

Power the SOC of the Future

Splunk Security



Alex Pilger

Partner Technical Manager (CISSP, GCSA)

apilger@splunk.com





**Expanding attack
surface**



**Siloed tools,
teams, data,
and workflows**



**Stalled
innovation**



**Compliance
mandates**



It's Time to
Reimagine
the SOC

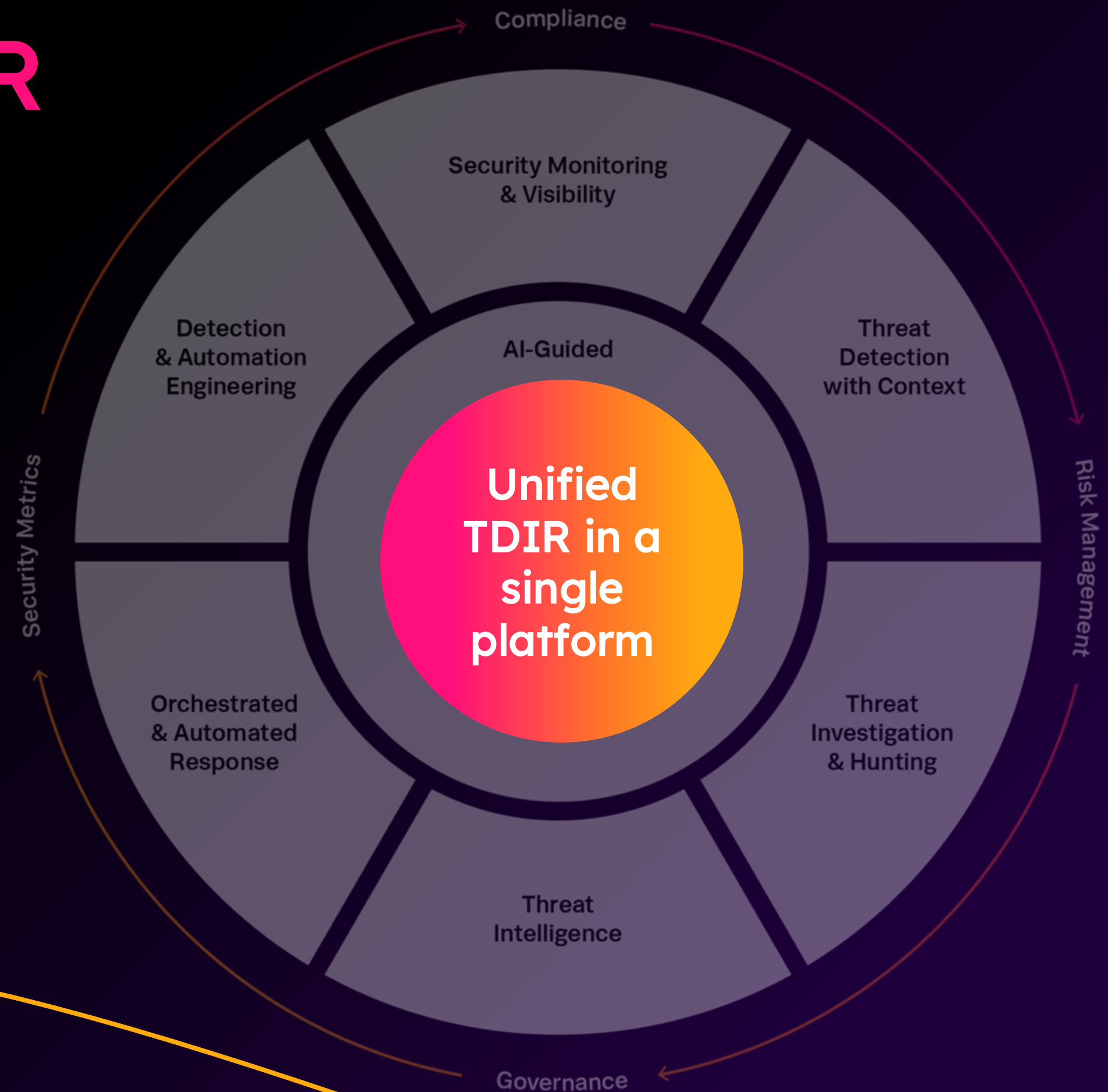
The SOC of the future

- ❑ 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

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



Investigation

Risk-Based Alerting | Threat Hunting | Integrated Analytics



Response

Enrichment | Automation | Orchestration | Playbooks



GenAI for SecOps
Summarization | Natural Language Search | Reporting



Common Services
Assets & Identities | Threat Intelligence | Risk



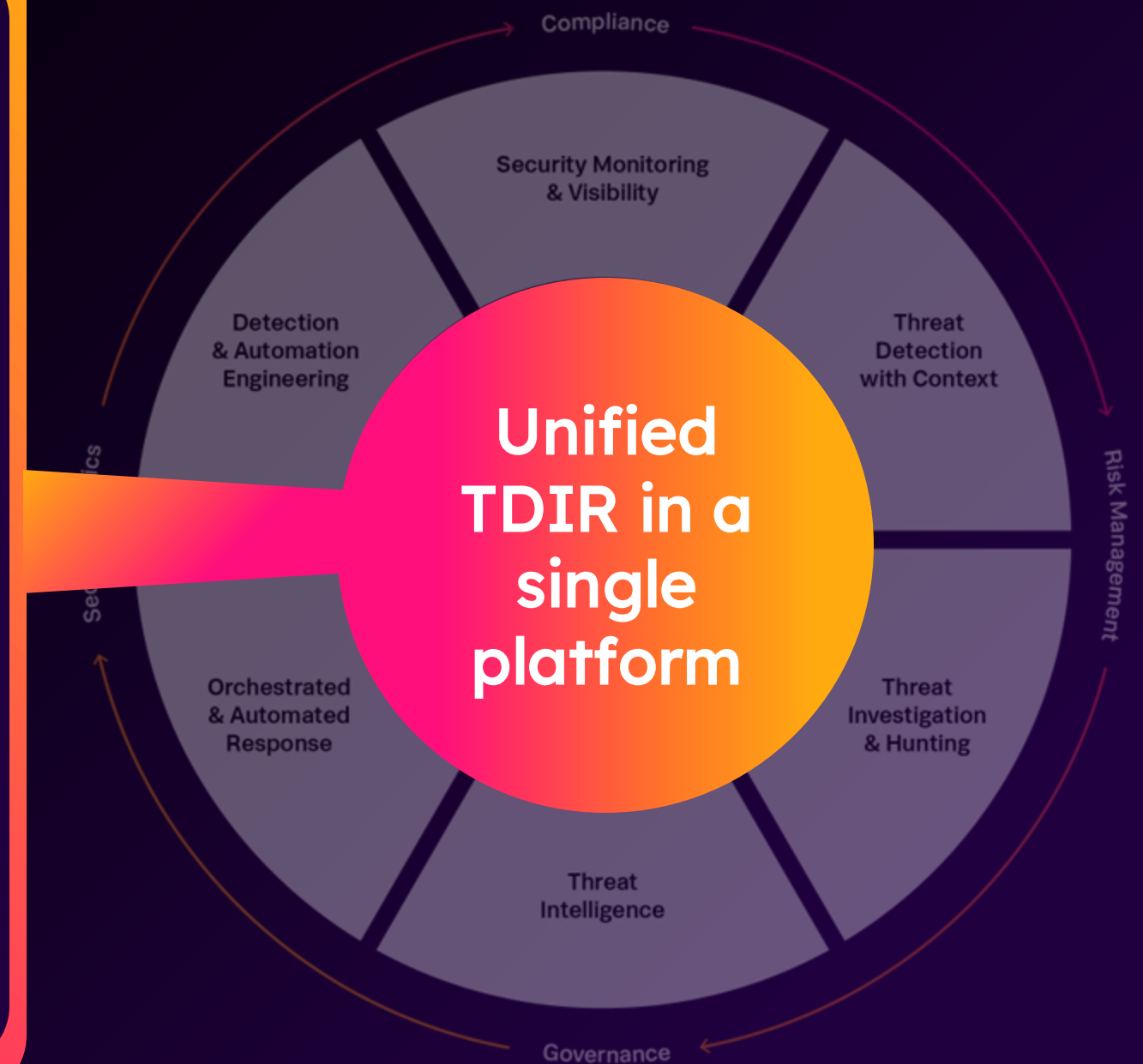
Data Management & Federation
Filter | Mask | Route | Access

Logs

Events

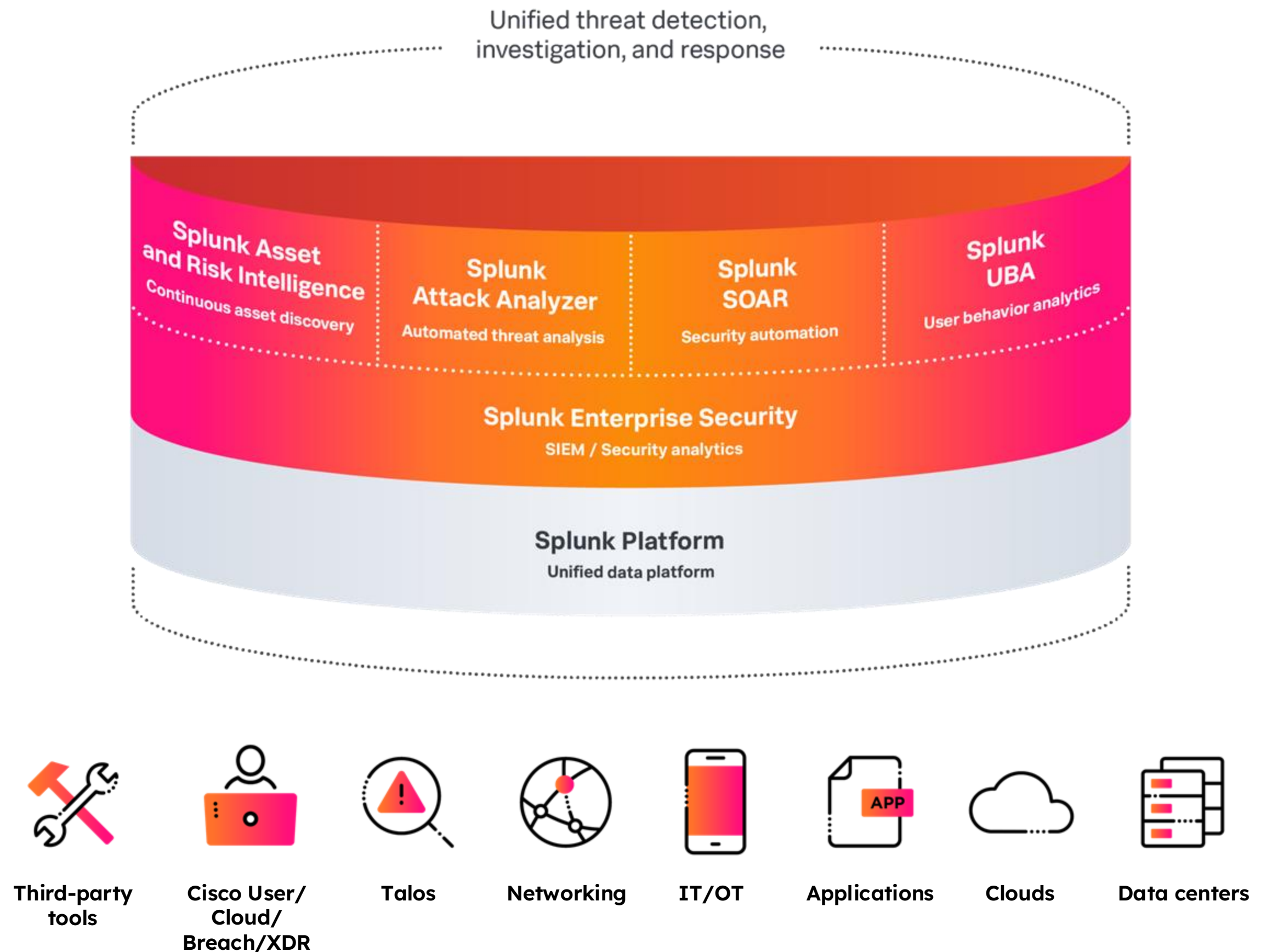
Alerts

Telemetry



Splunk Security

Powering the
SOC of the
future
with the
leading TDIR
solution



Splunk Enterprise Security

Industry-defining security analytics solution trusted by SOC teams 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.

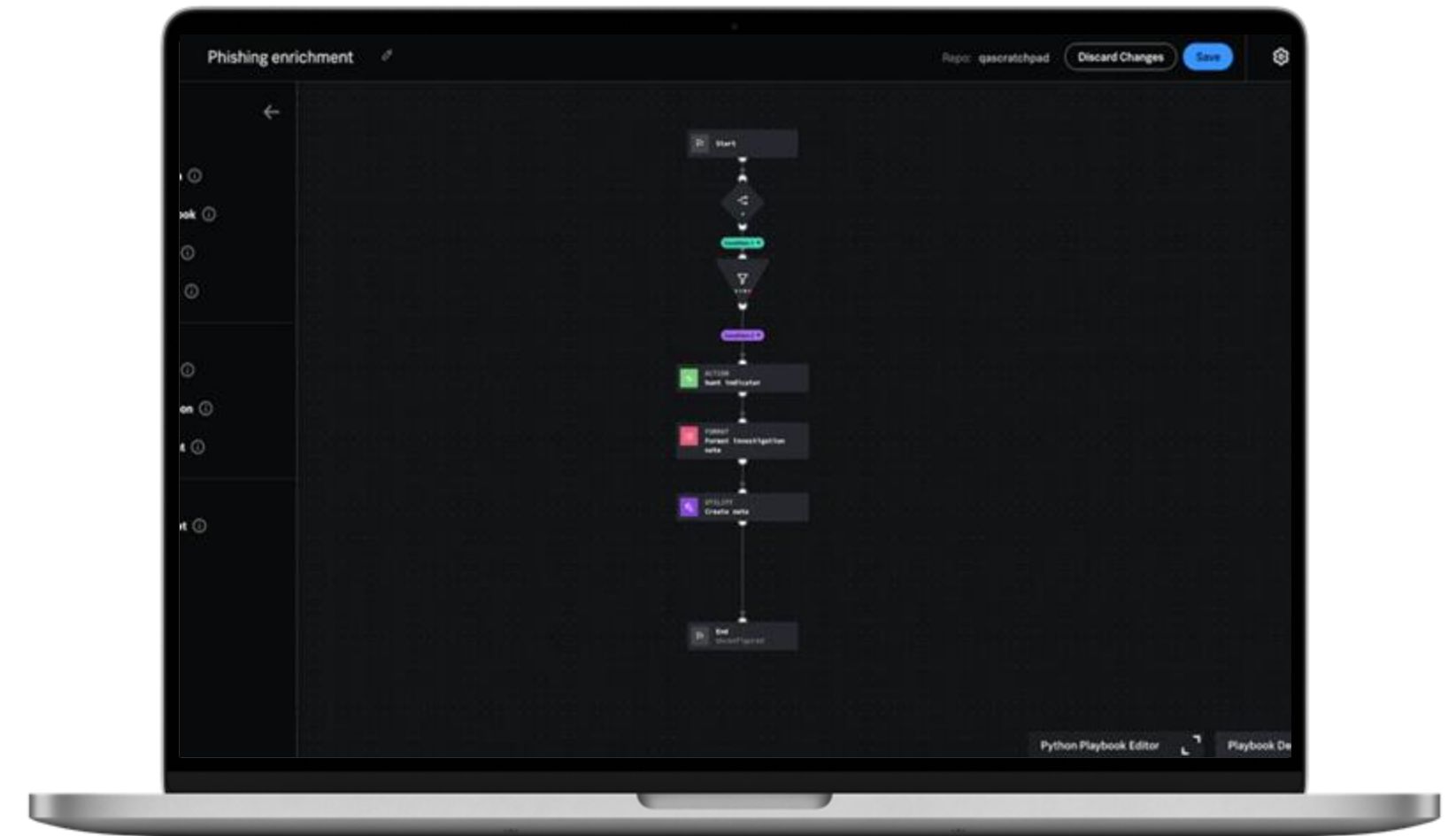


Chief Global Security Officer,

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.

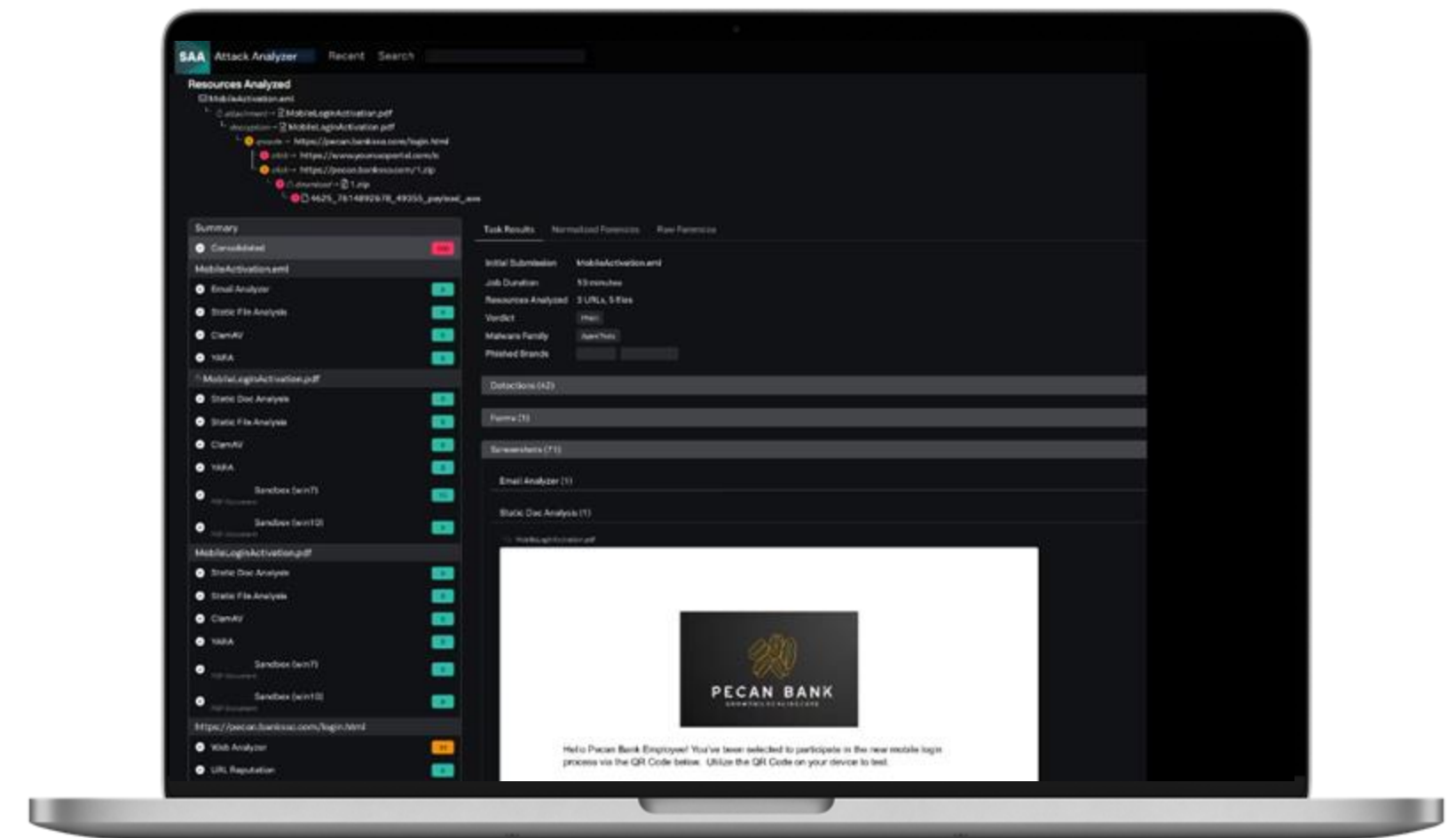


Security Detection Engineer, Tide

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.



For 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*

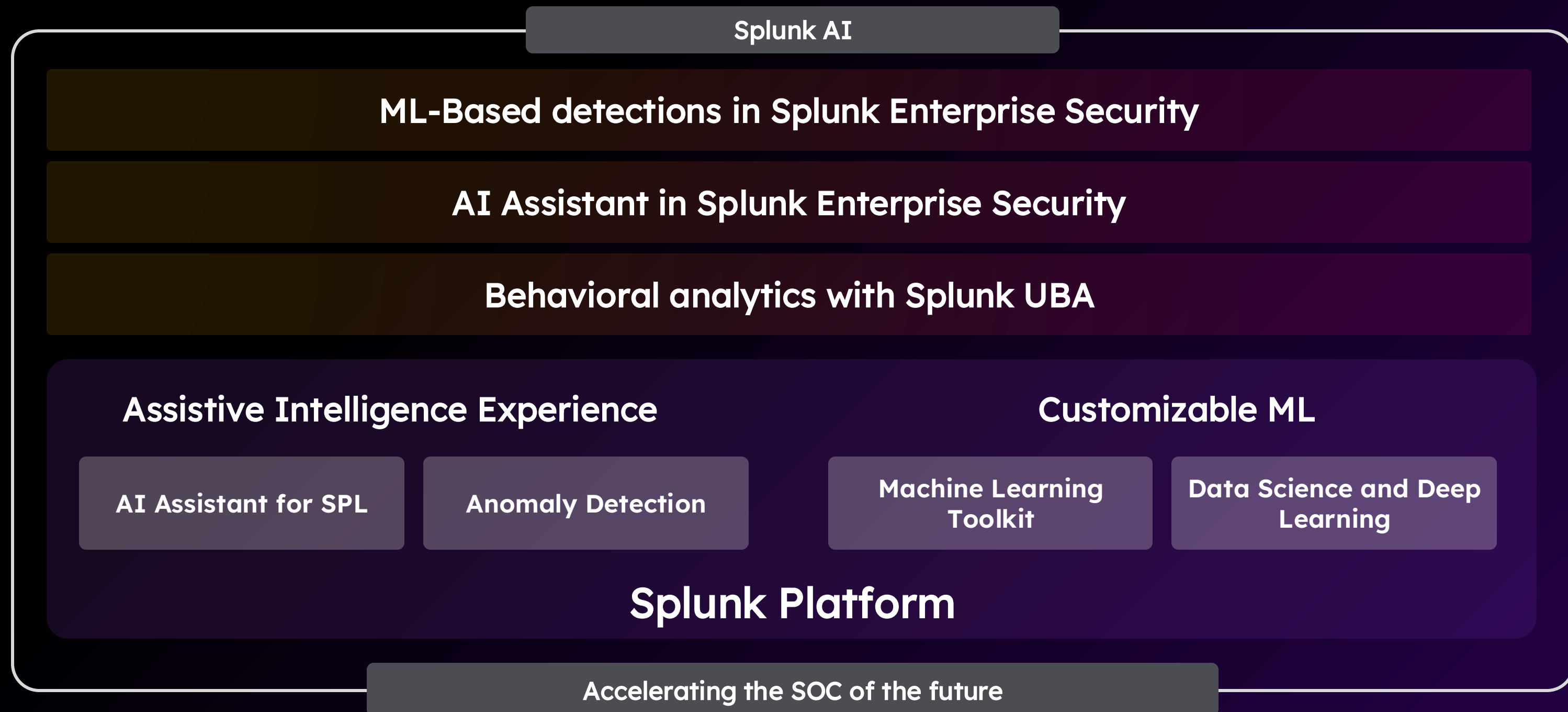
Secure AI

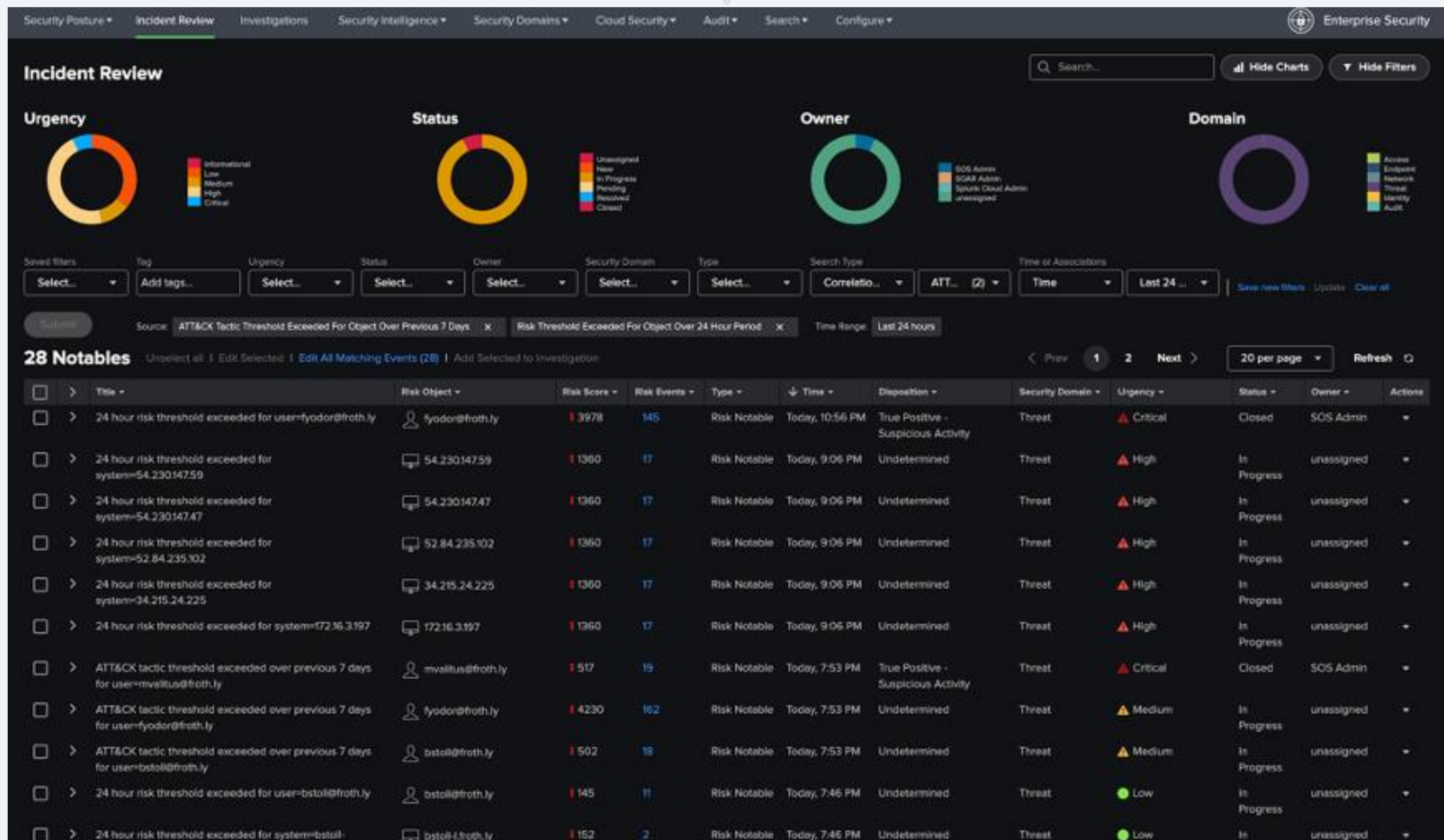
Detect and reduce AI-
based risk

*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

The screenshot displays the Splunk Enterprise Security interface. At the top, a navigation bar includes 'Mission Control', 'Analytics', 'Security content', 'Configure', and 'Search'. Below this, a 'Queue' section shows a message: '24 hour risk threshold exceeded for system=win-svr1.acme.local'. The 'Overview' tab is active, showing a 'MITRE ATT&CK map' with various techniques categorized by initial access, execution, persistence, privilege escalation, defense evasion, and credential access. A timeline view shows findings for the entity 'win-svr1.acme.local' from May 30 to June 1, 2024. The findings include: 'Suspicious registry keys added b...', 'An instance of procdump.exe sp...', 'An instance of cmd.exe spawnin...', 'Powershell.exe running with pot...', and 'The Windows Firewall was disa...'. A chat window on the right shows a conversation with 'John Smith' and an 'AI Assistant'.

JS John Smith May 31, 4:01 AM
Discover AI Assistant skills

AI May 31, 4:01 AM
Sure, here are the AI Assistant skills that can be leveraged:

1. **SPL Generation based on the user's Splunk environment:**
 - This involves creating or generating Splunk Processing Language (SPL) queries according to the user's requirements and the available structure and data in the user's Splunk environment.
2. **Summarizing security findings:**

JS John Smith May 30, 8:34 PM
Reviewed all process activity for user bstoll
"parent_process_name","process_name",process,count,first Time,lastTime
"svchost.exe","InstallAgent.exe","C:\Windows\System32\Inst

JS John Smith May 30, 8:31 PM
Compromised user account
user account bstoll appears compromised as that user is on leave. Have quarantined the machine pending further analysis. not other activity from this account on other

JS John Smith May 30, 8:30 PM
Escalated to service owner
Contacted service owner to verify situation given IT user

4. **Recommending Security Conte**
• This invo detection various t within th environm
These features enable reporting of security e advanced analytics an

Ask me anything about

UI shown is for illustration; not final product.

Your Questions?

Thank You!