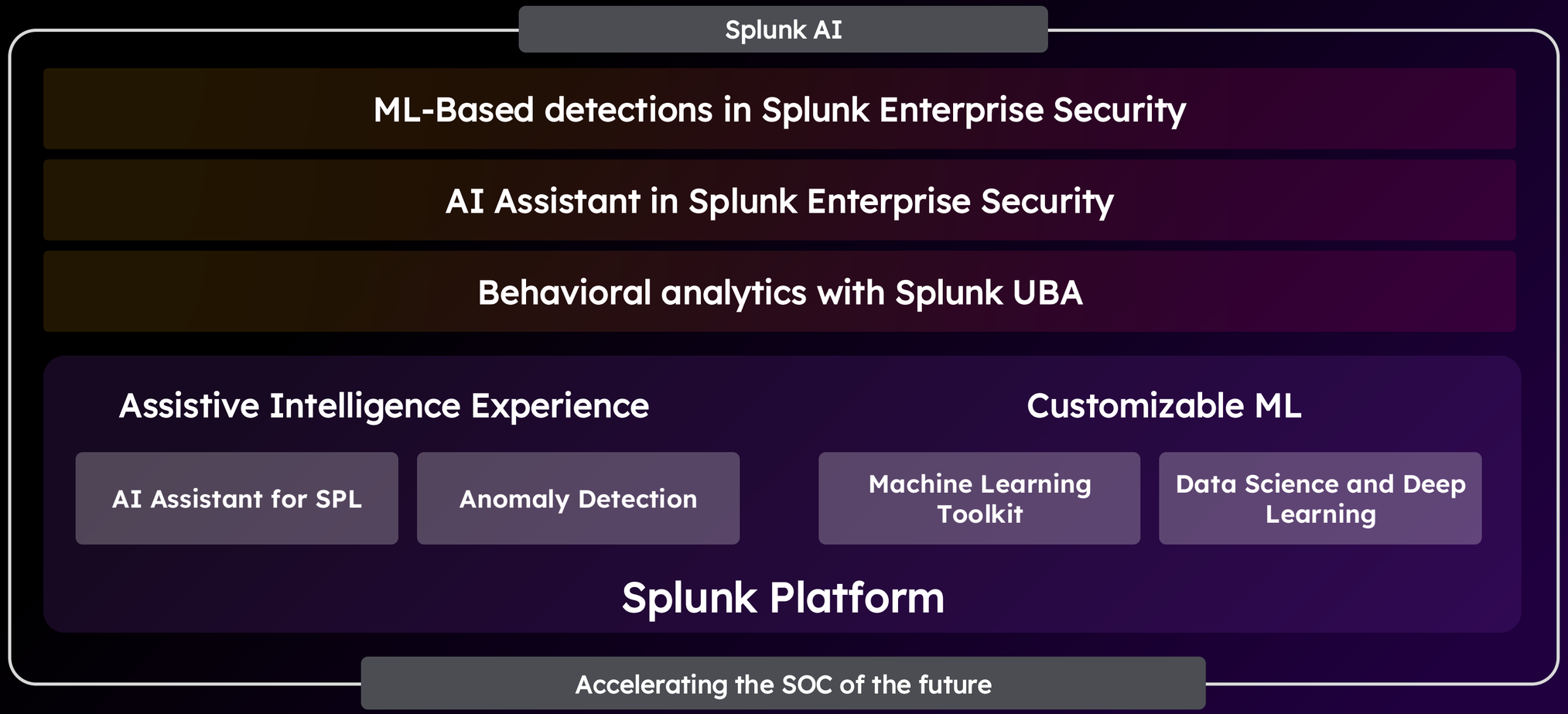
Secure AI

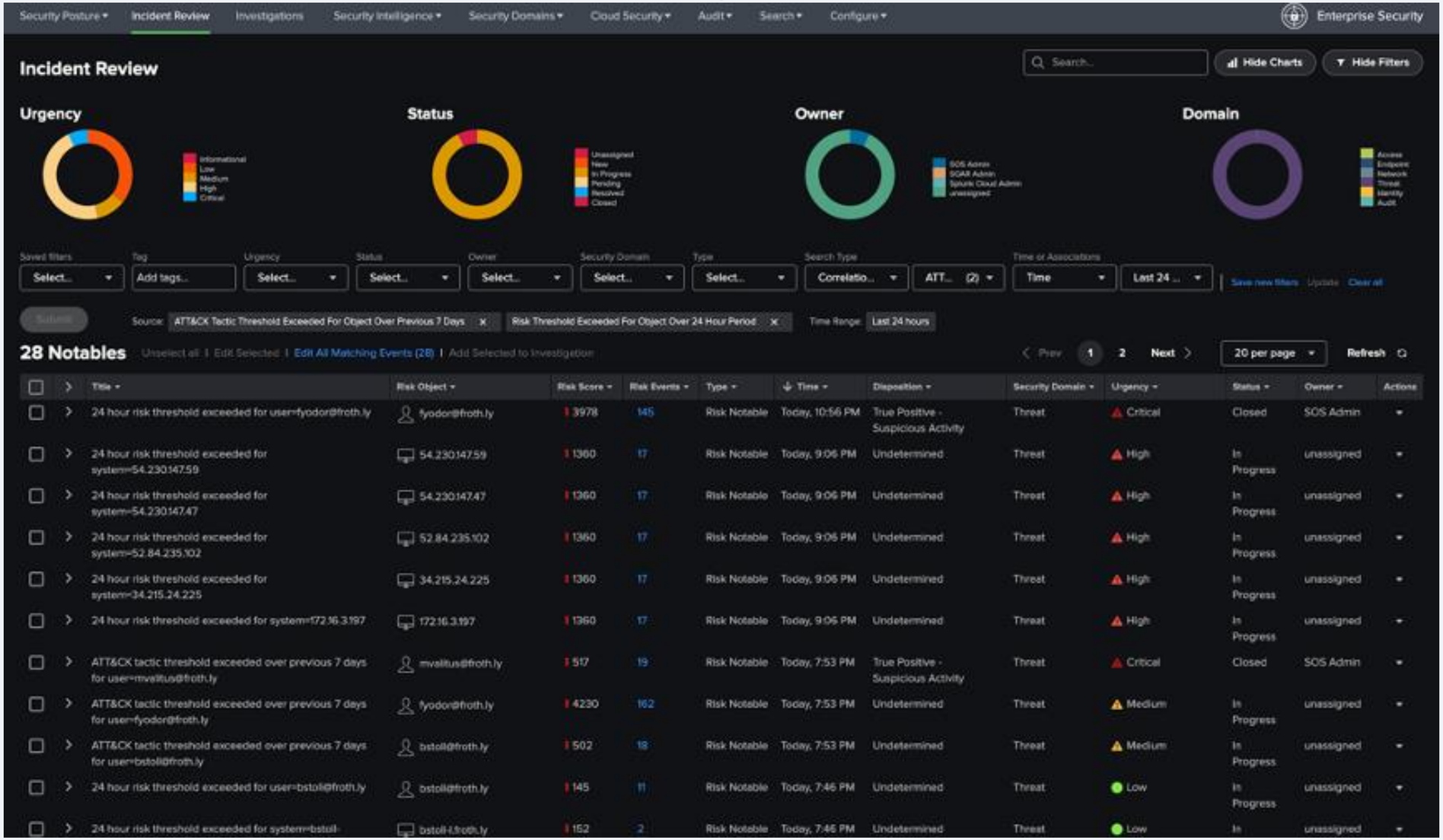
Detect and reduce AI-based risk

Splunk + AI Defense

Driving a new wave of maturity for the SOC

Powered by Splunk AI



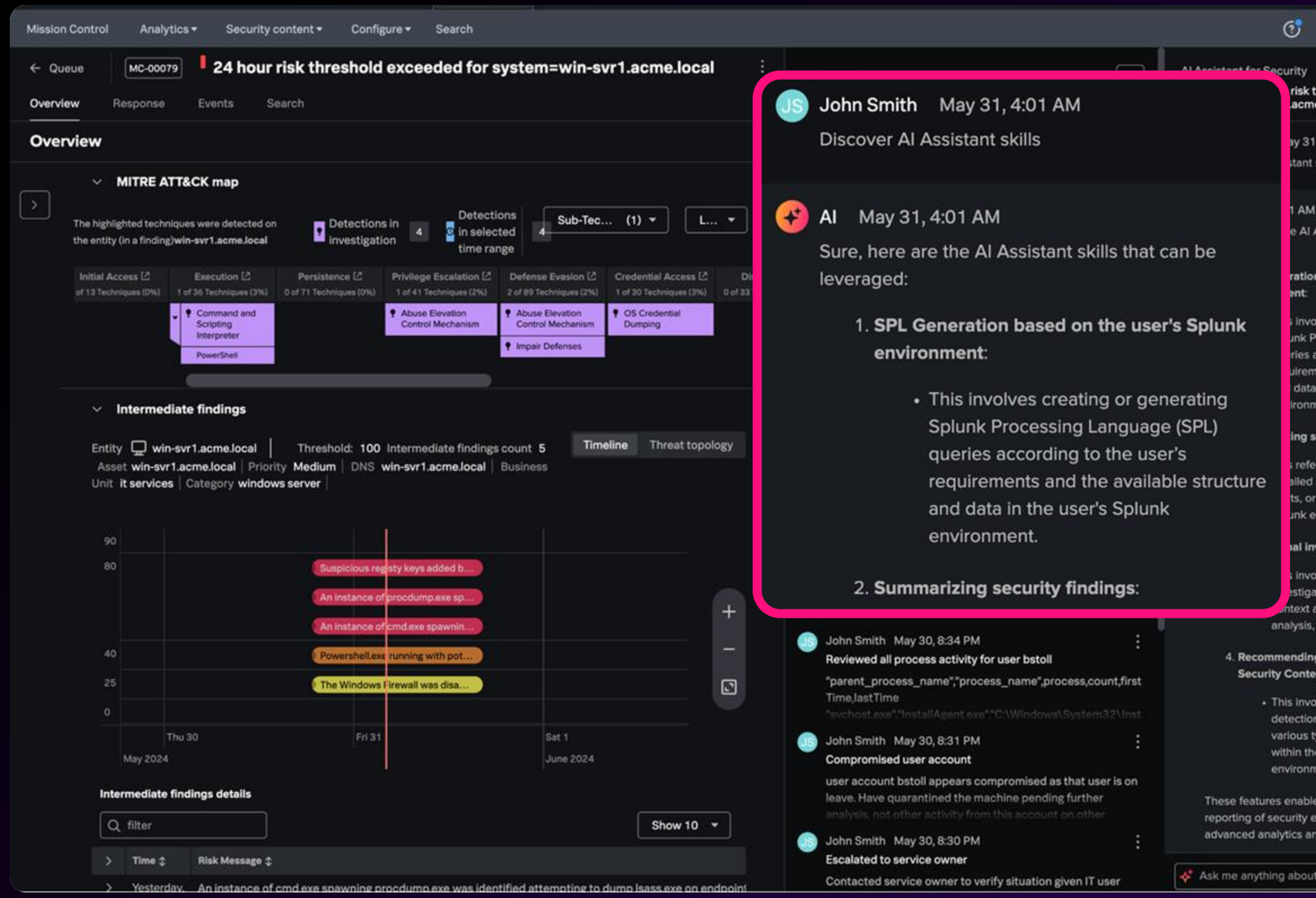


SOC Demo

AI Assistant in Enterprise Security

Guided security workflows where you do your work

- Answer analyst questions to guide daily workflows
- Save time while addressing threats more rapidly
- Use natural language queries to get answers during investigations



UI shown is for illustration; not final product.

Your Questions?

Thank You!