
.conf18
splunk>

Forward Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk>

HAIYAN SONG

SVP & General Manager, Security Markets

splunk>

1

SPLUNK FOR SECURITY TODAY

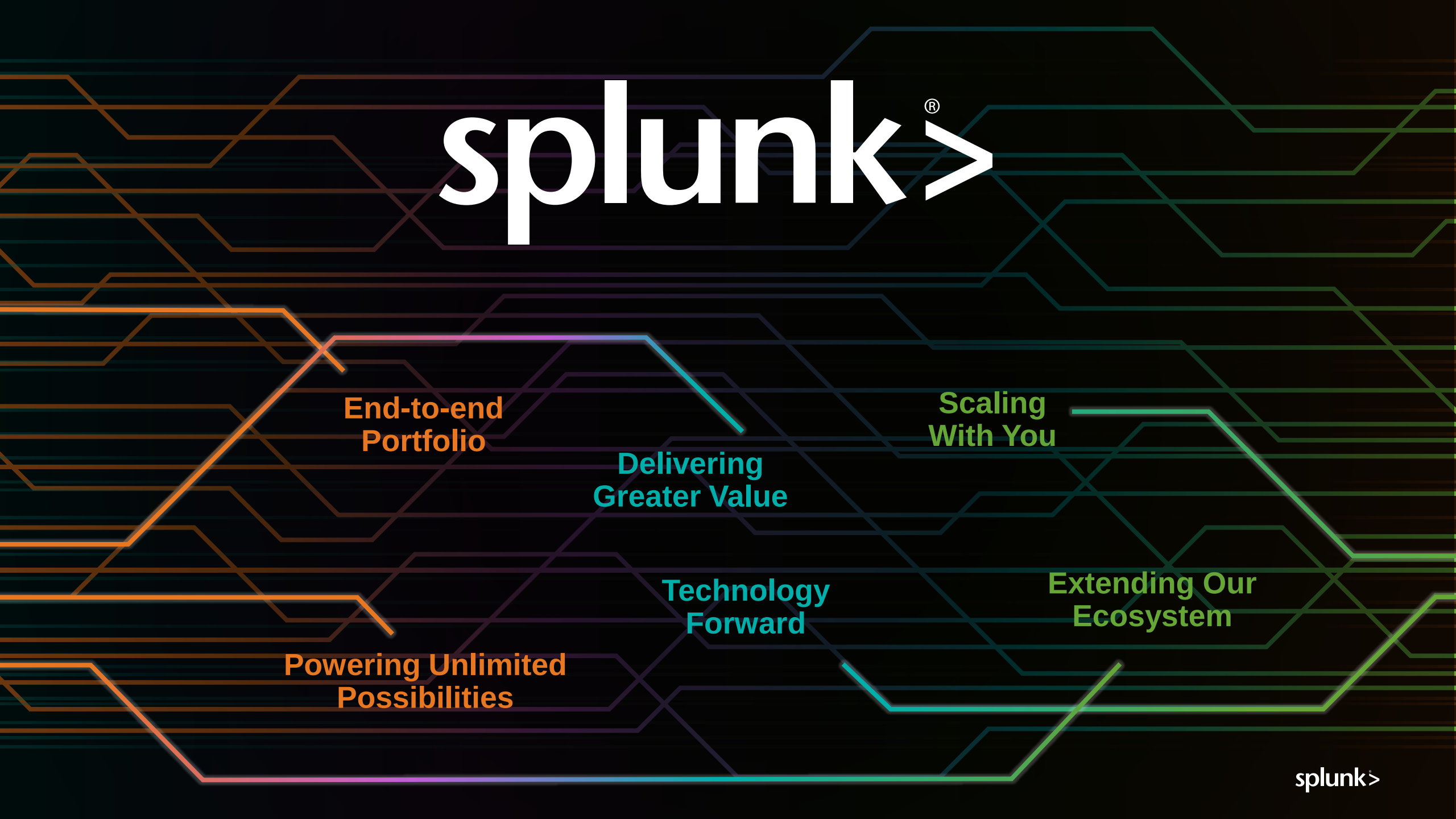
2

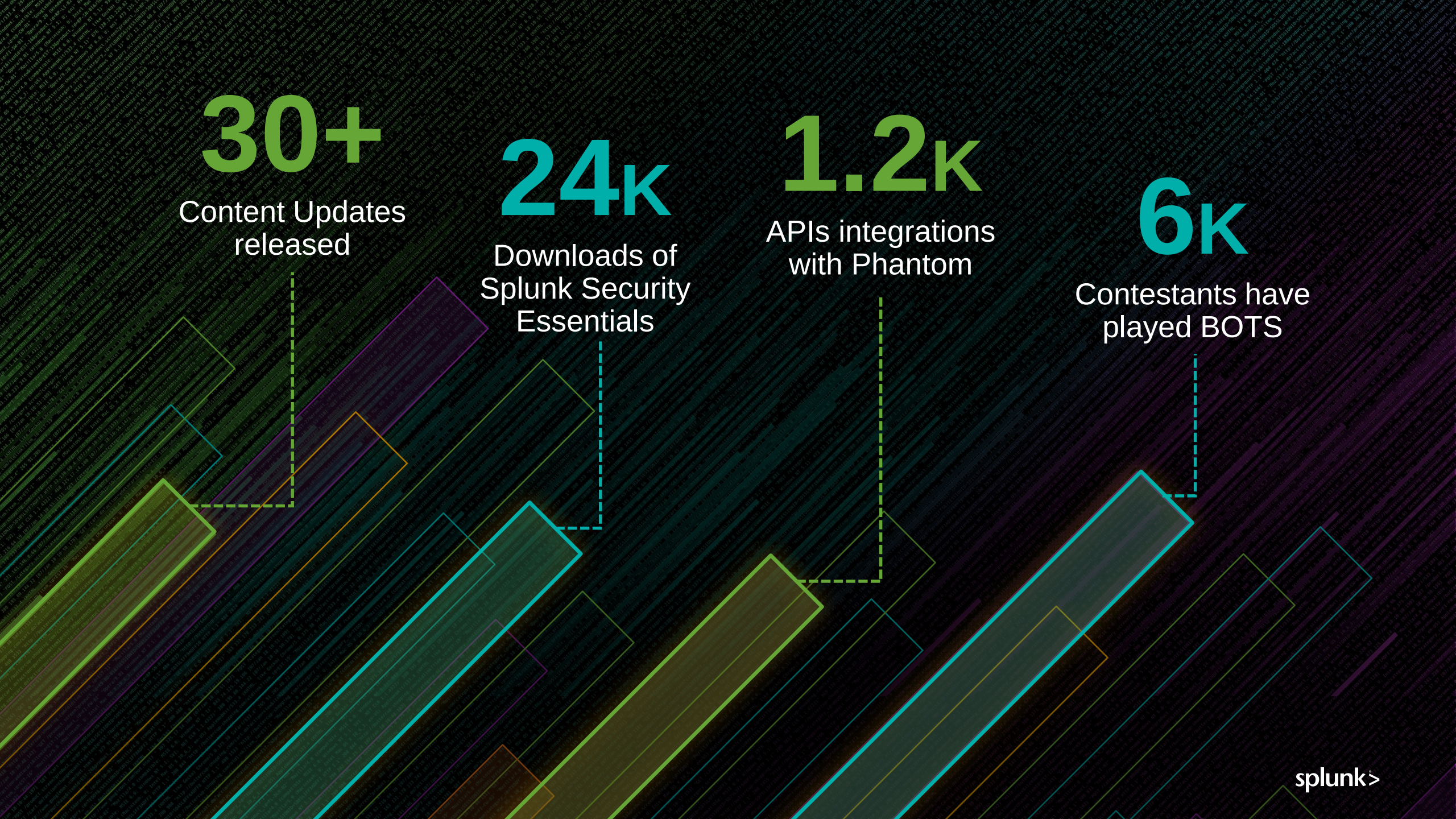
WHAT'S NEXT

3

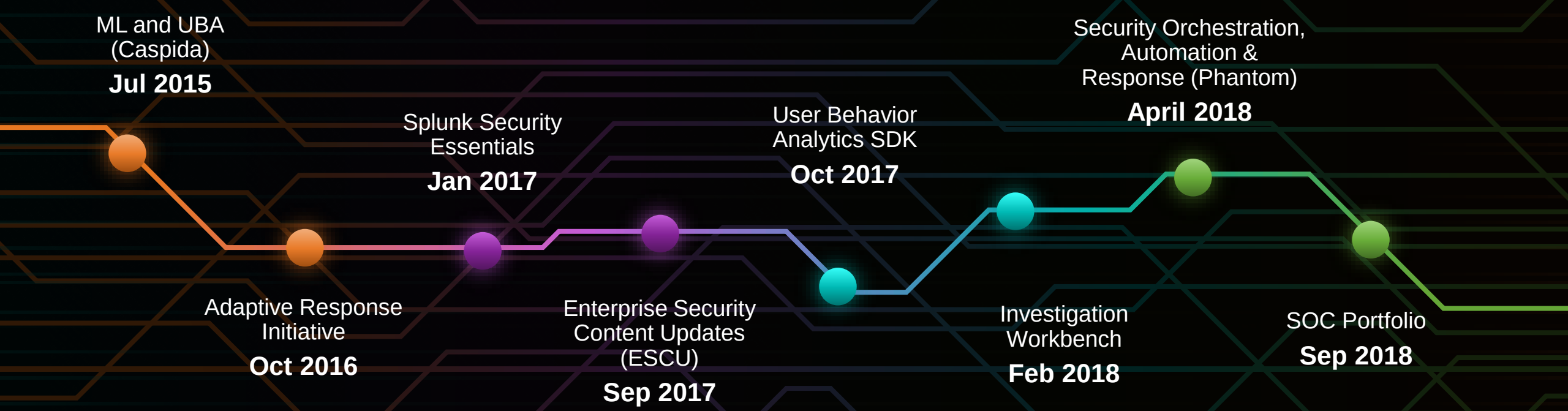
PAVING THE PATH FOR TOMORROW

splunk>


splunk>
End-to-end Portfolio
Delivering Greater Value
Scaling With You
Technology Forward
Extending Our Ecosystem
Powering Unlimited Possibilities
splunk>


30+
Content Updates released
24K
Downloads of Splunk Security Essentials
1.2K
APIs integrations with Phantom
6K
Contestants have played BOTS
splunk>

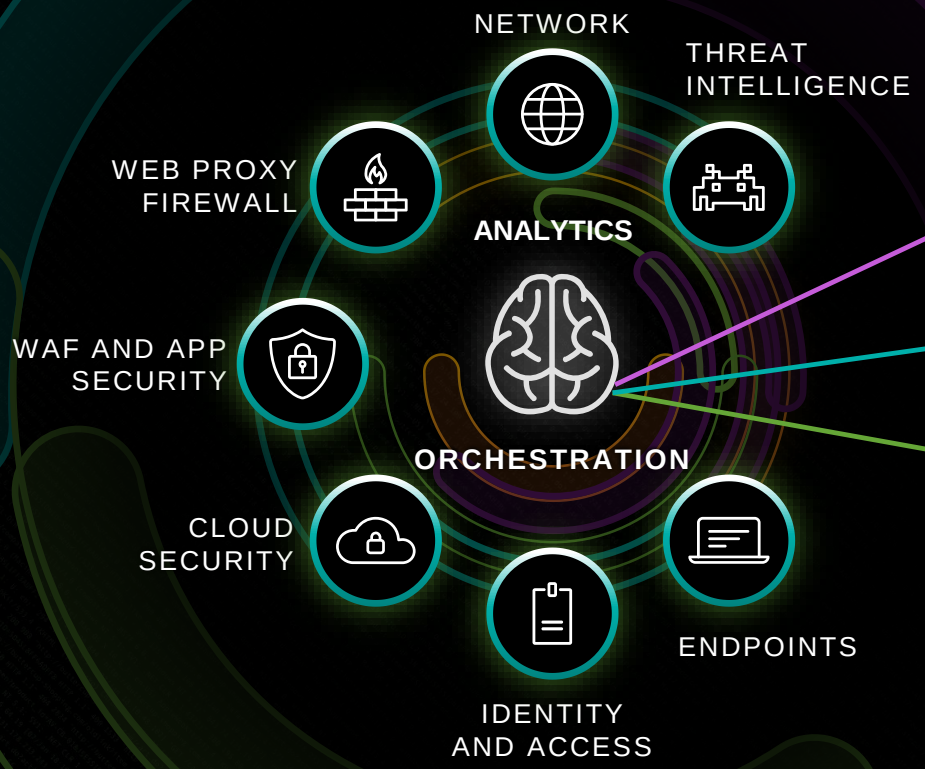
Splunk for Security

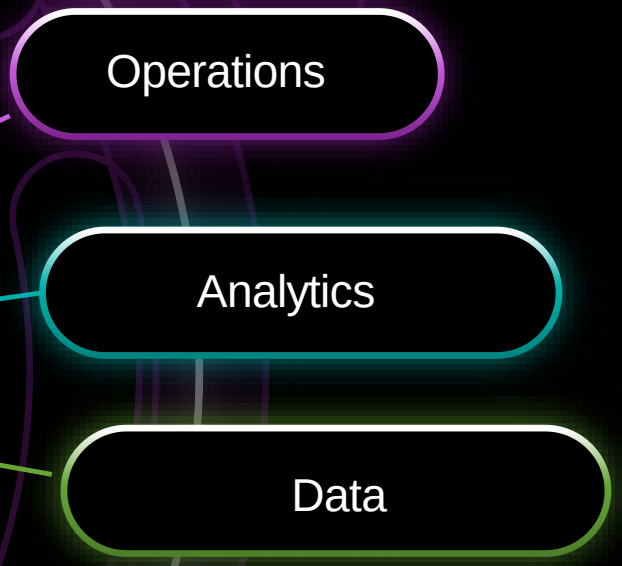


Security Nerve Center

splunk>

SOARing High with Phantom Buy



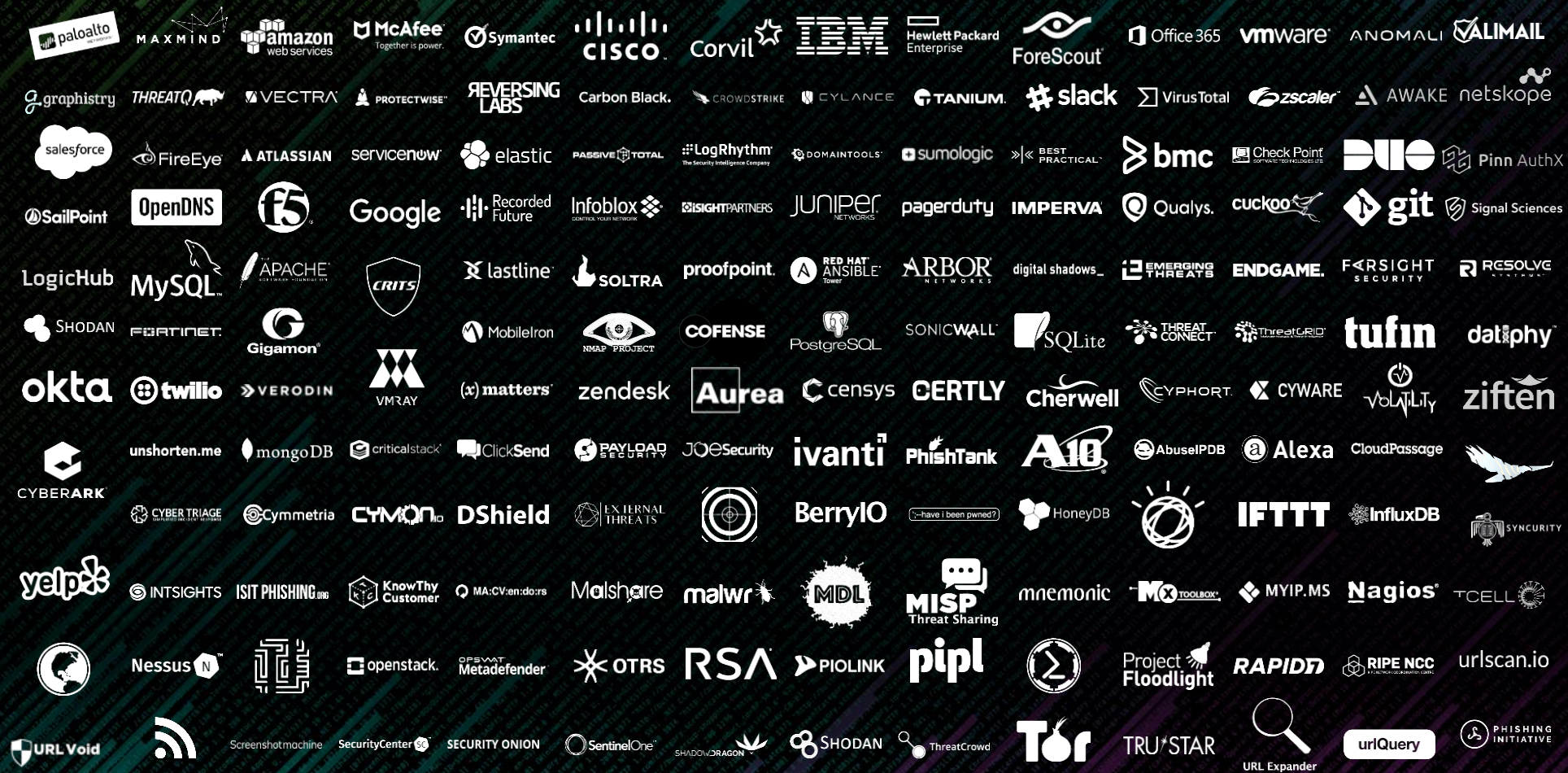


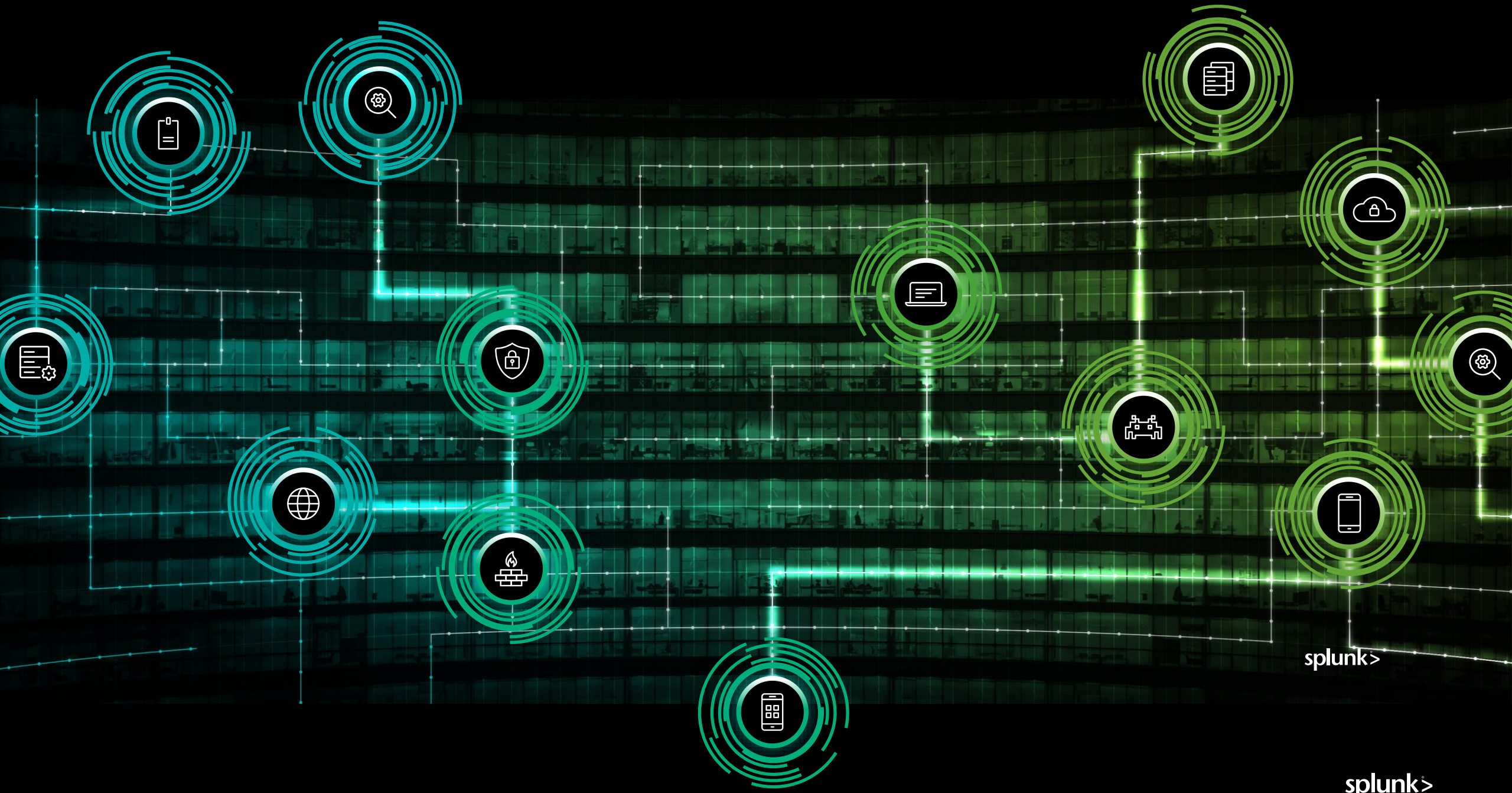
- **Advance cyber defense**, reduce risk using an analytics-driven approach
- **Respond faster** by accelerating incident response
- **Work smarter** and reduce staffing and skills challenges

splunk>

splunk>

Adaptive Operations Framework




splunk>
splunk>

Market Trends

Security Strategy Reliant on Data Strategy

Demand For Automation to Optimize Security Operations

Desire For Greater Collaboration

Compliance as a More Critical Driver

Cloud Enables Shared Intelligence

splunk>

OLIVER FRIEDRICHS

VP, Security Automation & Orchestration

splunk>

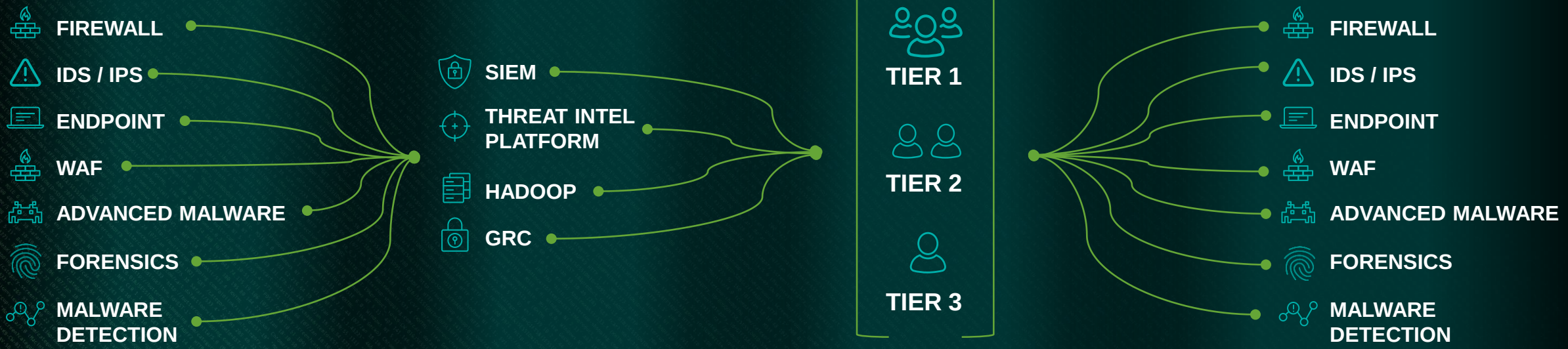
OODA

Observe
Point Products

Orient
Analytics

Decision Making
Automation

Acting
Orchestration



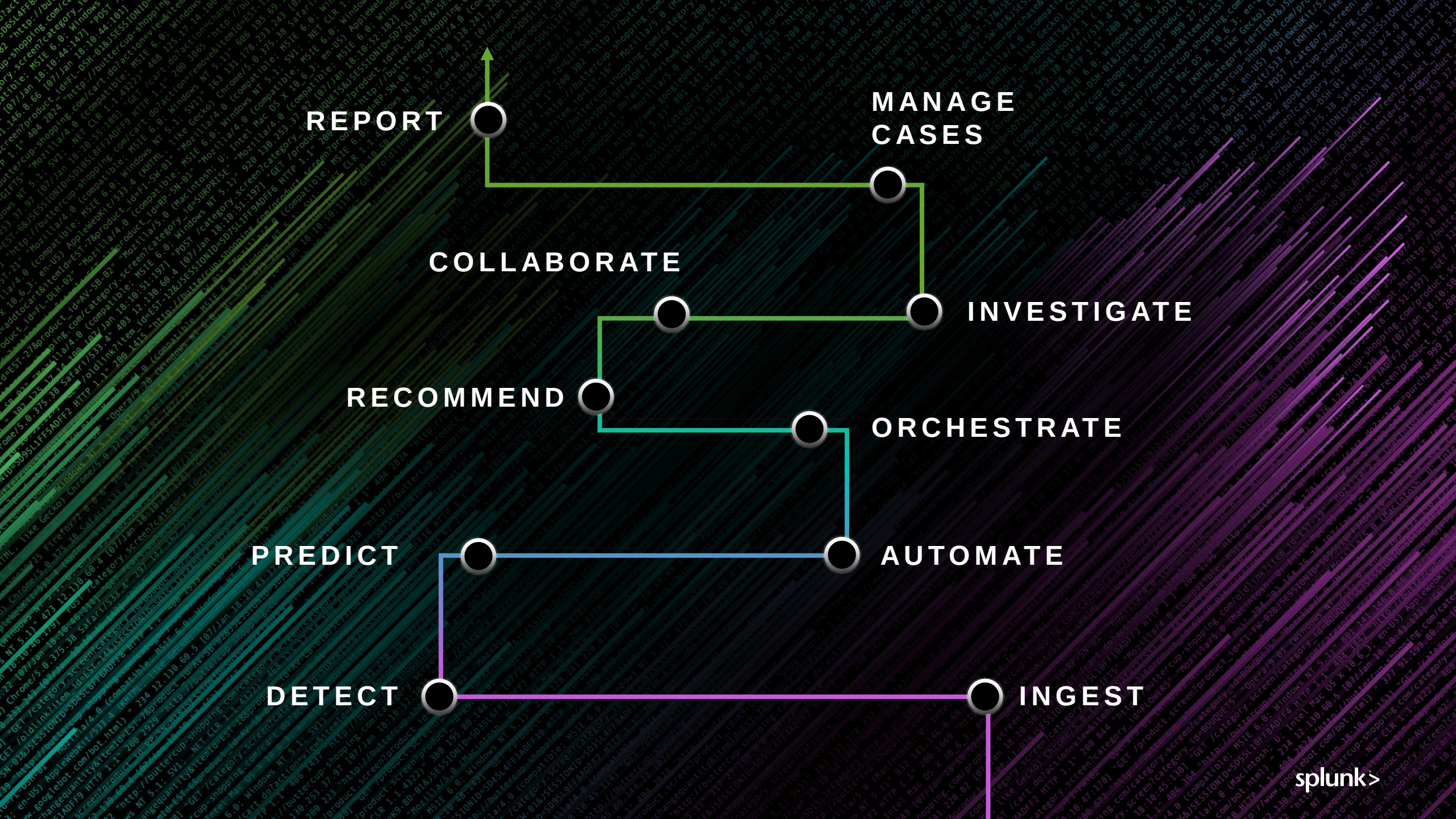
splunk>

Today's SOC

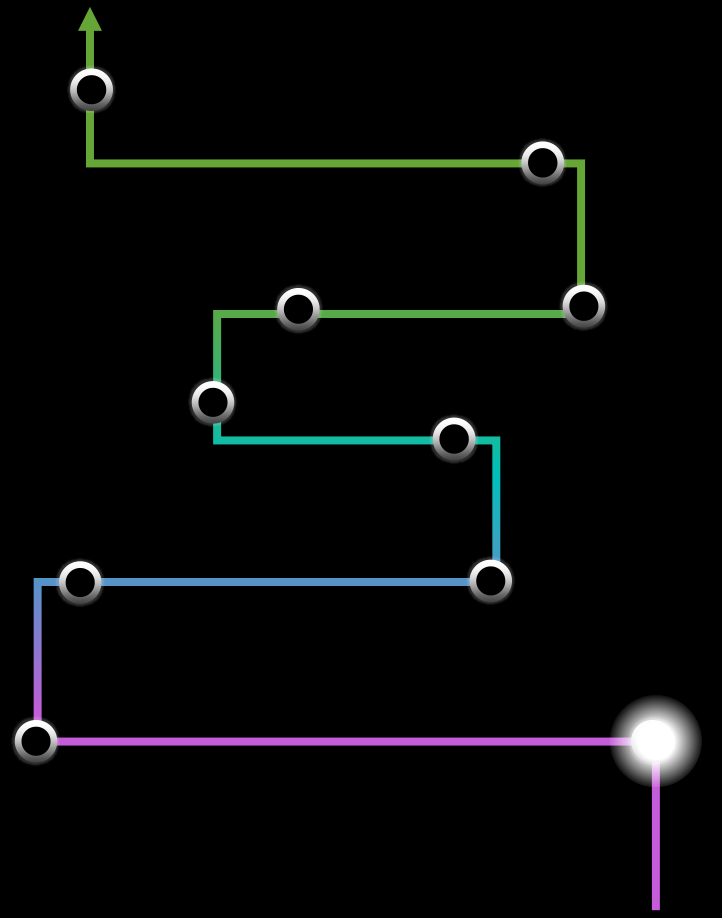
OPERATIONS TODAY vs OPERATIONS IN 2020

Re-imagine the SOC

splunk>

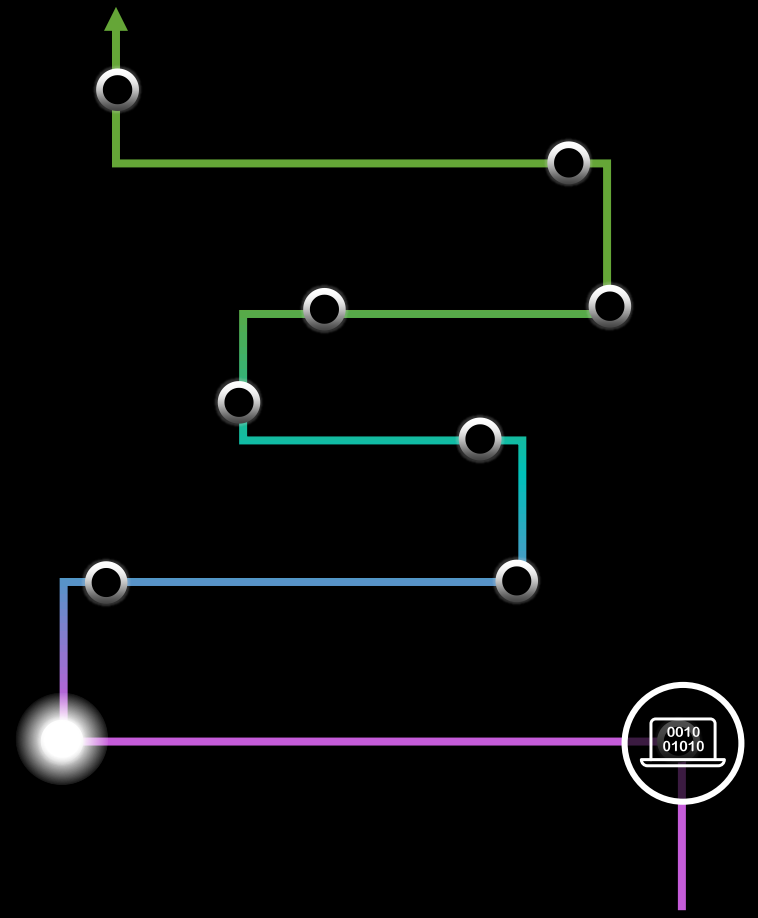

REPORT
MANAGE CASES
COLLABORATE
INVESTIGATE
RECOMMEND
ORCHESTRATE
PREDICT
AUTOMATE
DETECT
INGEST

INGEST



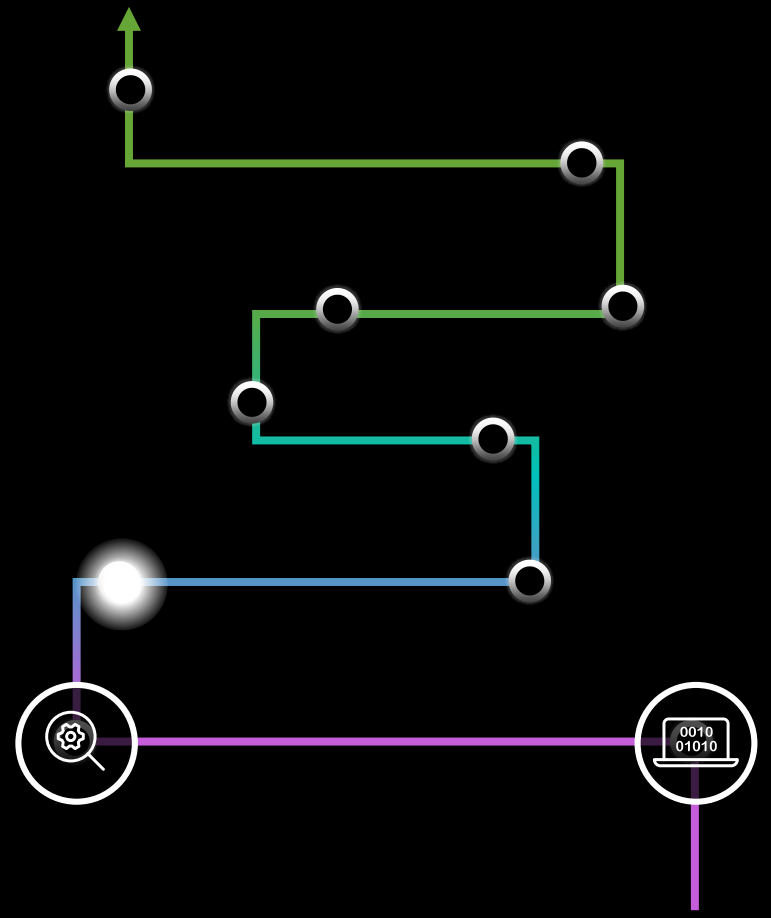
splunk>

DETECT



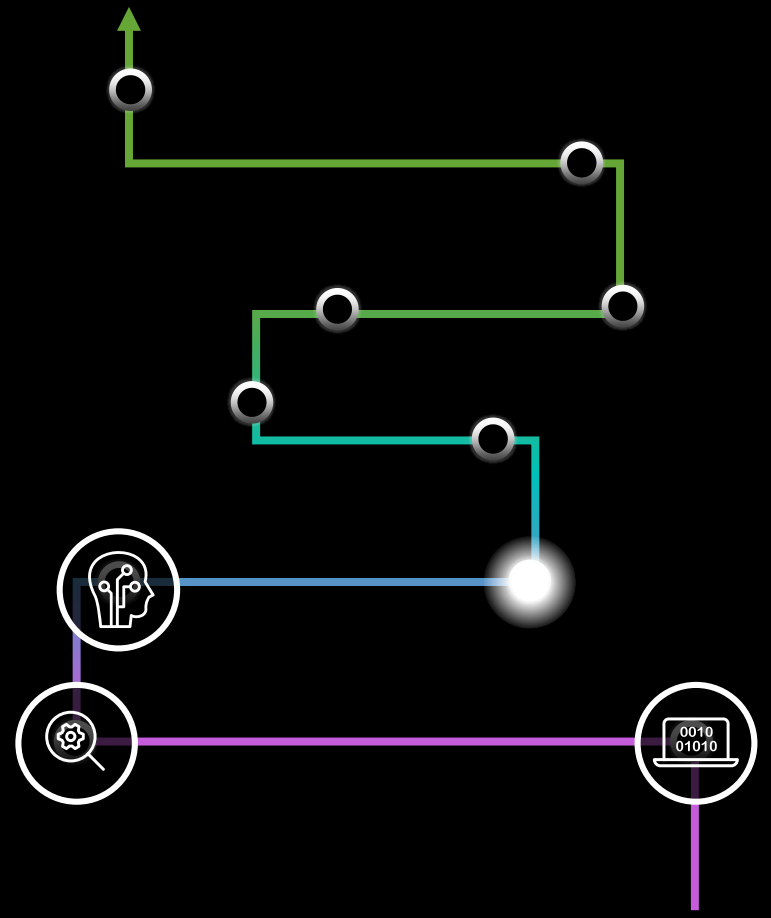
splunk>

PREDICT



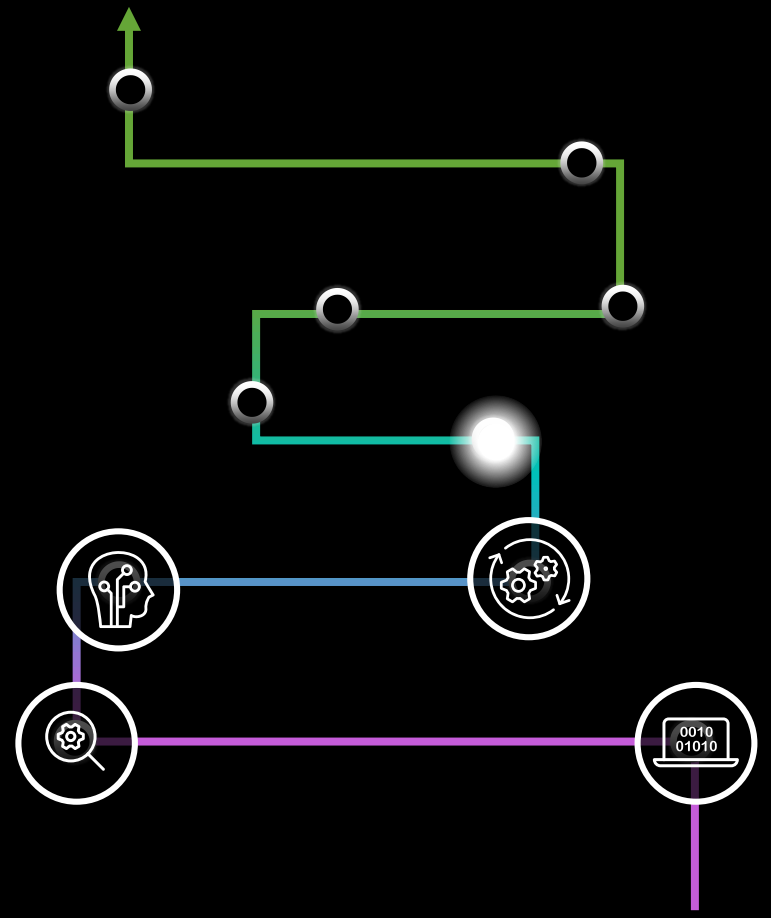
splunk>

AUTOMATE



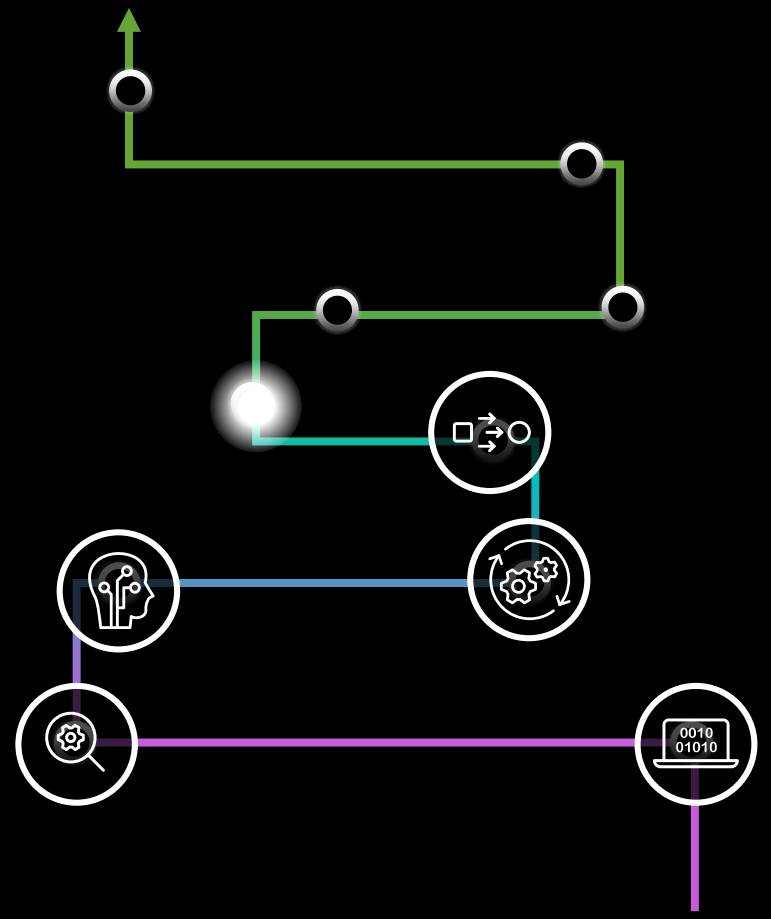
splunk>

ORCHESTRATE



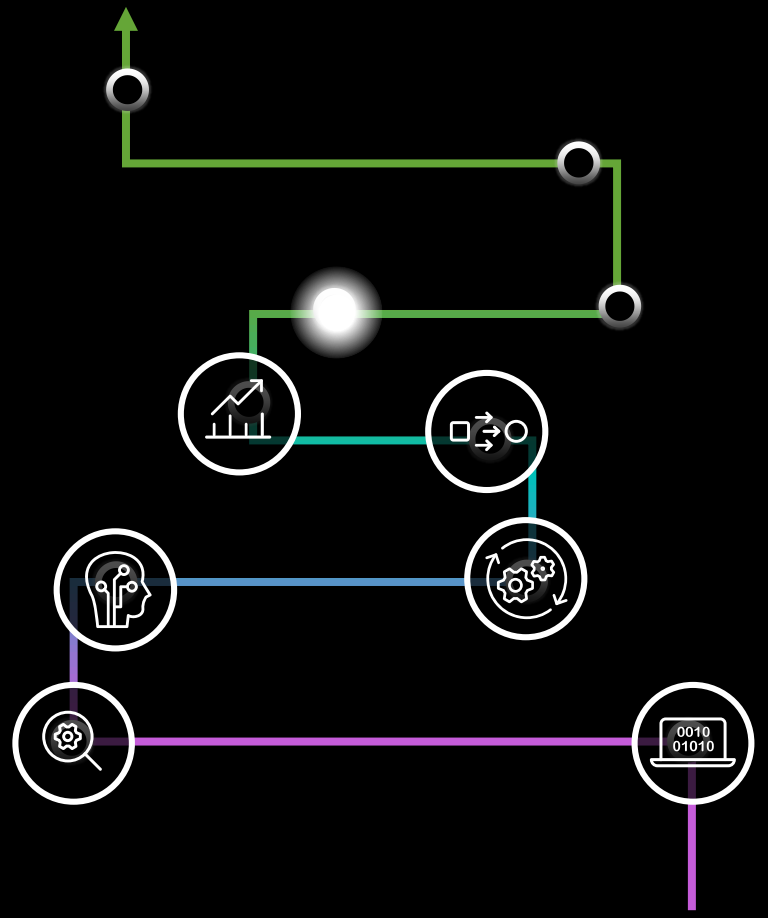
splunk>

RECOMMEND



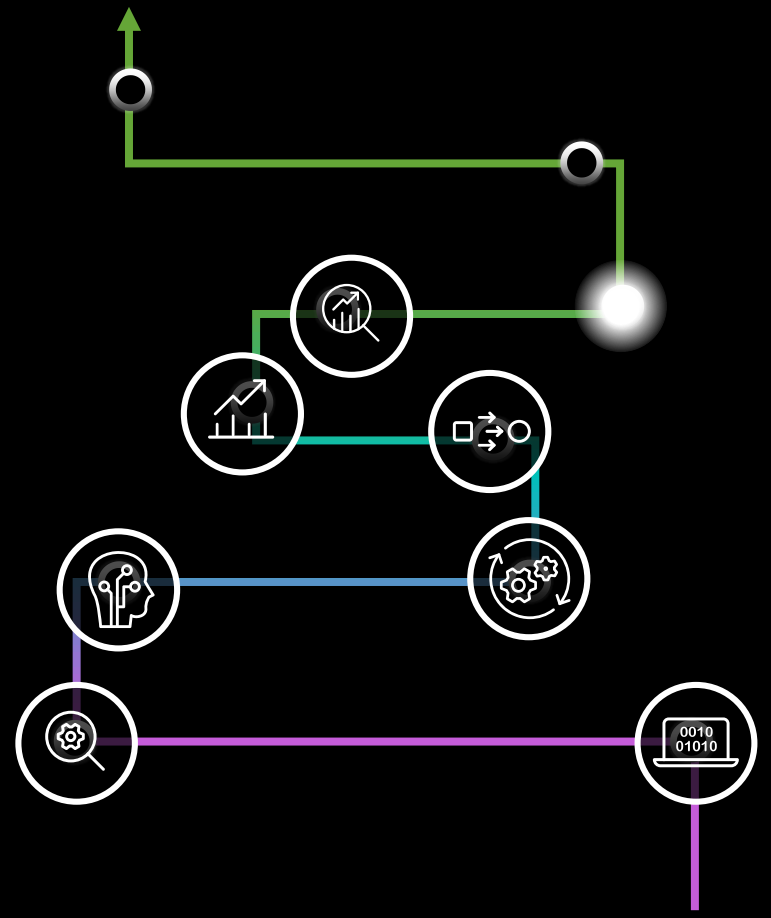
splunk>

INVESTIGATE



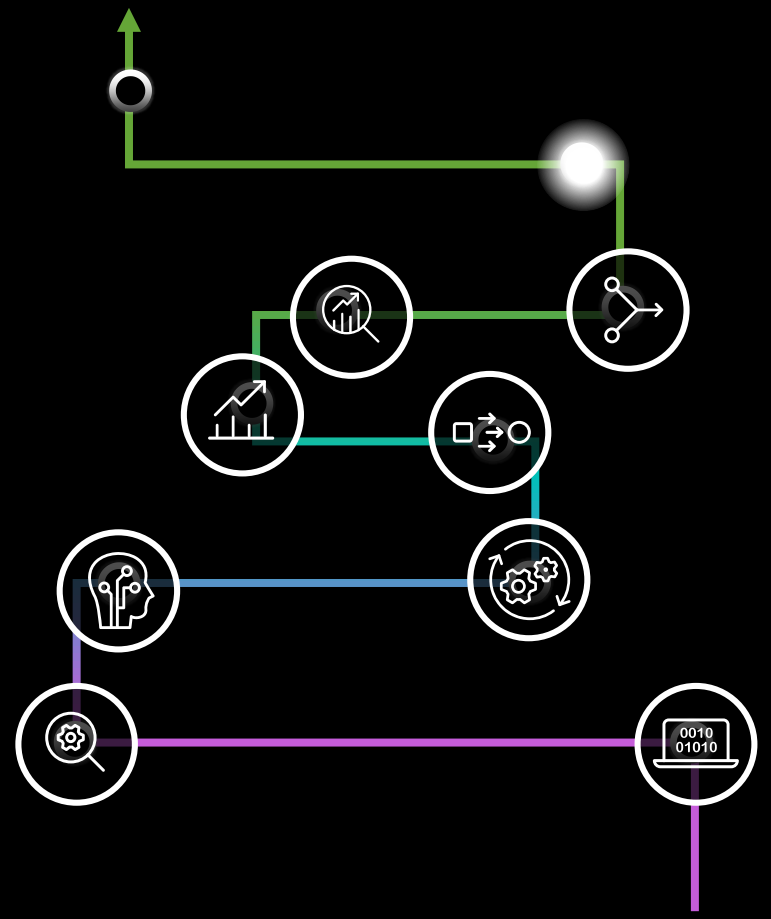
splunk>

COLLABORATE



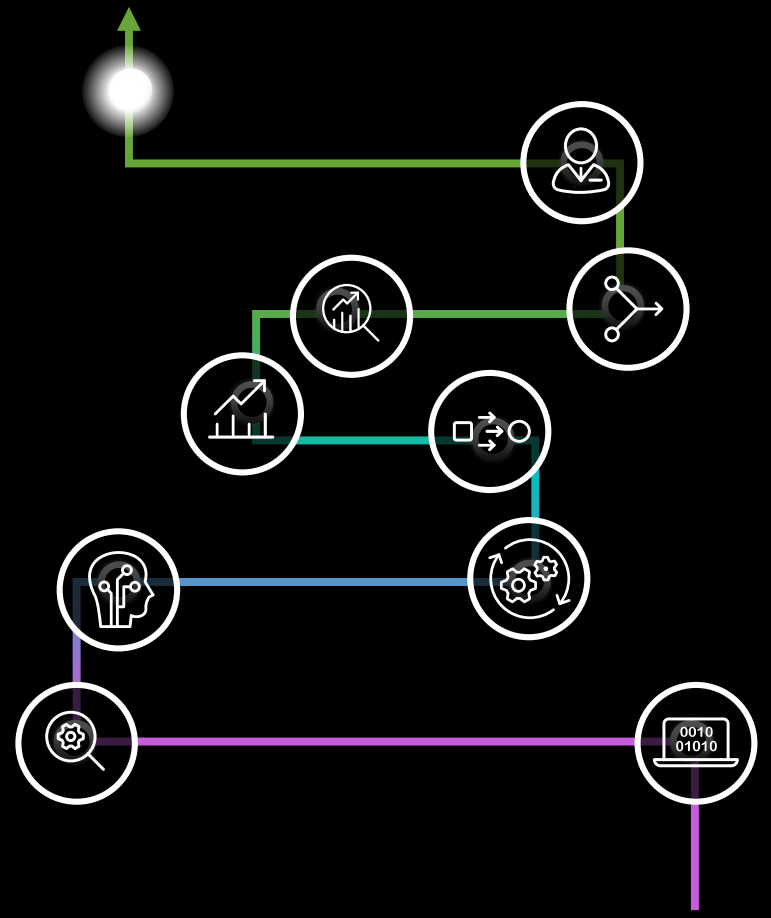
splunk>

MANAGE CASES

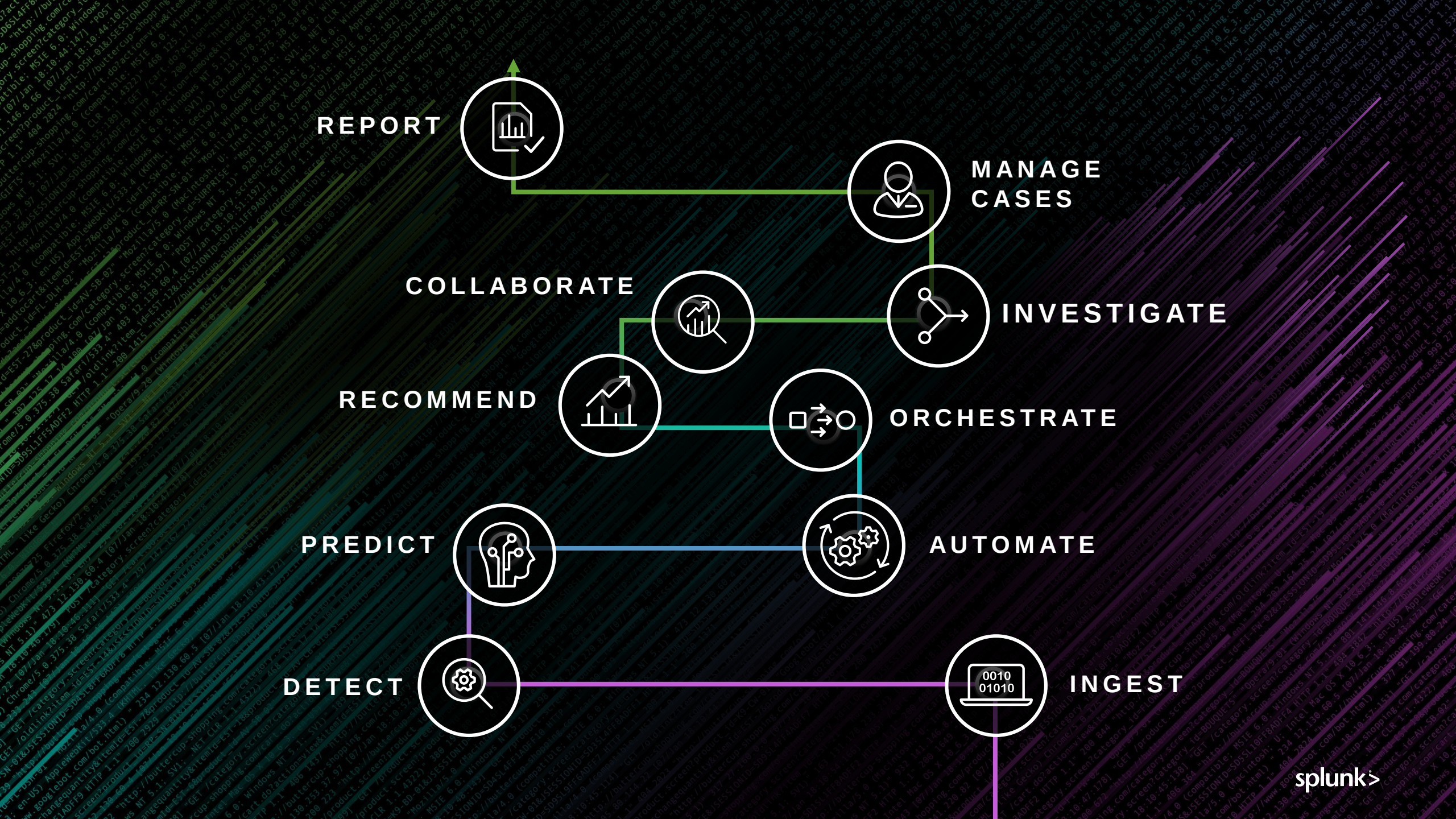


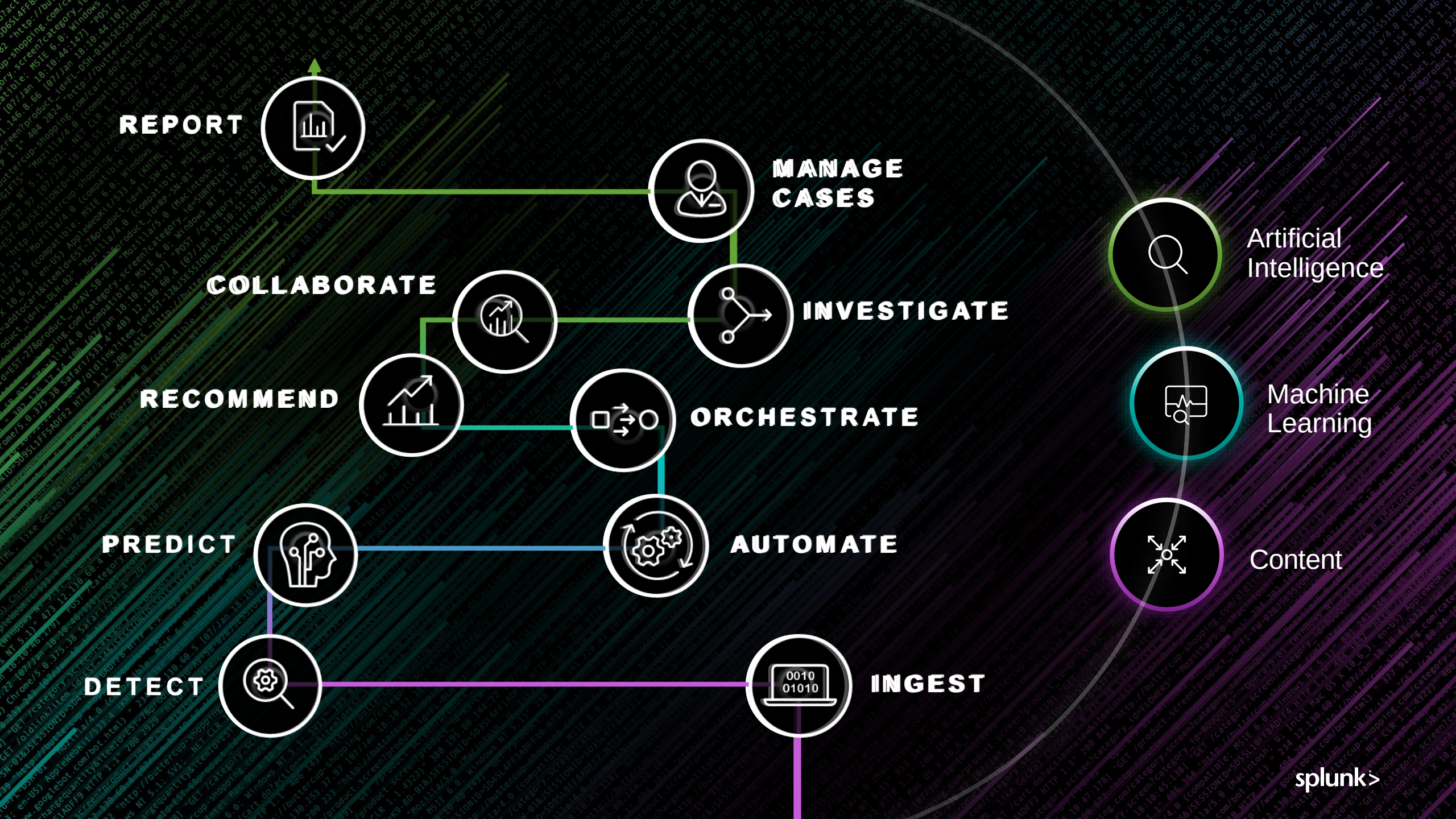
splunk>

REPORT



splunk>

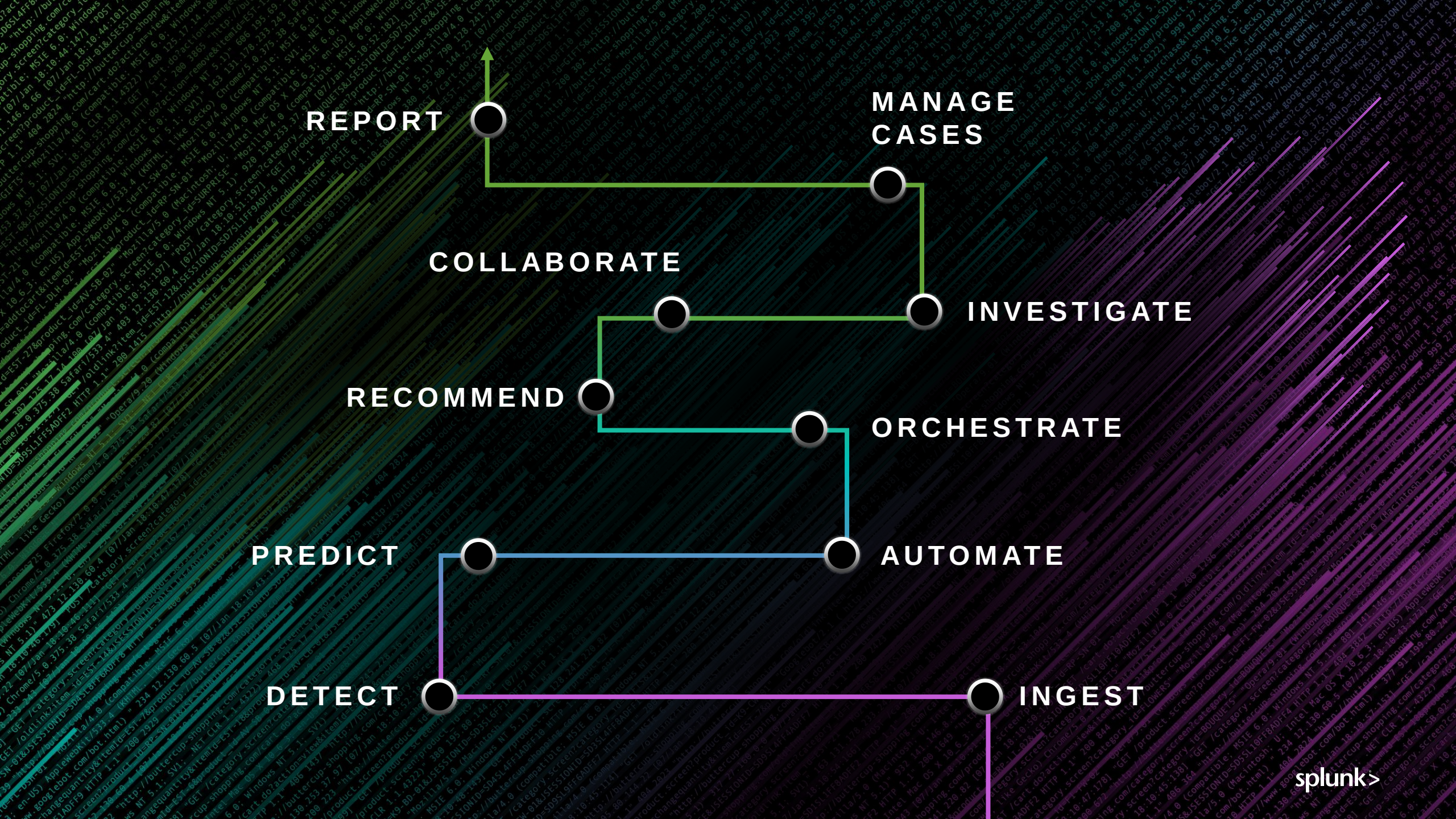

REPORT
MANAGE CASES
COLLABORATE
INVESTIGATE
RECOMMEND
ORCHESTRATE
PREDICT
AUTOMATE
DETECT
INGEST
0010
01010


REPORT
MANAGE CASES
COLLABORATE
INVESTIGATE
RECOMMEND
ORCHESTRATE
PREDICT
AUTOMATE
DETECT
0010
01010
INGEST
Artificial Intelligence
Machine Learning
Content
splunk>

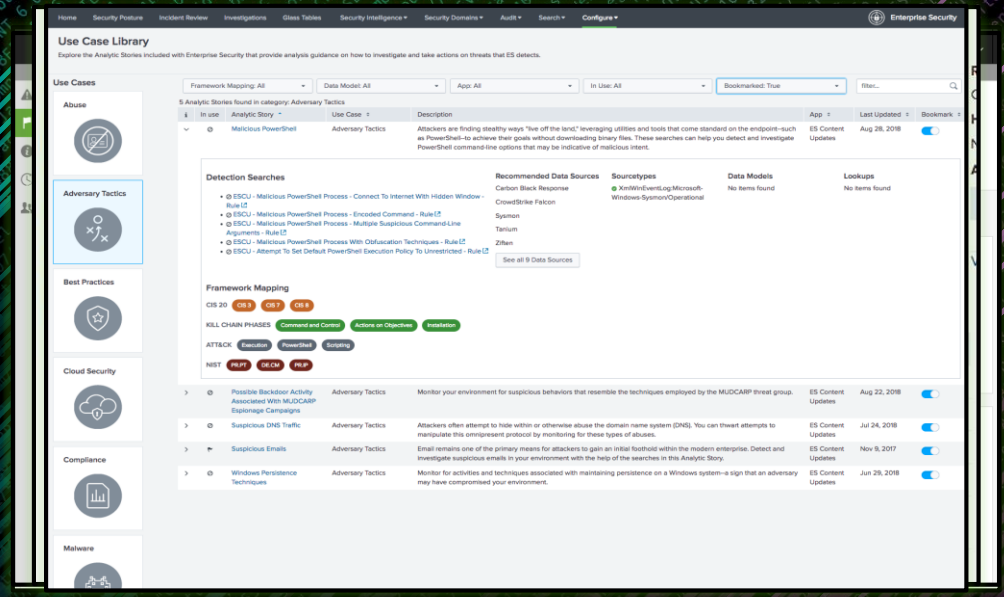
KARTHIK KANNAN

Head, Security Analytics

splunk>


REPORT
MANAGE CASES
COLLABORATE
INVESTIGATE
RECOMMEND
ORCHESTRATE
PREDICT
AUTOMATE
DETECT
INGEST

Tomorrow's SOC Starts Today



ES & UBA

- Built-in Detection Techniques
- ML-led Behavioral Detection
- Entity Risk Scoring
- Event Sequencing
- Content: Use Case Library

splunk>

Lateral Movement

Unusual Event Anomalies

Scanning & Privilege Escalation

Purpose-built Threat Model

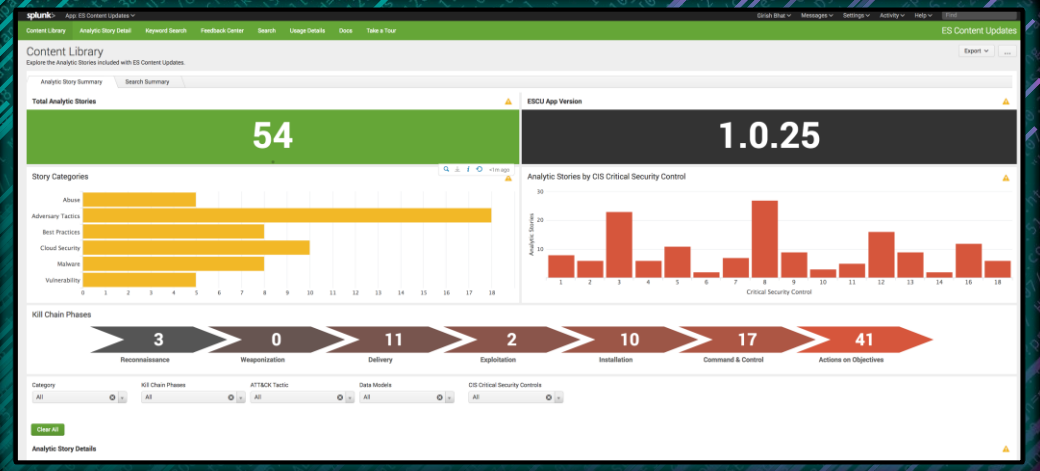
More Analytics, Peer Group Profiles

Device Finger-printing

Endpoints, More Anomalous Behavior

splunk>

Tomorrow's SOC Starts Today

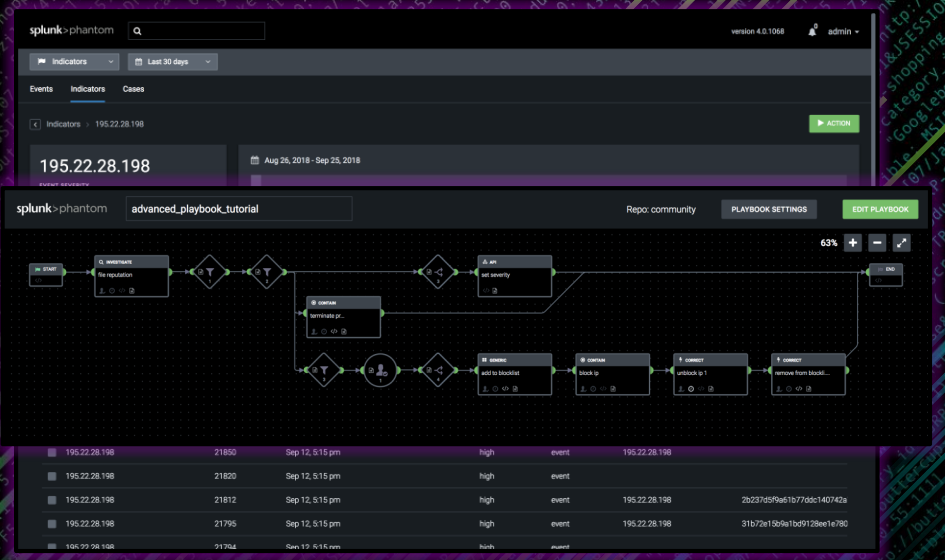


ES

- Ad-hoc Investigations
- Extensive Frameworks
- Investigation Workbench
- Pre-defined Dashboards, Templates

splunk>

Tomorrow's SOC Starts Today



Automation

Orchestration

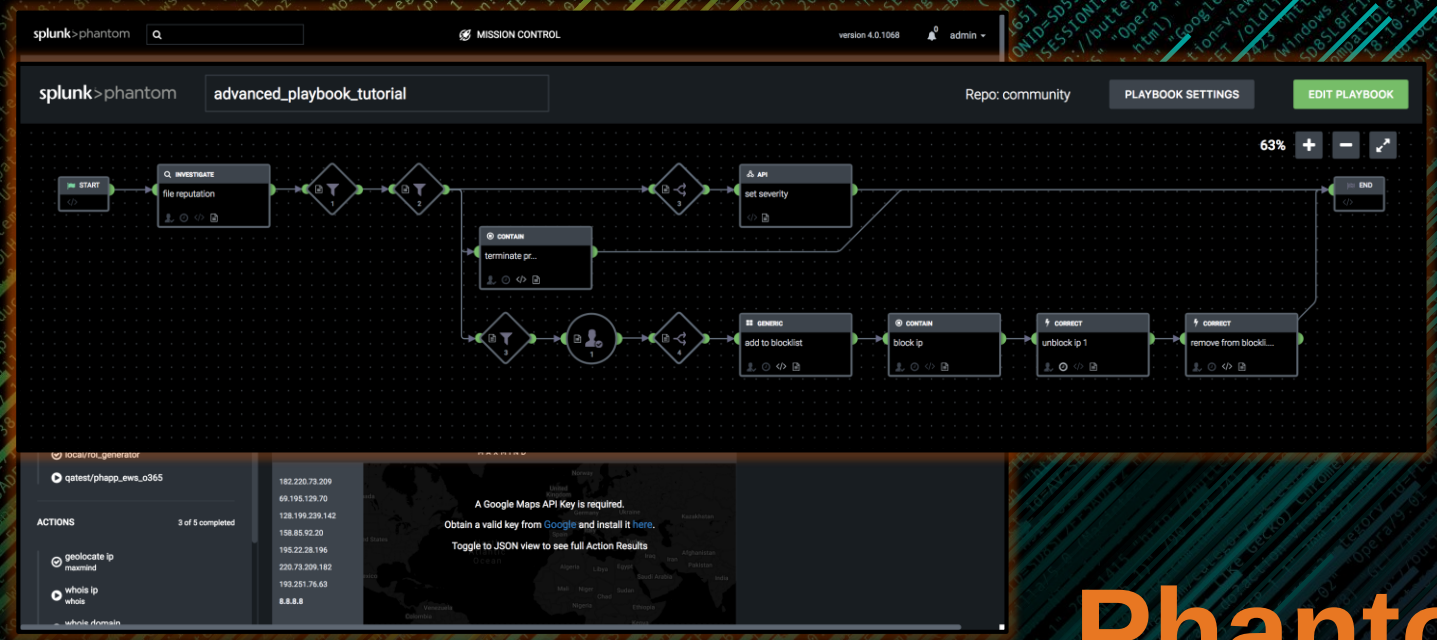
Case Management

Phantom

- Response Identification & Automation
- Indicator View
- Playbooks

splunk>

Tomorrow's SOC Starts Today



Recommendation

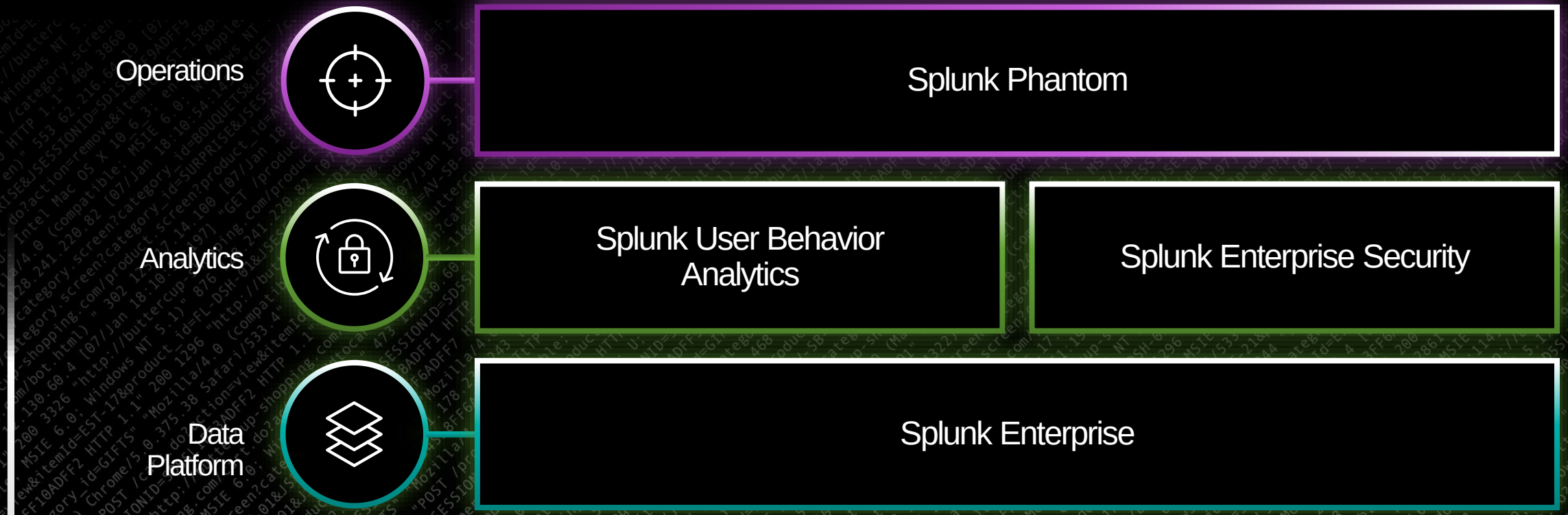
Phantom

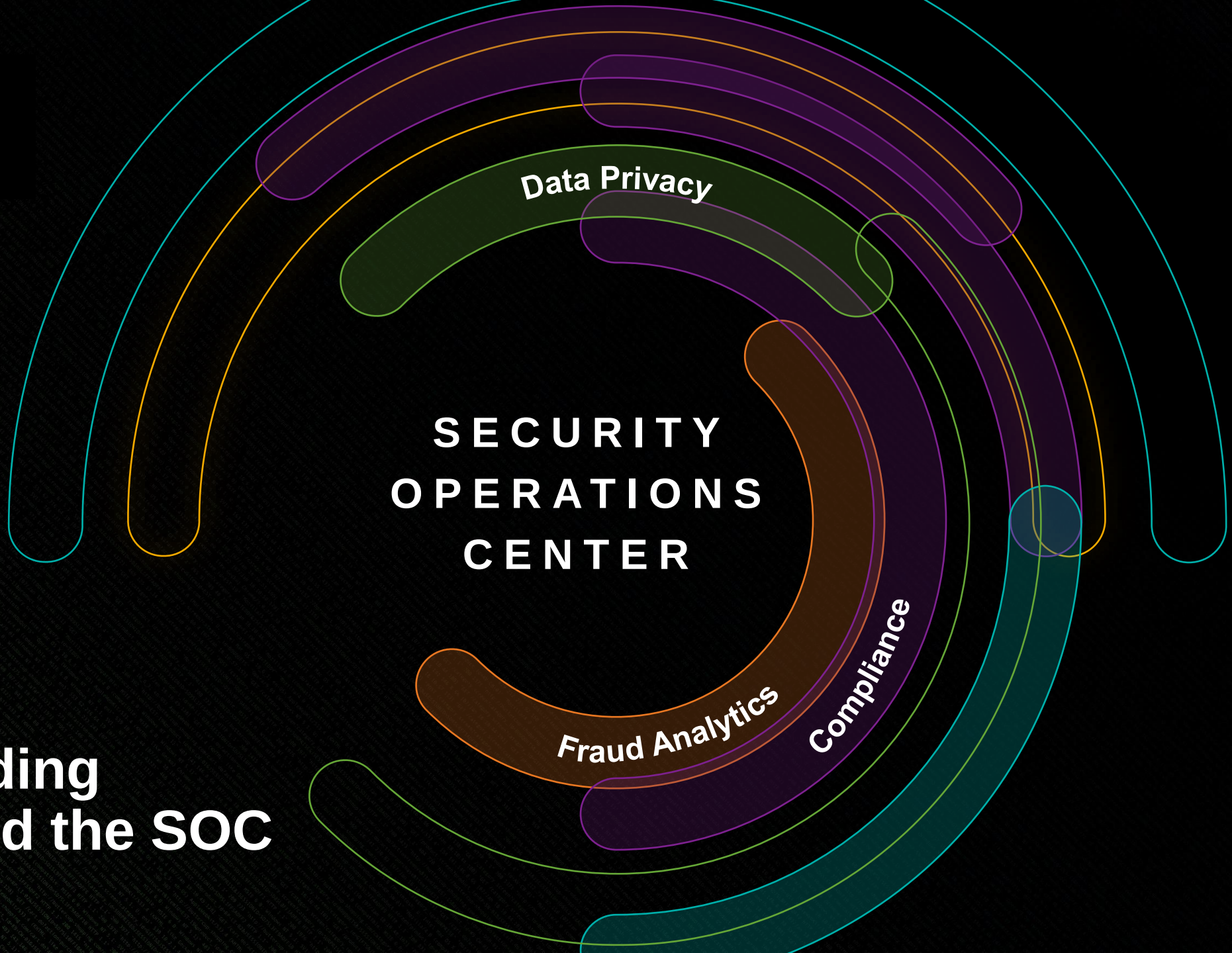
- Mission Guidance
- Playbooks

splunk>


REPORT
MANAGE CASES
COLLABORATE
90%
50%
RECOMMEND
ORCHESTRATE
TIER 1 ANALYST WORK WILL BE AUTOMATED
TIME NOW SPENT TUNING DETECTION AND RESPONSE LOGIC
PREDICT
AUTOMATE
DETECT
INGEST

splunk>


Operations
Splunk Phantom
Analytics
Splunk User Behavior Analytics
Splunk Enterprise Security
Data Platform
Splunk Enterprise



Extending Beyond the SOC

splunk>

splunk>

JENNINGS ASKE

CISO
New York-Presbyterian

NewYork-Presbyterian

splunk>

NewYork-Presbyterian

splunk>

SPLUNK ENTERPRISE
CUSTOMERS

SEC1798
The Great SIEM Migration
Today @ 4:45pm

SEC1272
Incident Response Automation with Splunk Phantom
Tomorrow @ 12:45PM

Ask The Experts
SIEM and SOAR

Demo @ App Showcase
Security & Risk Monitoring
SOC Automation

Splunk Enterprise Security
Splunk Phantom

splunk>

SPLUNK ENTERPRISE SECURITY

CUSTOMERS

SEC1983 | Splunk UBA
Methods and Best Practices to Get Started Now
Thursday @ 12:15PM

SEC1272
Incident Response Automation with Splunk Phantom
Tomorrow @ 12:45PM

Ask The Experts

UBA and SOAR

Demo @ App Showcase

Insider + Advanced Threat Detection

SOC Automation

Splunk User Behavior Analytics

Splunk Phantom

splunk>

SPLUNK PHANTOM CUSTOMERS

SEC1798
The Great SIEM Migration
Today @ 4:45pm

SEC1983 | Splunk UBA
Methods and Best Practices to Get Started Now
Thursday @ 12:15PM

Ask The Experts
SIEM and UBA

Demo @ App Showcase
Security & Risk Monitoring
Insider + Advanced Threat Detection

Splunk Enterprise Security

Splunk User Behavior Analytics

splunk>

SPLUNK ENTERPRISE
SPLUNK ES
SPLUNK UBA
SPLUNK PHANTOM

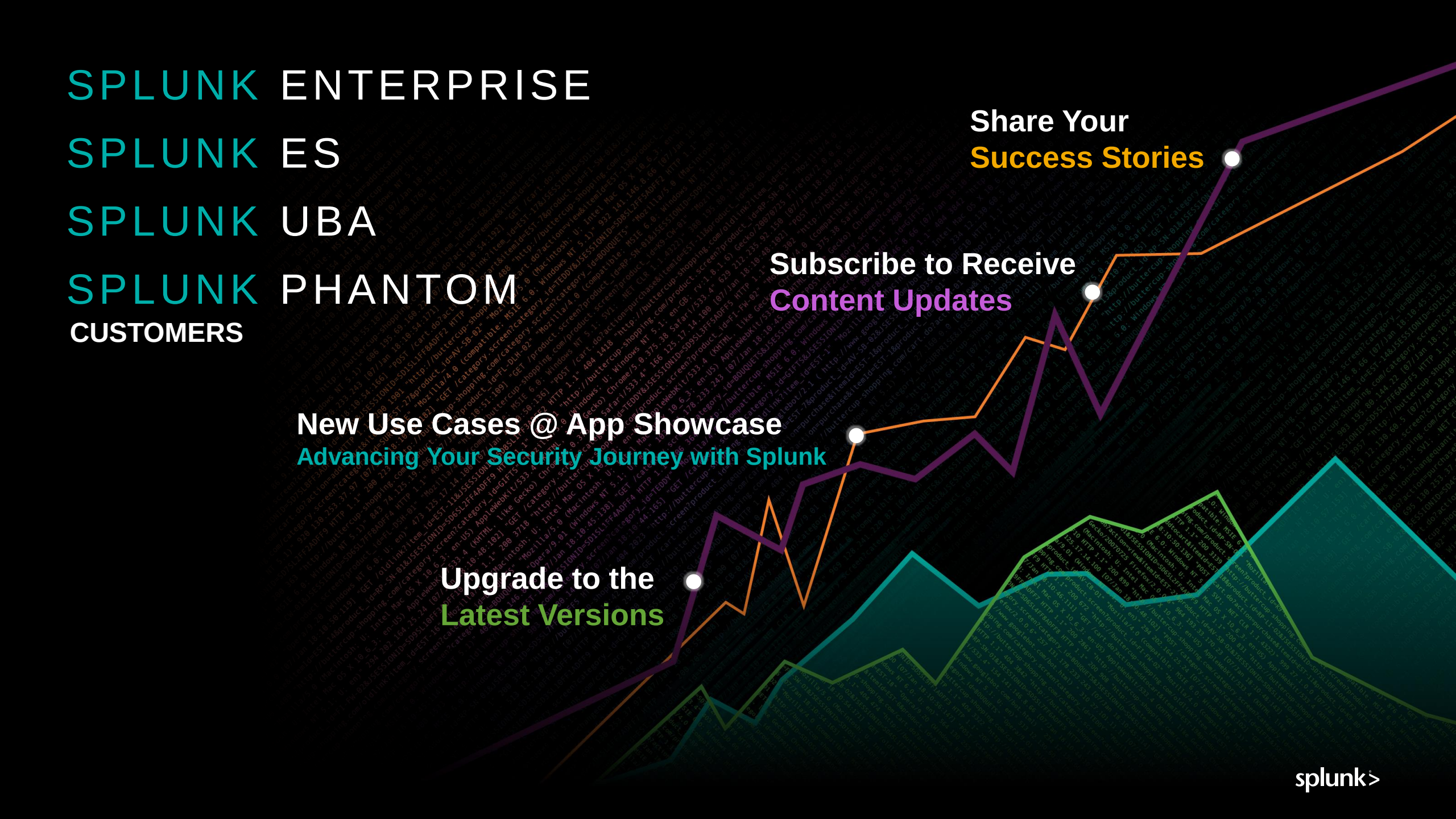
CUSTOMERS

Share Your
Success Stories

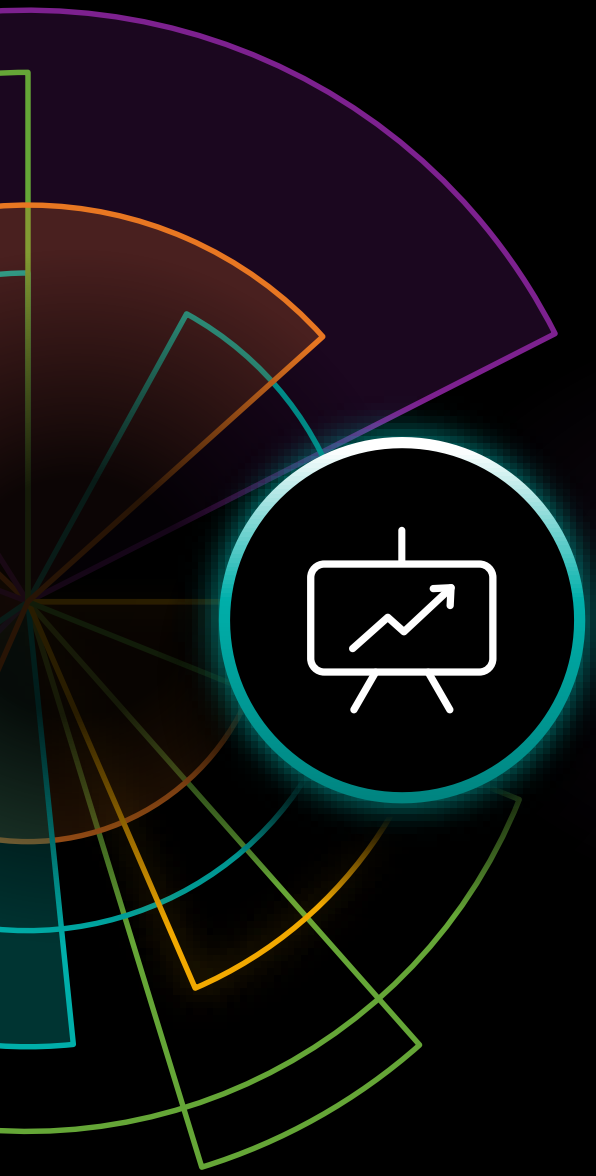
Subscribe to Receive
Content Updates

New Use Cases @ App Showcase
Advancing Your Security Journey with Splunk

Upgrade to the
Latest Versions



splunk>



LEARN MORE

80+
Security Breakout and Theater Sessions

3
BOTS-related Hands-on Sessions

4
New Security Projects @ Innovation Labs

1
Phantom Playbook Hackathon

splunk>

Customer First.

Technology Forward.

Solution Centric.

splunk>


.conf18
splunk>
BOSS
of the SOC

3RD

1ST

GODS OF OR

splunk>

Thank You

splunk>