



.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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

# HAIYAN SONG

**SVP & General Manager,  
Security Markets**



splunk>



1

## SPLUNK FOR SECURITY TODAY

## WHAT'S NEXT

2

## PAVING THE PATH FOR TOMORROW

splunk>



End-to-end  
Portfolio

Delivering  
Greater Value

Scaling  
With You

Powering Unlimited  
Possibilities

Technology  
Forward

Extending Our  
Ecosystem

**30+**

Content Updates  
released

**24k**

Downloads of  
Splunk Security  
Essentials

**1.2k**

APIs integrations  
with Phantom

**6k**

Contestants have  
played BOTS

# Splunk for Security

ML and UBA  
(Caspida)

**Jul 2015**

Splunk Security  
Essentials  
**Jan 2017**

Adaptive Response  
Initiative

**Oct 2016**

Enterprise Security  
Content Updates  
(ESCU)  
**Sep 2017**

User Behavior  
Analytics SDK  
**Oct 2017**

Security Orchestration,  
Automation &  
Response (Phantom)

**April 2018**

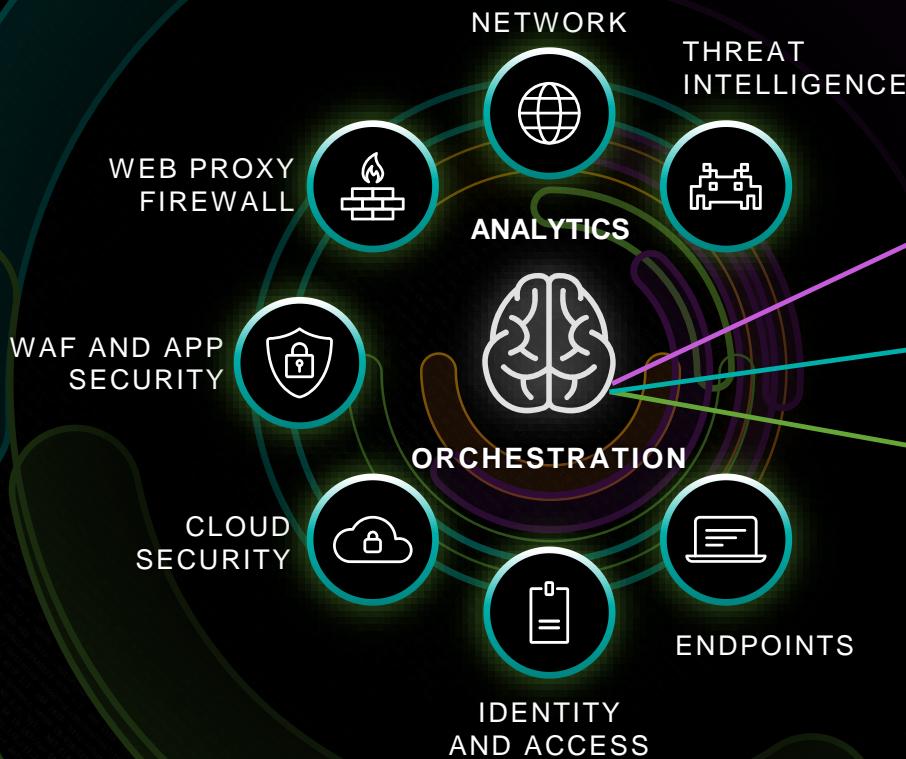
Investigation  
Workbench  
**Feb 2018**

SOC Portfolio  
**Sep 2018**

# Security Nerve Center



# SOARing High with Phantom Buy



Operations

Analytics

Data

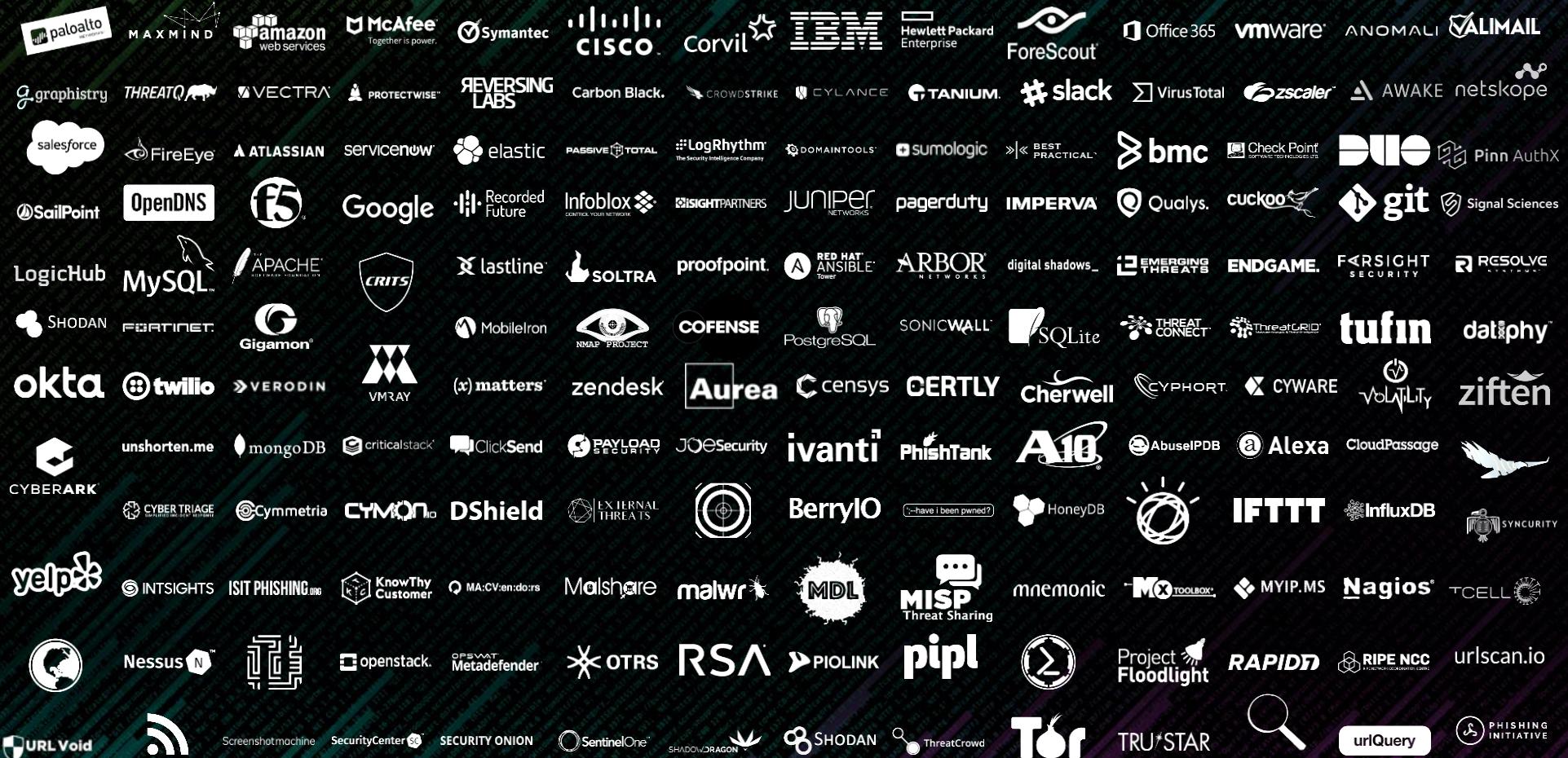
- **Advance cyber defense**, reduce risk using an analytics-driven approach
- **Respond faster** by accelerating incident response
- **Work smarter** and reduce staffing and skills challenges



TM

splunk&gt;

# 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>

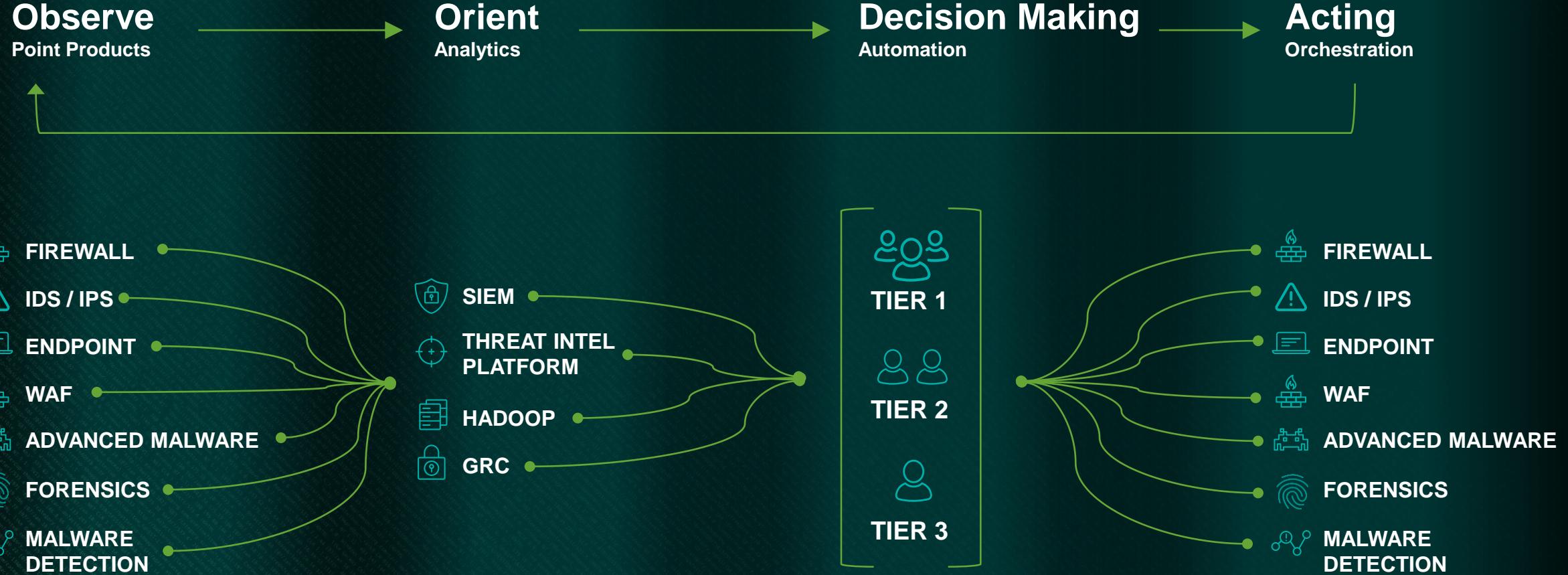
# OLIVER FRIEDRICH

VP, Security Automation  
& Orchestration



splunk>

# OODA



# Today's SOC



OPERATIONS TODAY vs OPERATIONS IN 2020

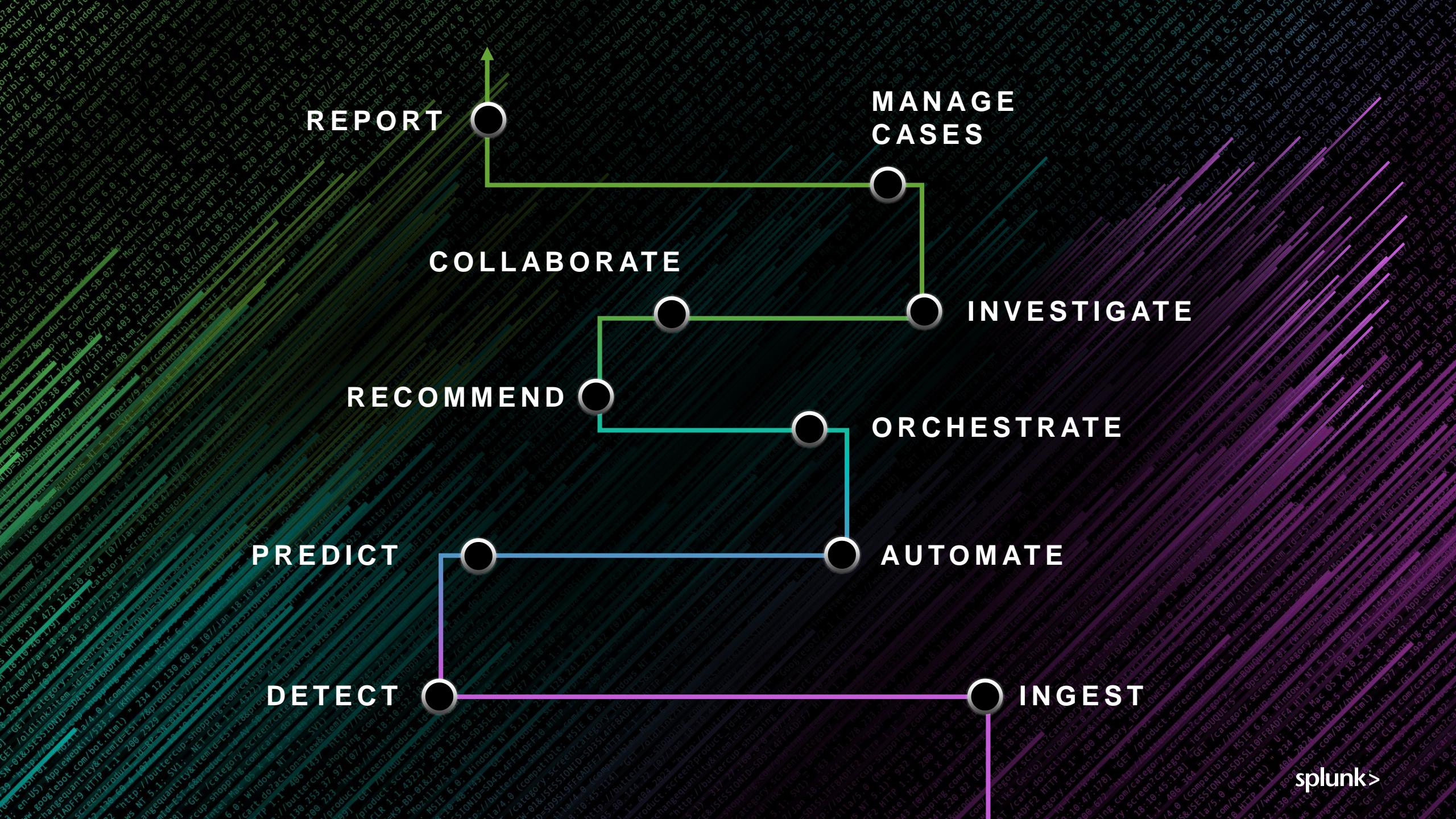
# Re-imagine the SOC

90% OPERATIONS IN 2020

TIER 1 ANALYST WORK  
WILL BE AUTOMATED

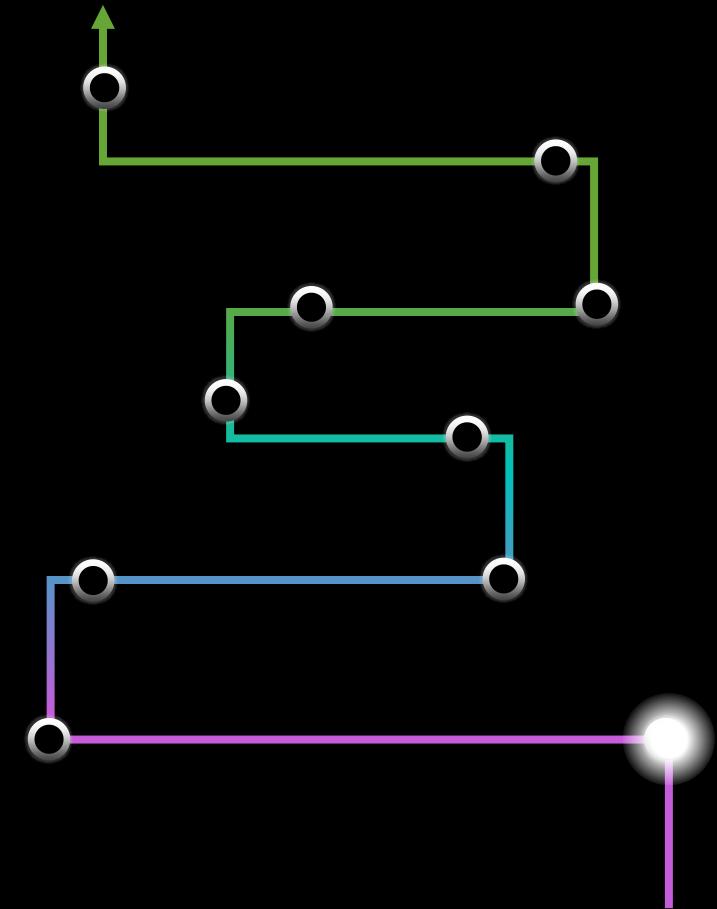
TIME NOW SPENT  
TUNING DETECTION AND  
RESPONSE LOGIC

1  
2020  
PLATFORM TO  
ORCHESTRATE THEM ALL



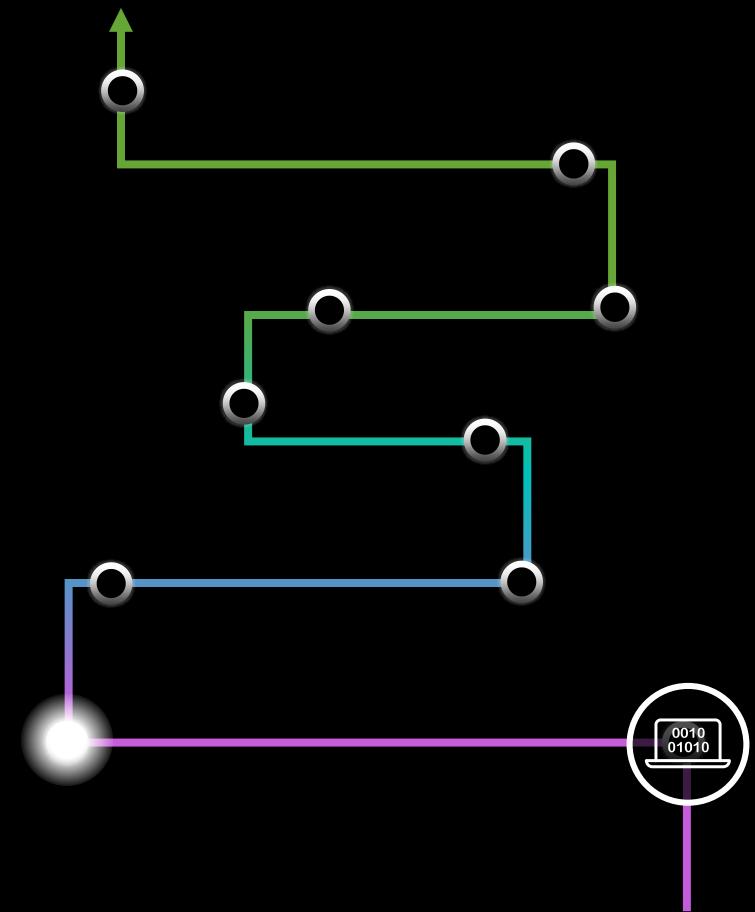


# INGEST



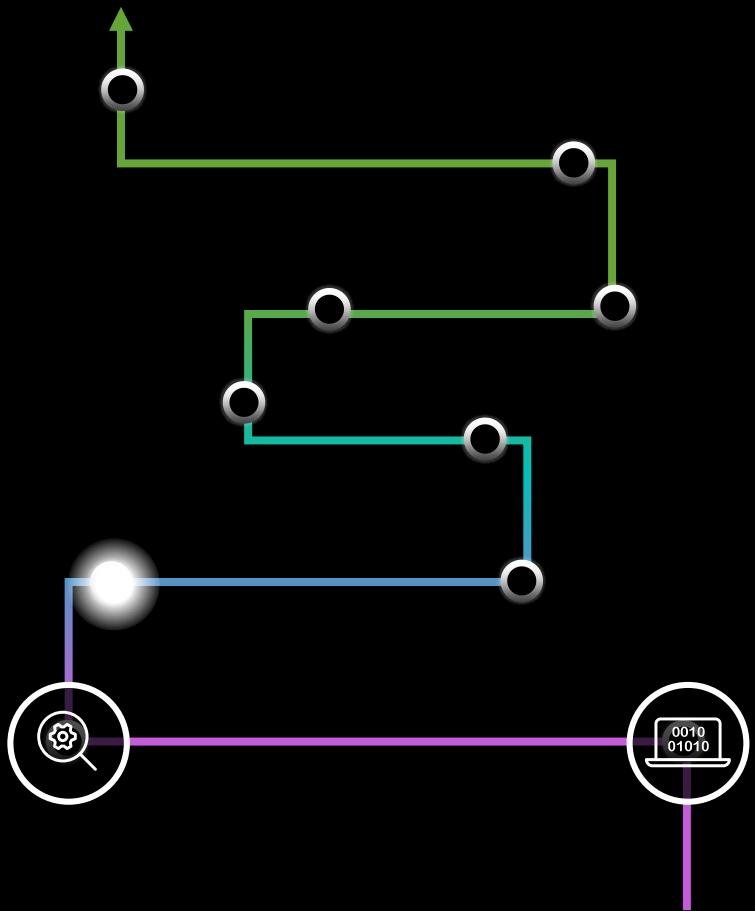


# DETECT



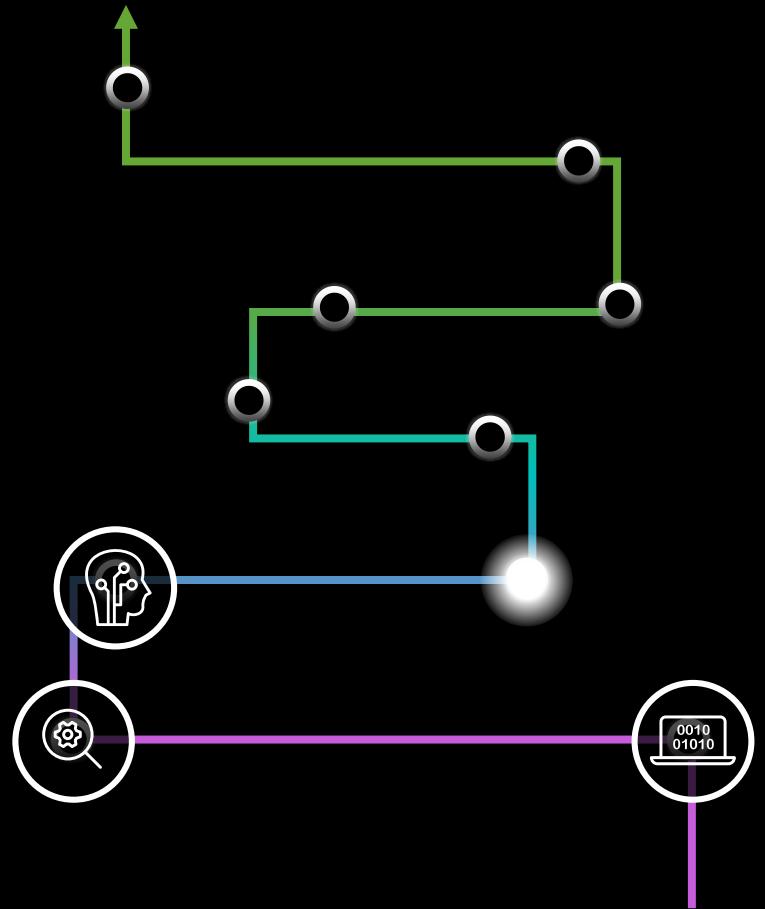


# PREDICT



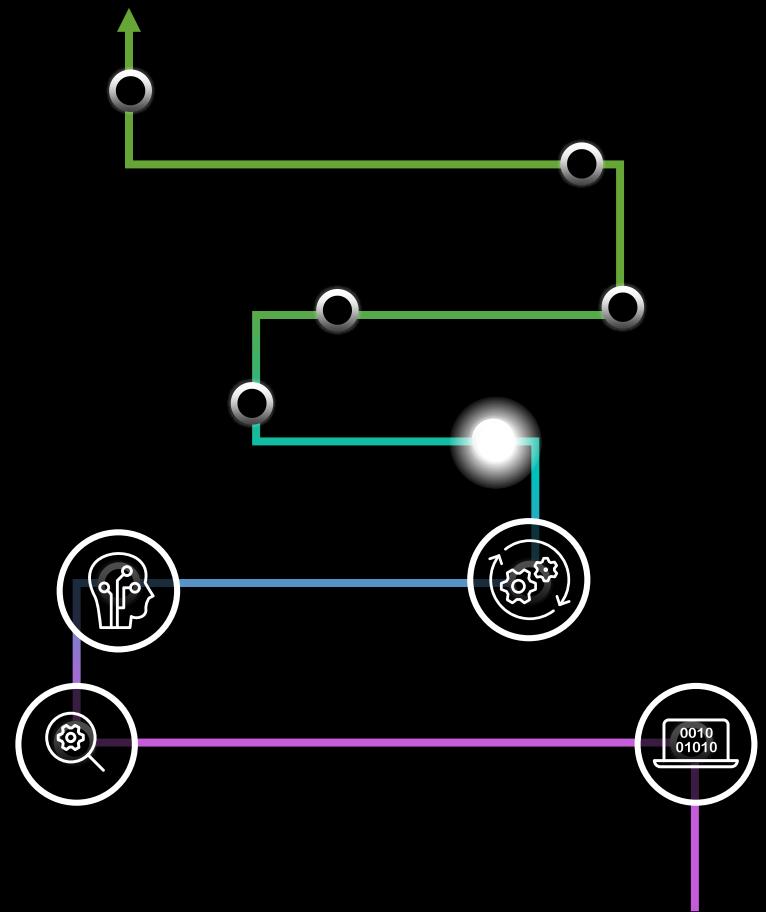


# AUTOMATE



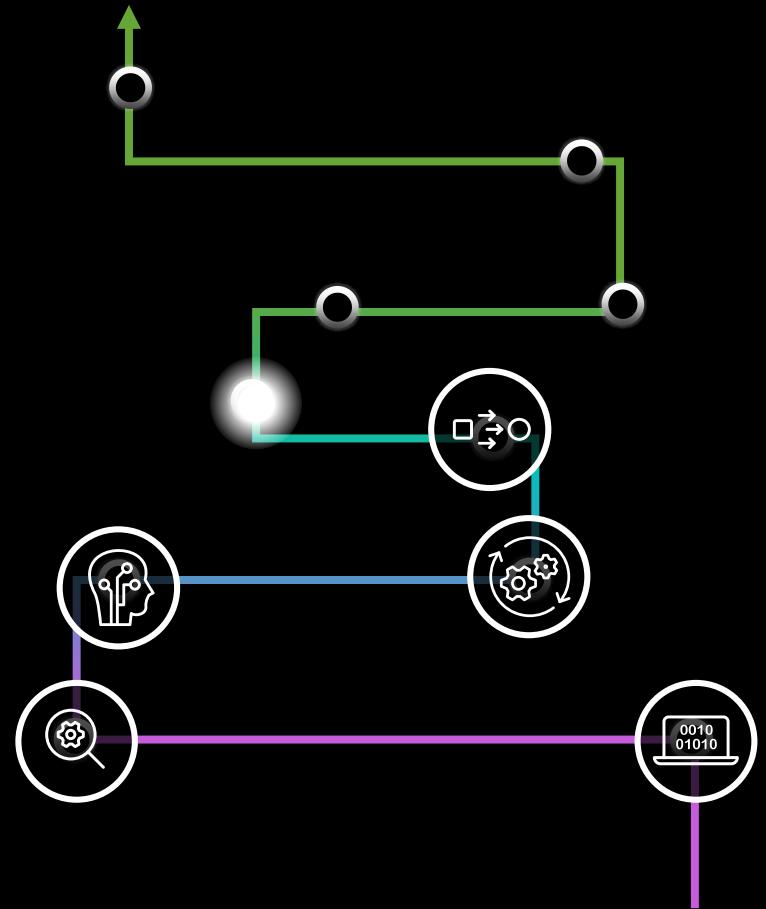


# ORCHESTRATE



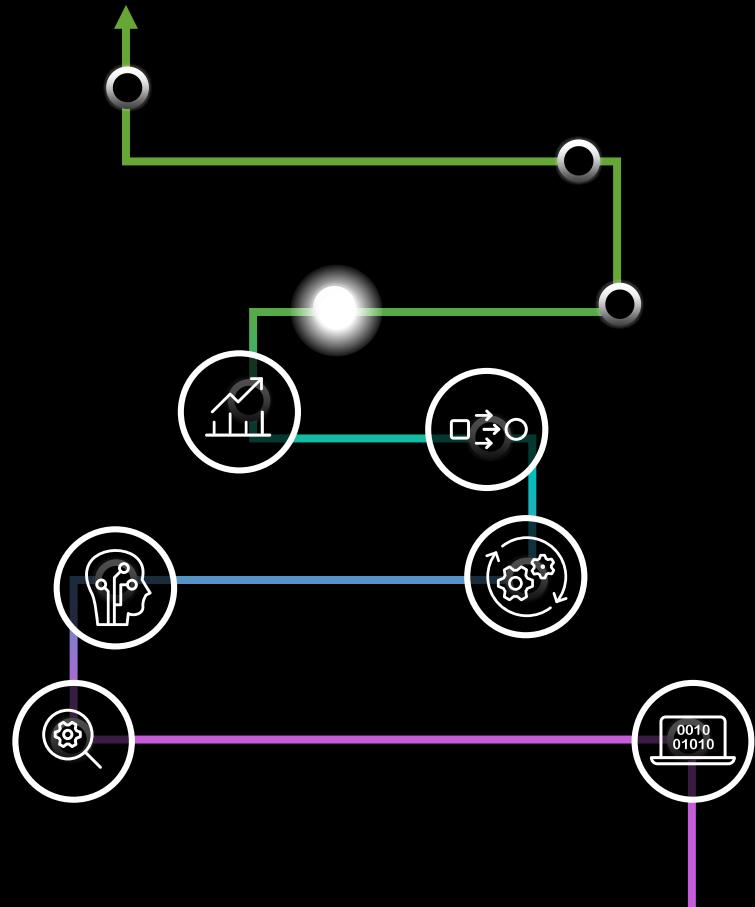


# RECOMMEND



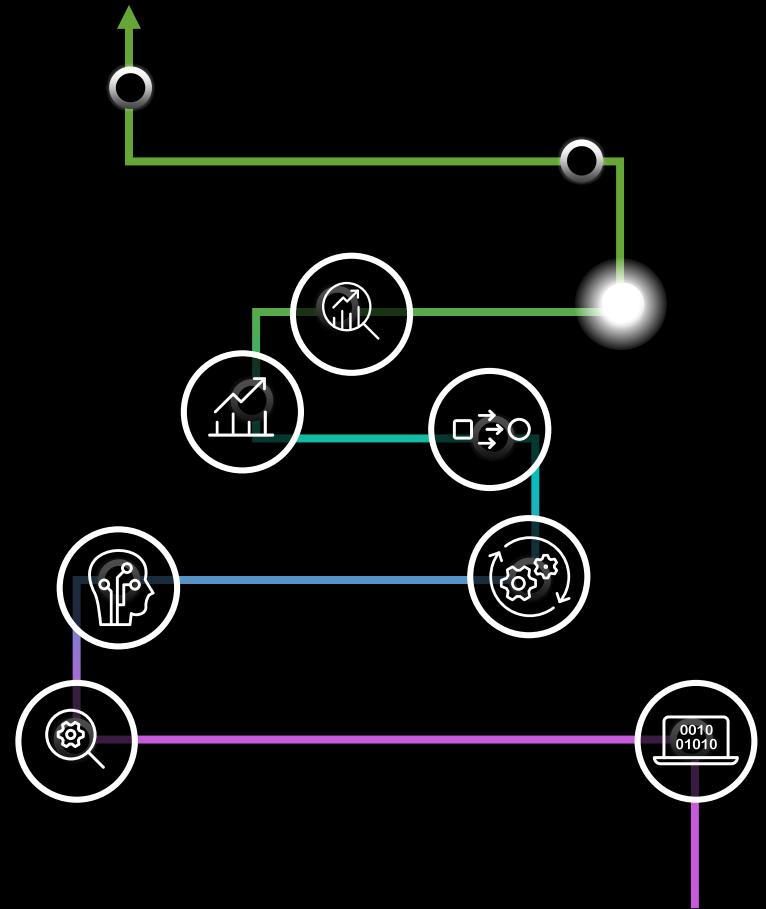


# INVESTIGATE



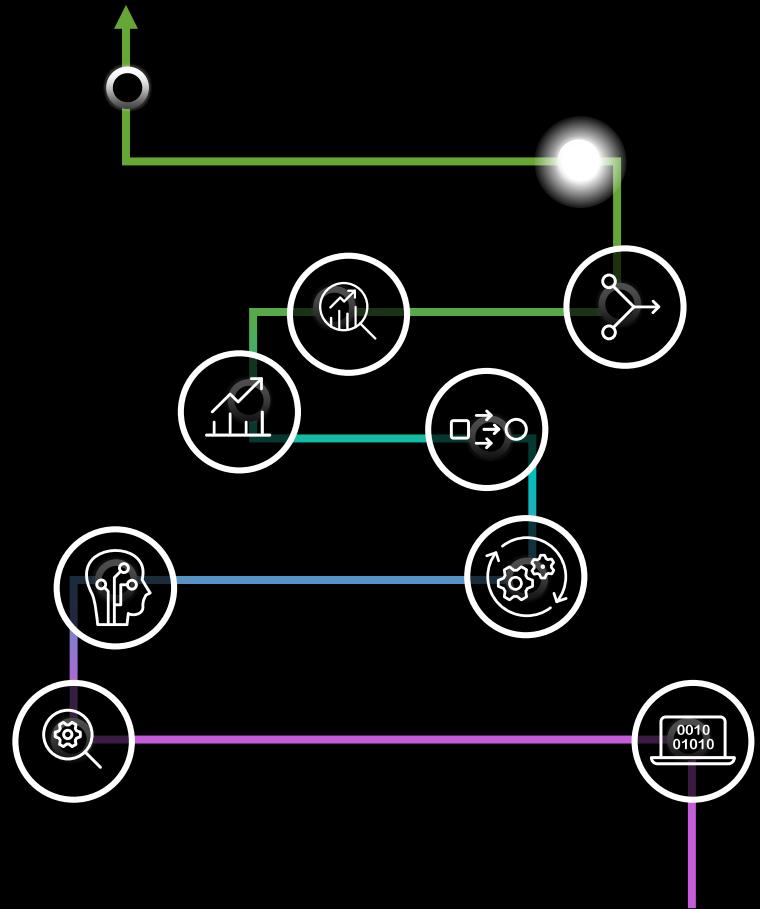


# COLLABORATE



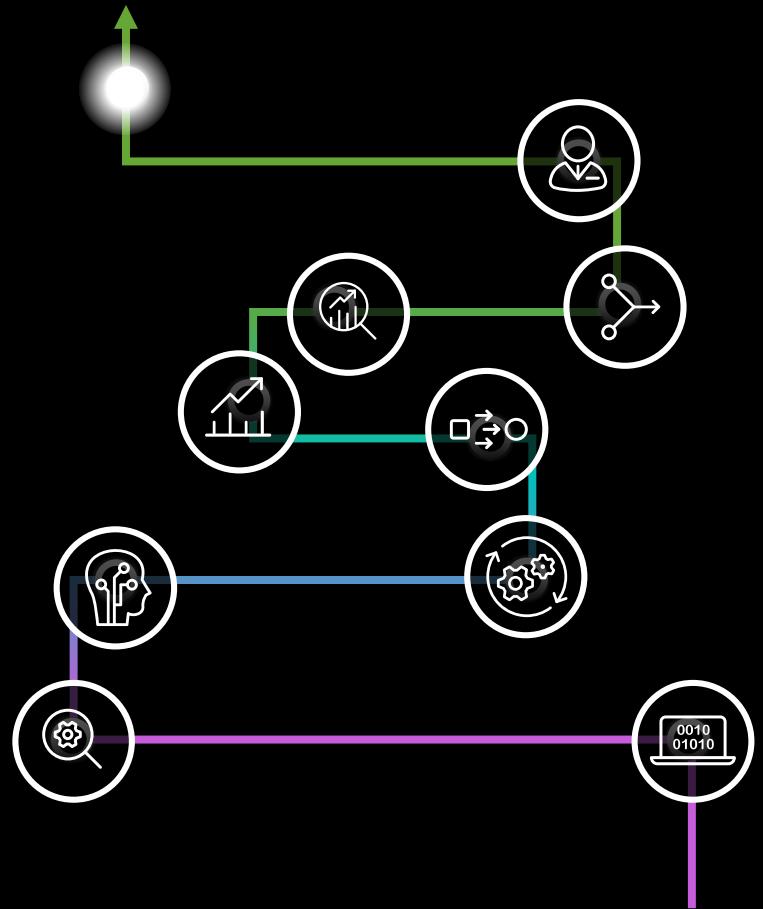


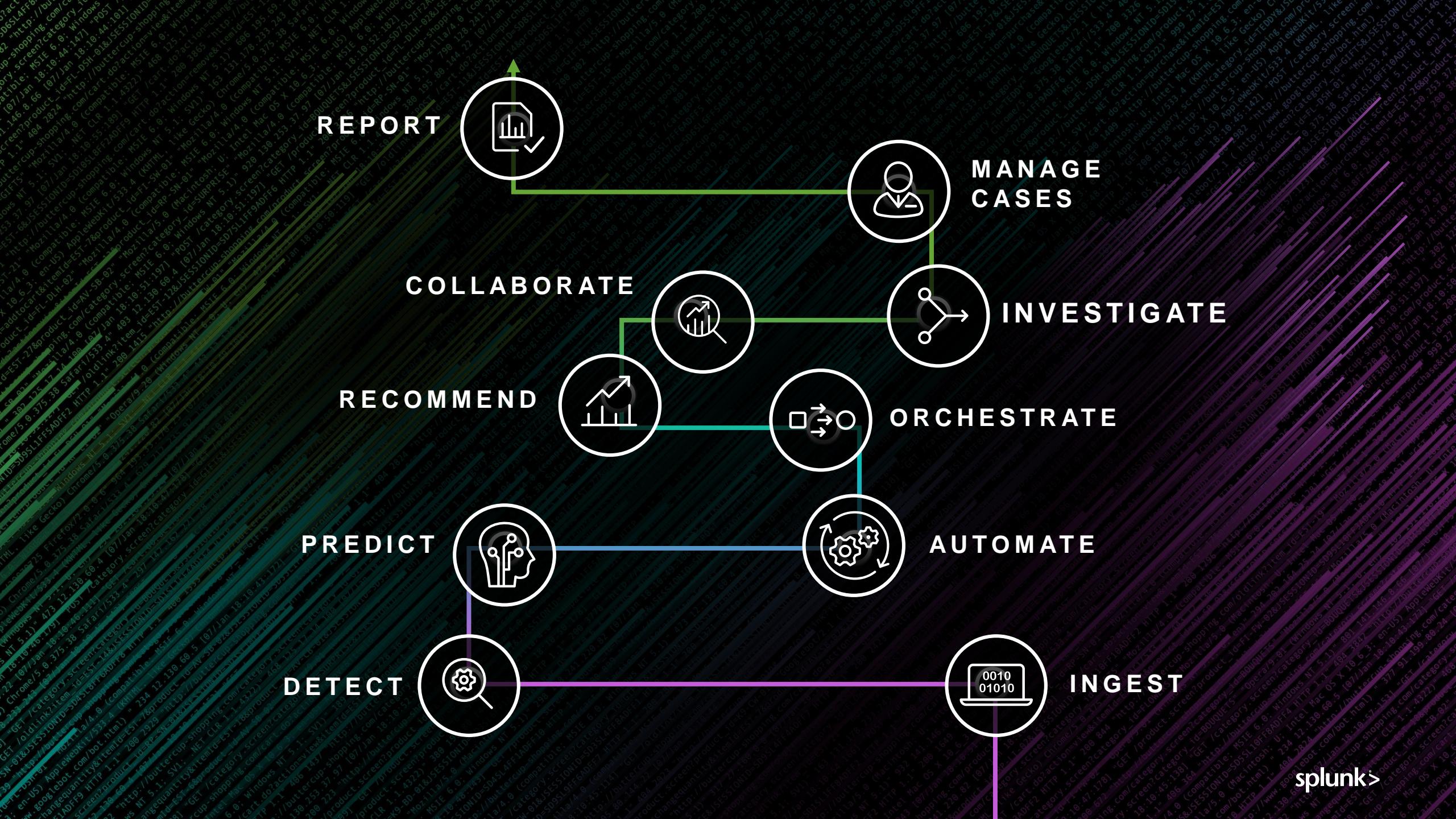
# MANAGE CASES

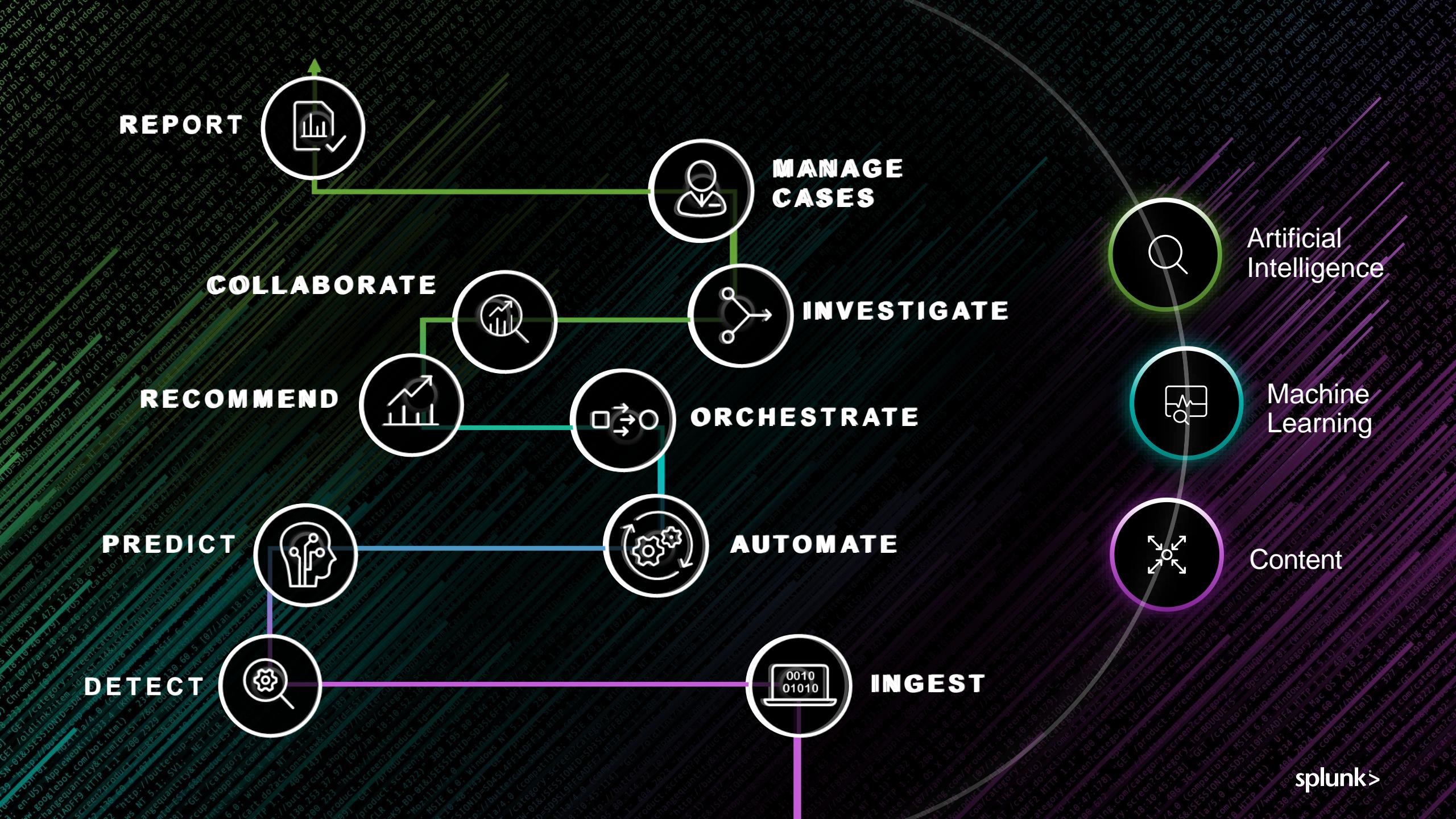




# REPORT





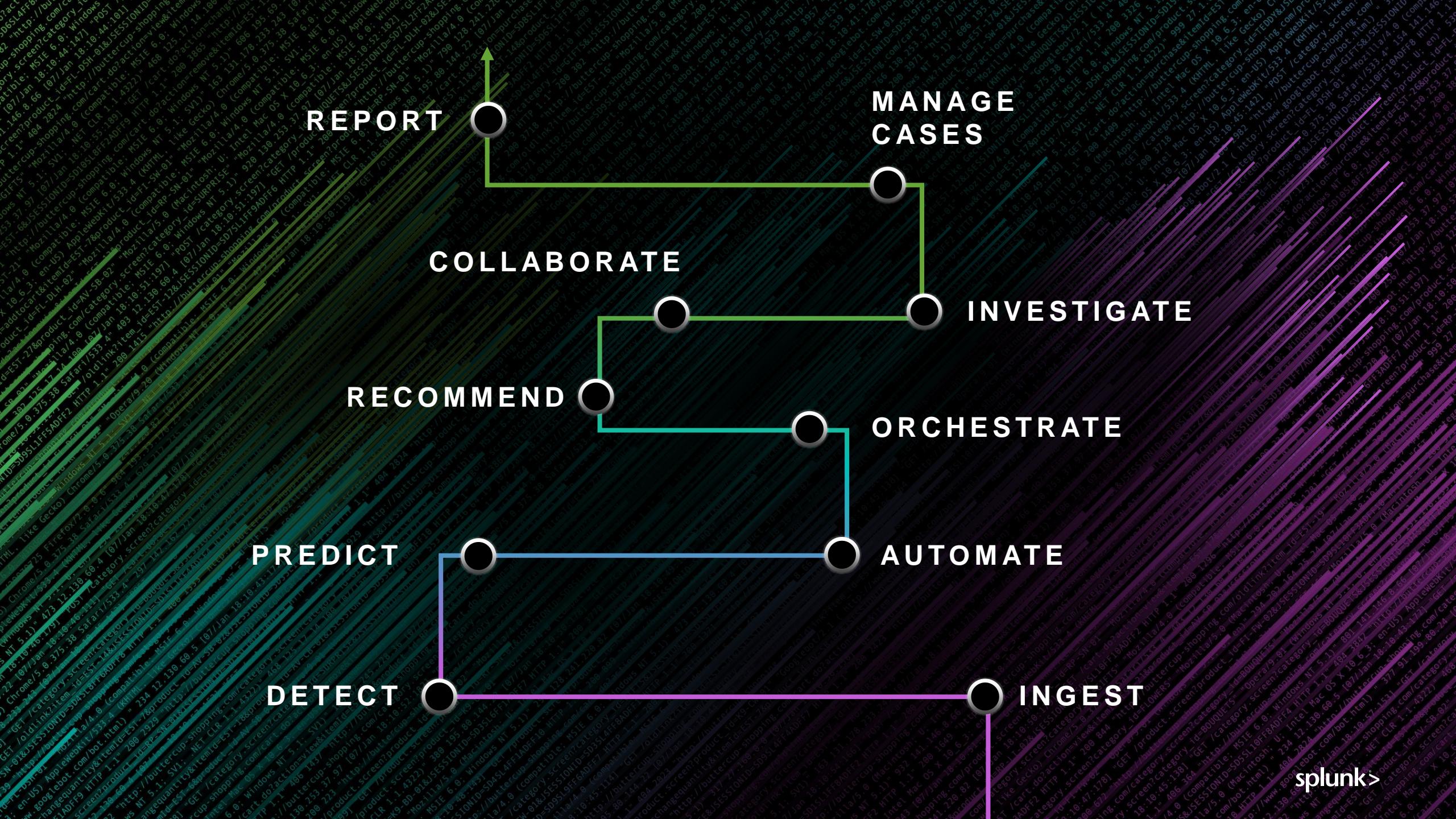


# KARTHIK KANNAN

Head, Security Analytics

*See the forest and\* the trees.*

splunk>



# Tomorrow's SOC Starts Today

Prediction



Detection



## ES & UBA

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

The screenshot displays the Splunk Enterprise Security web interface. At the top, a navigation bar includes links for Home, Security Posture, Incident Review, Investigations, Gloss Tables, Security Intelligence+, Security Domains+, Audit, Search, and Configure. A search bar and a 'Bookmark' button are also present. The main content area is titled 'Use Case Library' and contains a sub-section for 'Abuse'. Under 'Abuse', there is a section for 'Malicious PowerShell' which describes how attackers are finding ways to run PowerShell scripts without download binary files. It lists several recommended data sources like Carbon Black Response, CrowdStrike Falcon, Symantec, Tanium, and Ziffen. Below this is a 'Framework Mapping' section for CIS 20, Kill Chain Phases, and ATT&CK. The bottom part of the interface shows a list of analytic stories categorized under 'Adversary Tactics', such as 'Possible Backdoor Activity Associated With MUDCARP Espionage Campaigns' and 'Suspicious DNS Traffic'.

# Lateral Movement



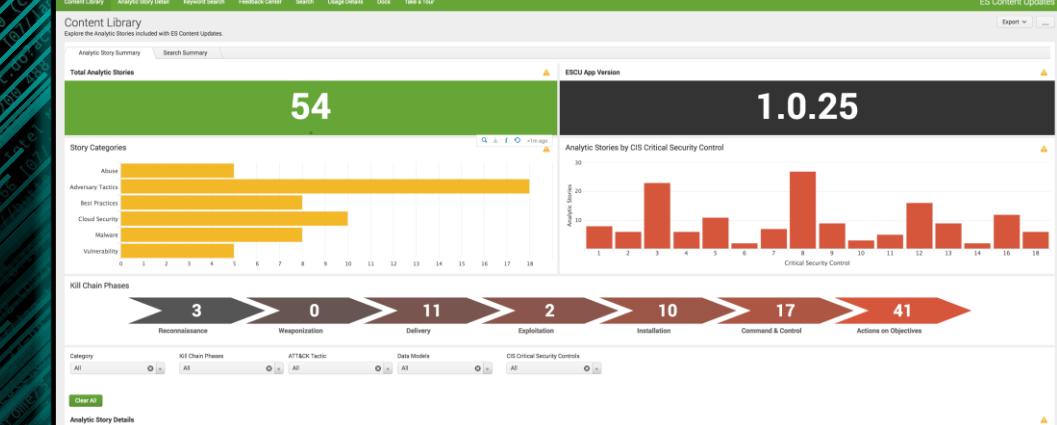
splunk>

# Tomorrow's SOC Starts Today

Collaboration

Reporting

Investigation



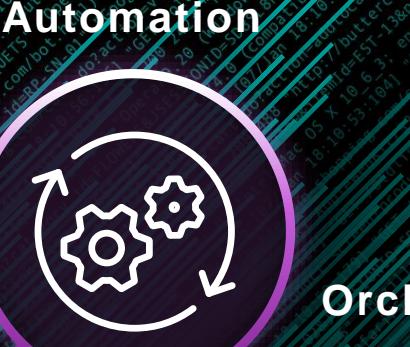
# ES

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

# Tomorrow's SOC Starts Today

**Phantom**  
- Response Identification & Automation  
- Indicator View  
- Playbooks

The screenshot shows two main sections. On the left is the "Indicator View" for IP address 195.22.28.198, displaying a timeline from Aug 26, 2018 - Sep 25, 2018. It lists several events, each with a timestamp, source, type, and ID. On the right is the "Playbook Editor" titled "advanced\_playbookTutorial". It shows a flowchart with various steps: "Q: INVESTIGATE file reputation", "IF: file reputation", "IF: terminate pr.", "IF: add to blacklist", "IF: set severity", "IF: block ip", "IF: confirm", "CONNECT", "unlock 1", and "remove from blacklist". The editor also includes "PLAYBOOK SETTINGS" and "EDIT PLAYBOOK" buttons.



Automation



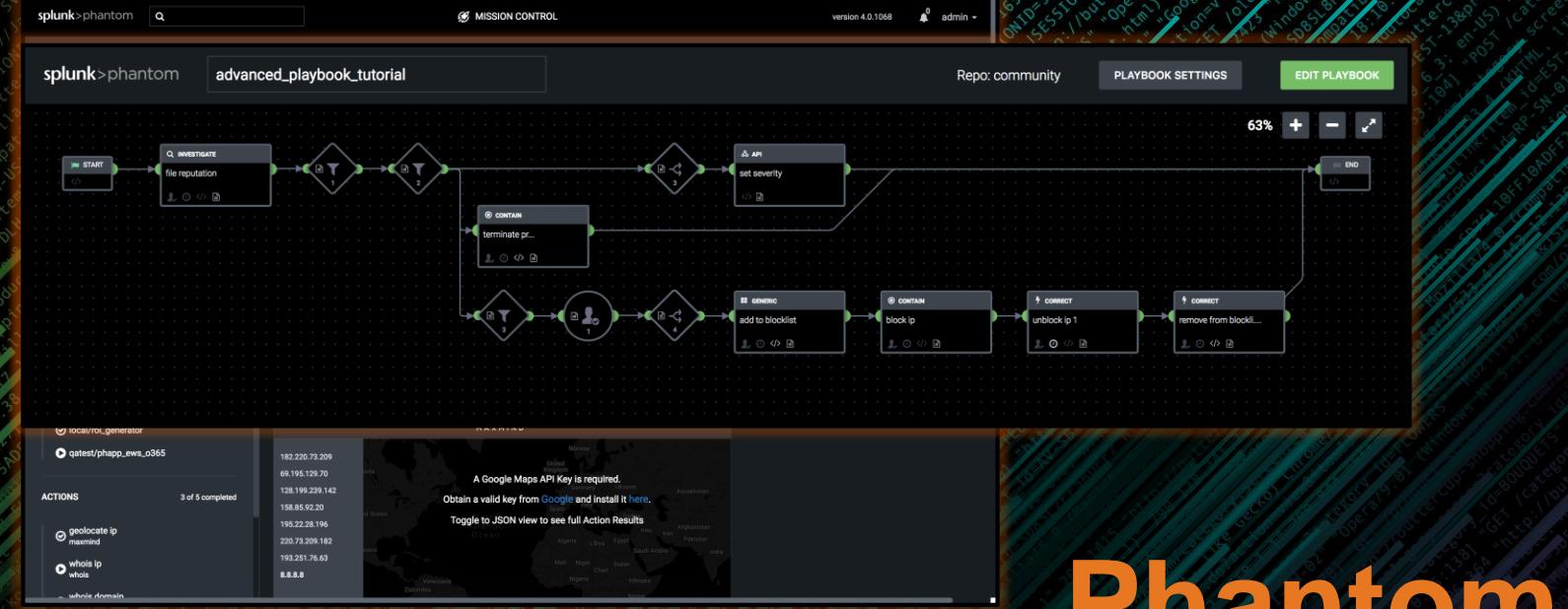
Orchestration



Case  
Management

splunk>

# Tomorrow's SOC Starts Today



Recommendation

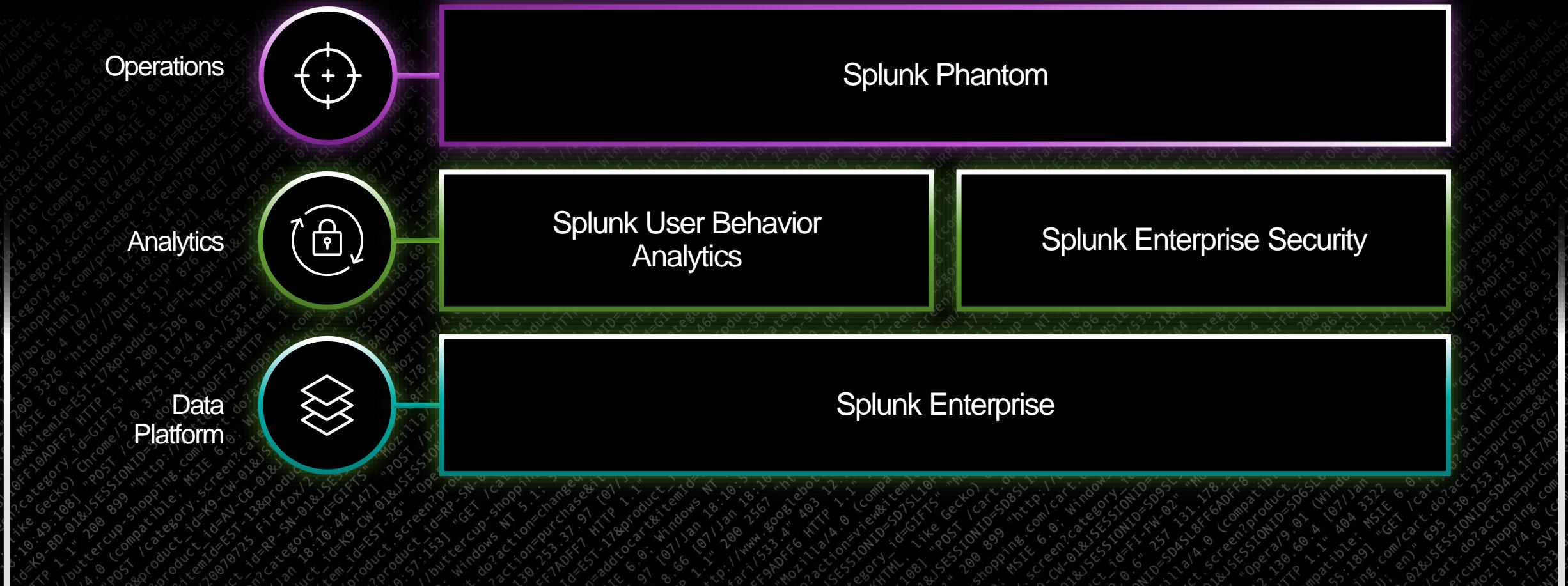
Phantom  
Mission Guidance  
Playbooks



splunk>



splunk>



# Extending Beyond the SOC

SECURITY  
OPERATIONS  
CENTER

Fraud Analytics

Compliance

Data Privacy

# NewYork-Presbyterian

splunk>

# JENNINGS ASKE

CISO  
New York-Presbyterian

NewYork-Presbyterian

splunk>

NewYork-Presbyterian

splunk®

splunk®

# SPLUNK ENTERPRISE CUSTOMERS

Splunk Enterprise Security  
Splunk Phantom

Demo @ App Showcase  
Security & Risk Monitoring  
SOC Automation

**SEC1798**  
The Great SIEM Migration  
Today @ 4:45pm

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

Ask The Experts  
SIEM and SOAR

# SPLUNK ENTERPRISE SECURITY

CUSTOMERS

**Splunk User Behavior Analytics**  
**Splunk Phantom**

**Demo @ App Showcase**  
**Insider + Advanced Threat Detection**  
**SOC Automation**

**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**

# SPLUNK PHANTOM CUSTOMERS

Splunk Enterprise Security  
Splunk User Behavior Analytics

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

**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

# 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



LEARN  
MORE

**80+**

Security Breakout and Theater Sessions

**3**

BOTS-related Hands-on Sessions

**4**

New Security Projects @ Innovation Labs

**1**

Phantom Playbook Hackathon

# Customer First. Technology Forward. Solution Centric.



.conf18

splunk>

BOSS

of the SOC

3RD

# 1ST GODS OF OR



splunk>

# Thank You