RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SPO3-R03

Effectiveness vs. Efficiency:
10 Capabilities of the Modern Security Operations Center

Oliver Friedrichs

VP, Security Automation & Orchestration
Splunk

Oliver Friedrichs

- VP, Security Automation & Orchestration, Splunk
- Founder and CEO, Phantom
- Sourcefire (Cisco), Symantec, McAfee
- Two decades of security expertise

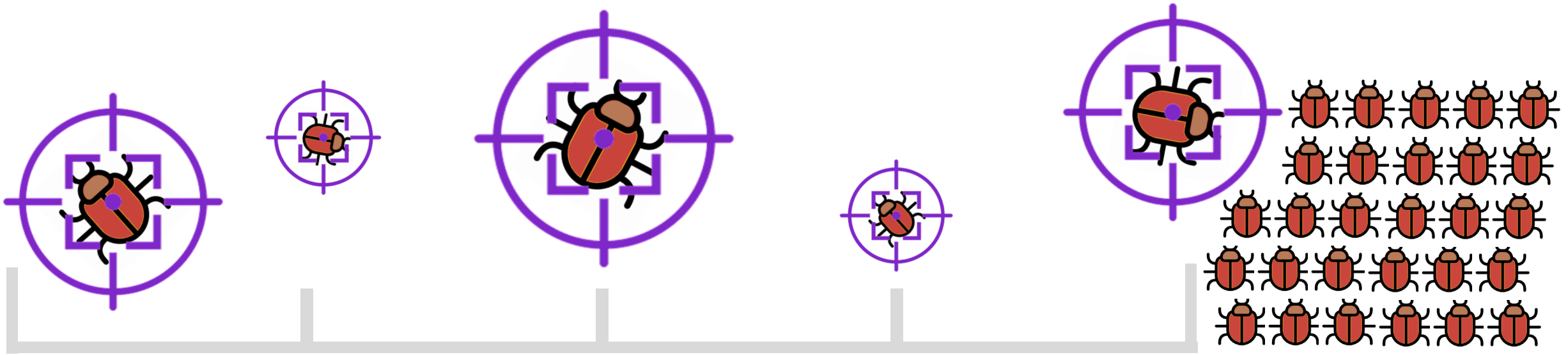
Effectiveness vs. Efficiency

Accelerating your detection and response workflows

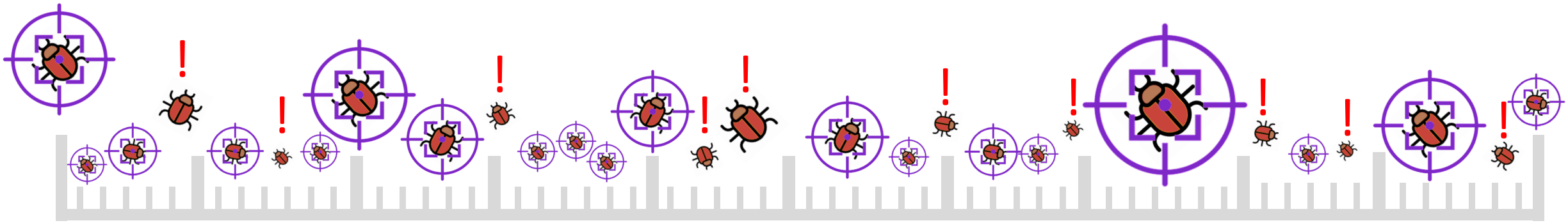
Scaling your resources

Optimizing your security operations

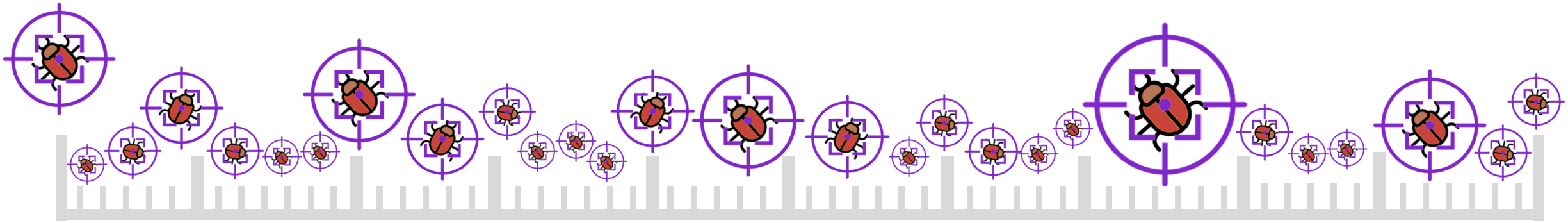
Effectiveness



Efficiency

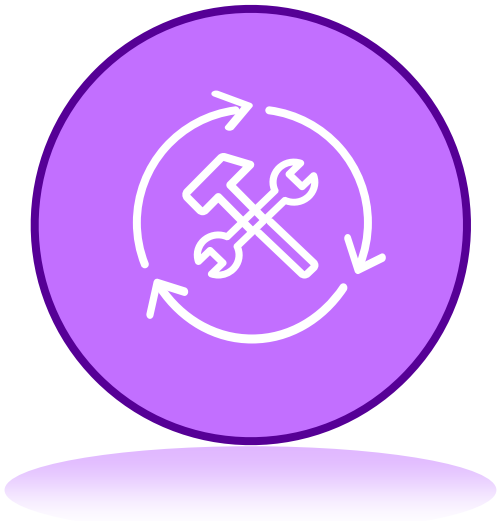


Effectiveness AND Efficiency



But…security people are hard to find…

SKILL SHORTAGE



3.5 Million

Unfilled cybersecurity jobs by 2021

75% YOY increases

Expertise Needed

TIER 1

TIER 2

- Security Knowledge
- Computer Networking
- Application Layer Protocols
- Database and Query Languages
- Unix
- Windows
- Basic Parsing
- Command Line Familiarity
- Security Monitoring Tools
- Coding/Scripting
- Regulatory Compliance
- Security Compliance
- Vulnerability Scanning
- Investigations
- Troubleshooting
- Security Clearance
- Communication & Writing
- Critical Thinking
- Creativity & Curiosity
- Motivation

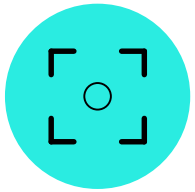
And that's not all…

Too many tools

Analysts are wasting time logging into multiple tools to cross check data and investigate.

Escalating to ticketing systems is arduous

Users cannot easily escalate to ticketing systems, causing a lot of manual copying and pasting or "hacky" solutions that may surface sensitive data.

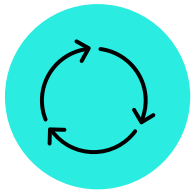


Events lack context

Users are unable to grasp the big picture of an event easily and have challenges with event handoff.

Baby steps towards automation

SOCs are heavily prioritizing orchestration and automation, but taking baby steps.



Difficulty tracking event lifecycle

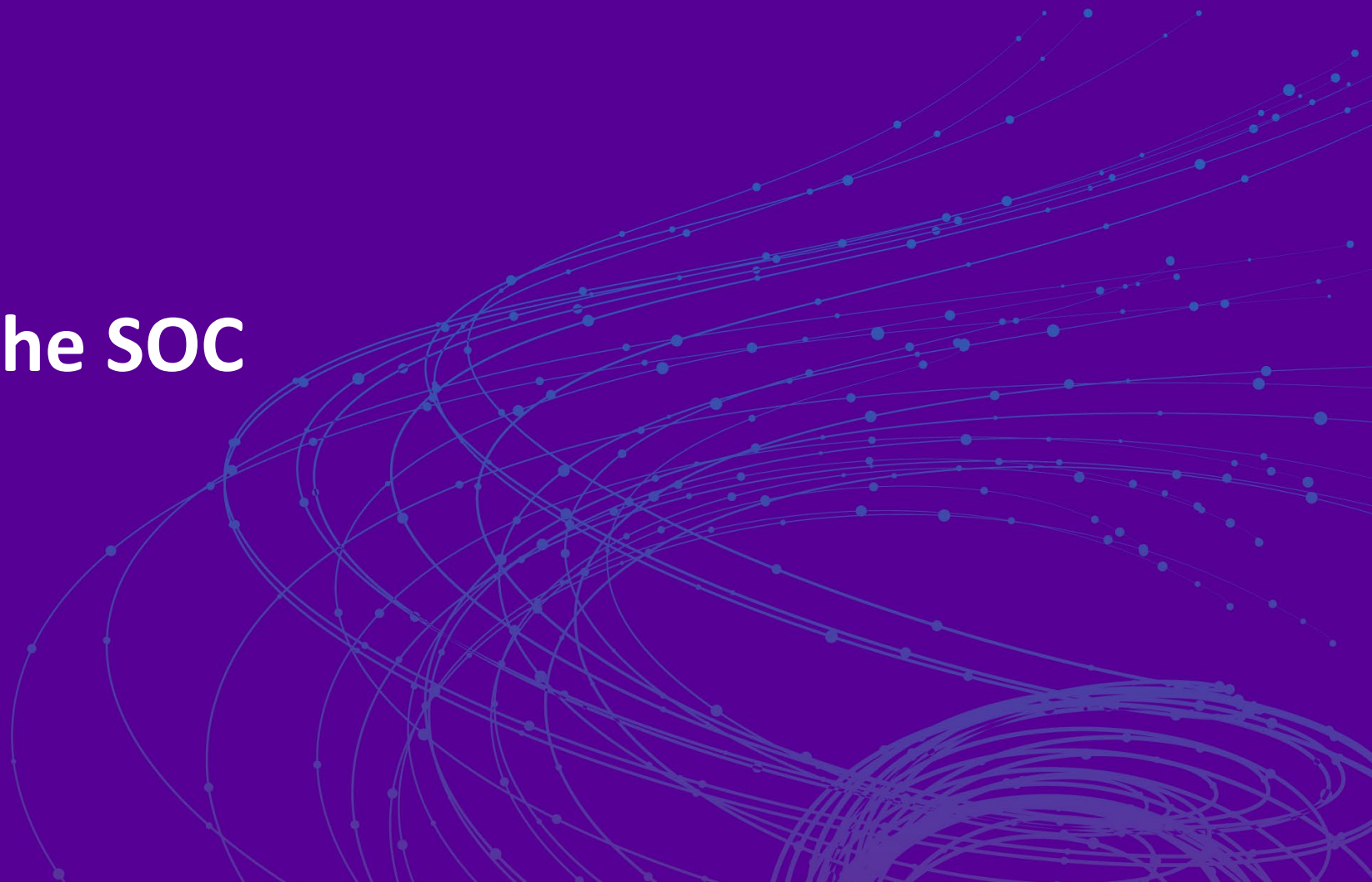
Users want visibility into full alert/event/case lifecycle in a single tool.

Lack of process

SOCs acknowledge they need to continue to develop out and mature their processes. There is still a long way to go.

RSAConference2019

Re-Imagine the SOC



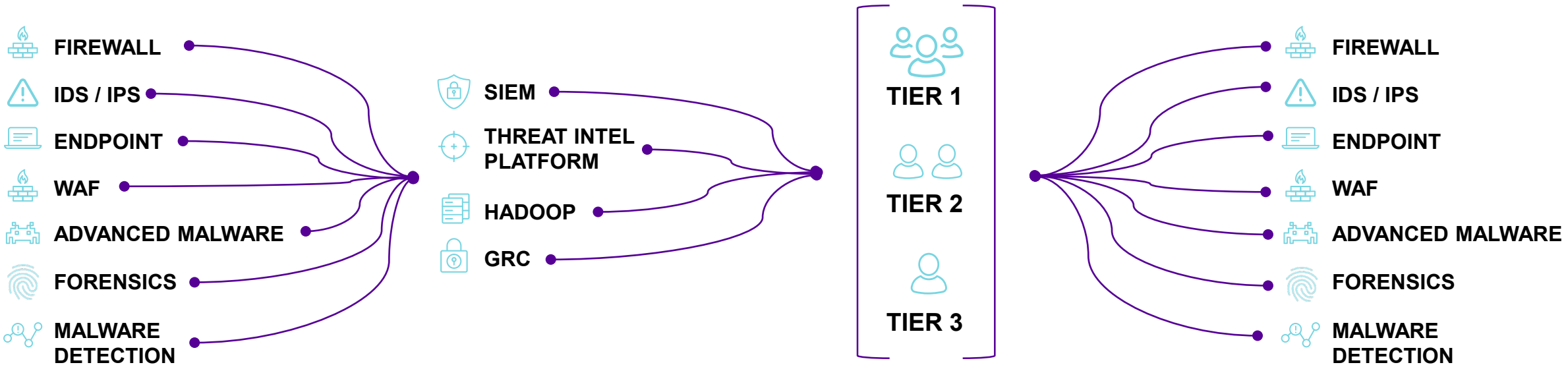
OODA

Observe
Point Products

Orient
Analytics

Decision Making

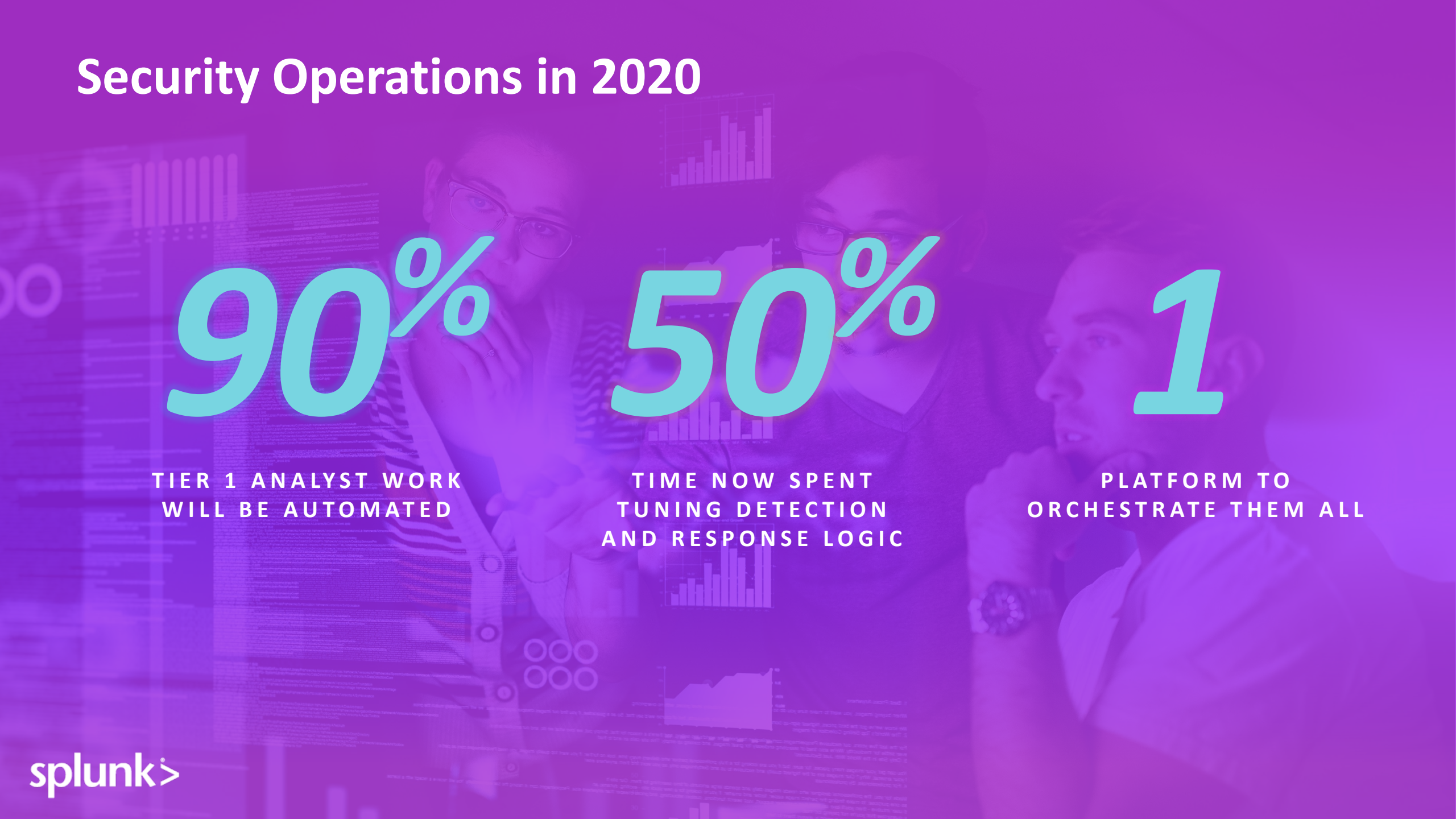
Acting



Security Operations TODAY

splunk>

Security Operations in 2020



90%

TIER 1 ANALYST WORK WILL BE AUTOMATED

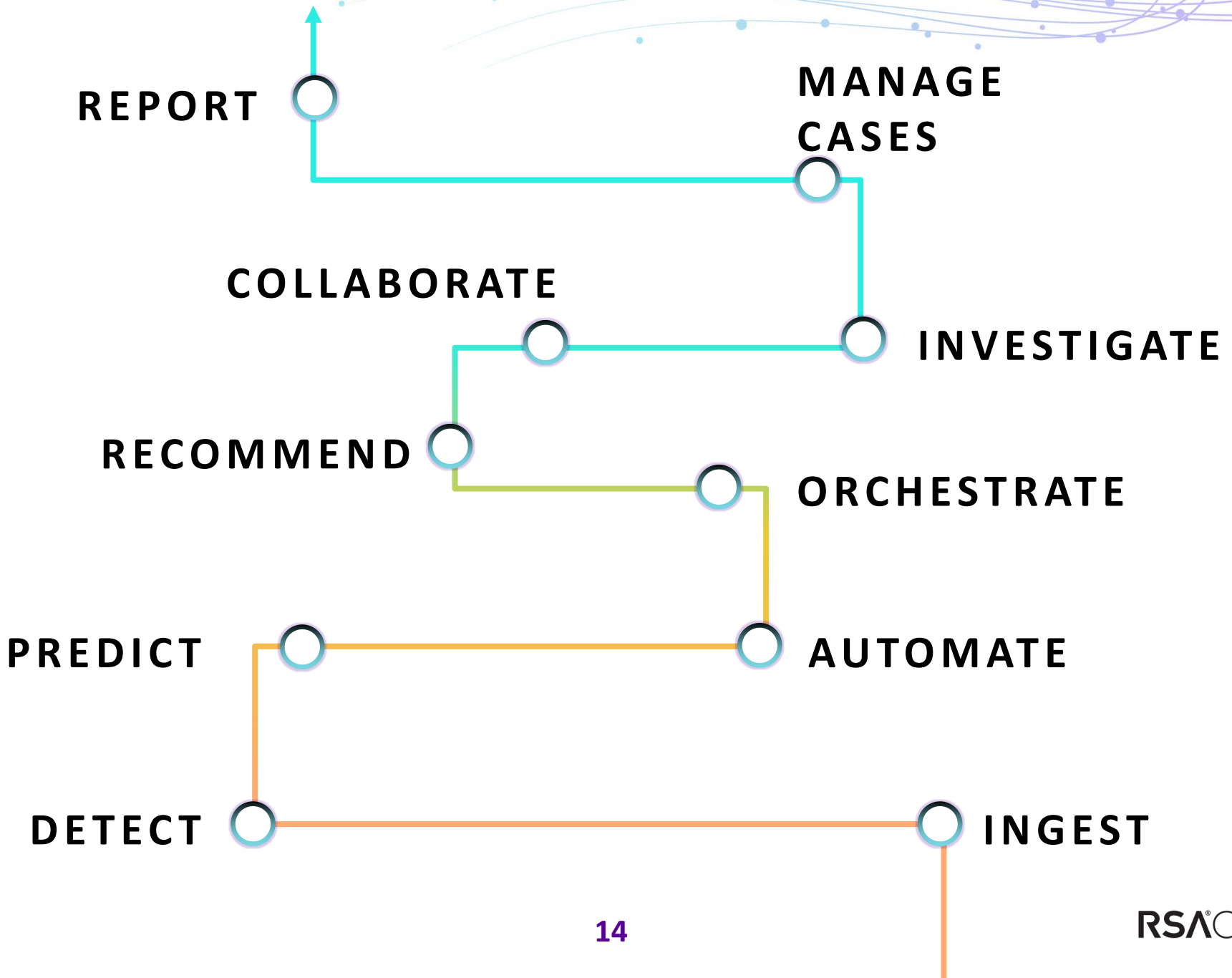
50%

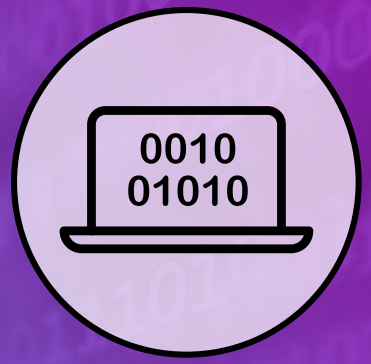
TIME NOW SPENT TUNING DETECTION AND RESPONSE LOGIC

1

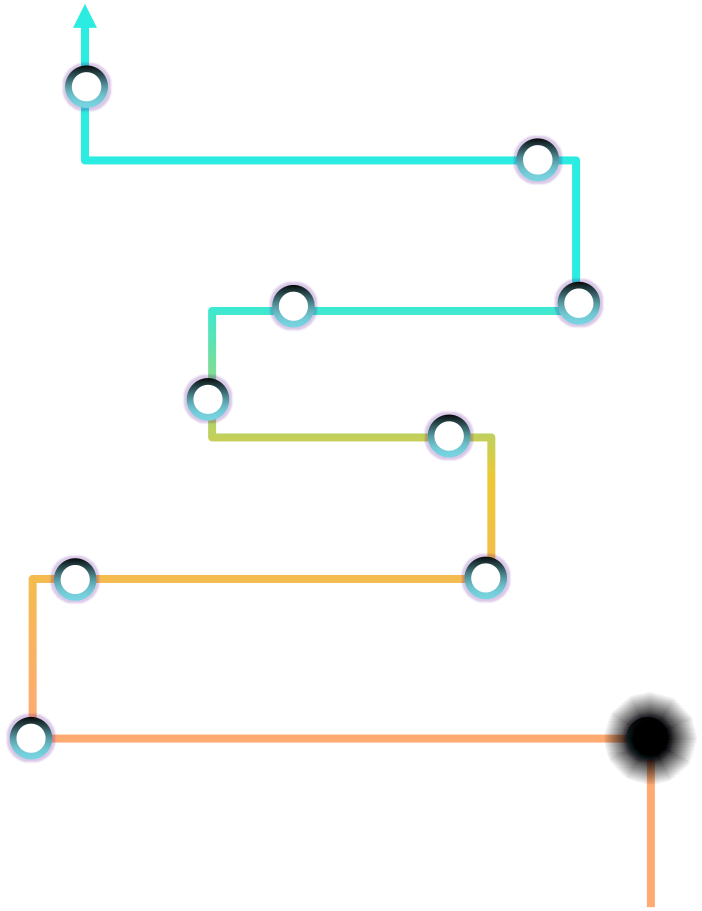
PLATFORM TO ORCHESTRATE THEM ALL

splunk>

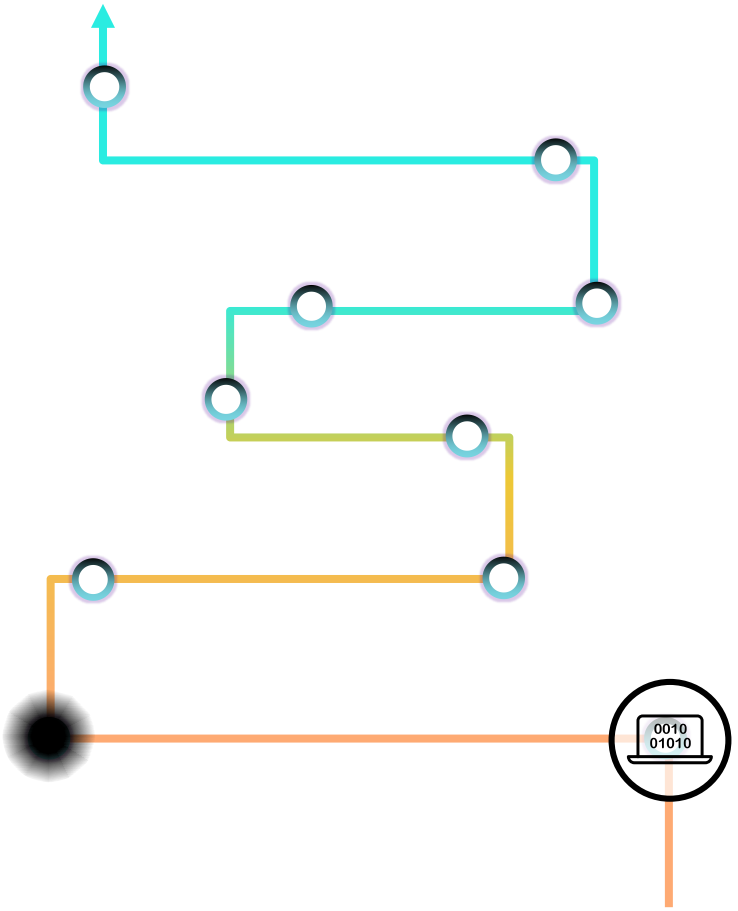

REPORT
MANAGE CASES
COLLABORATE
INVESTIGATE
RECOMMEND
ORCHESTRATE
PREDICT
AUTOMATE
DETECT
INGEST



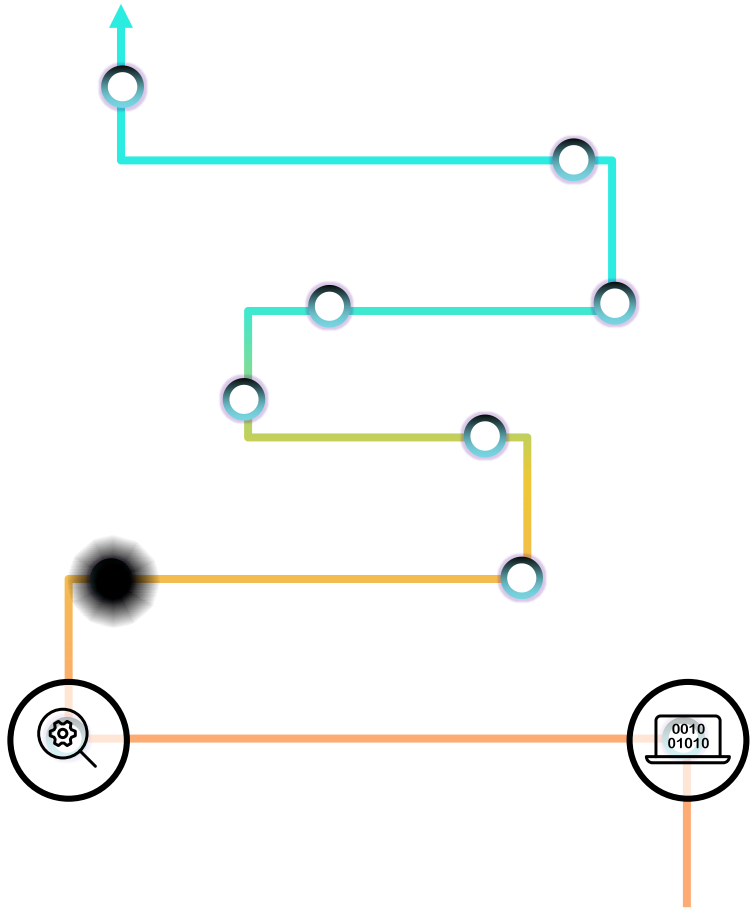
INGEST

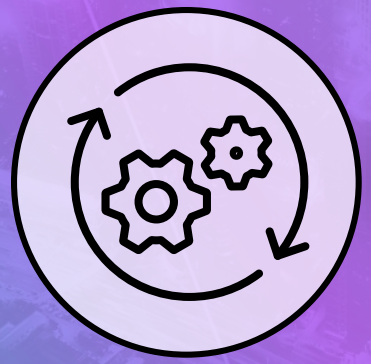


DETECT

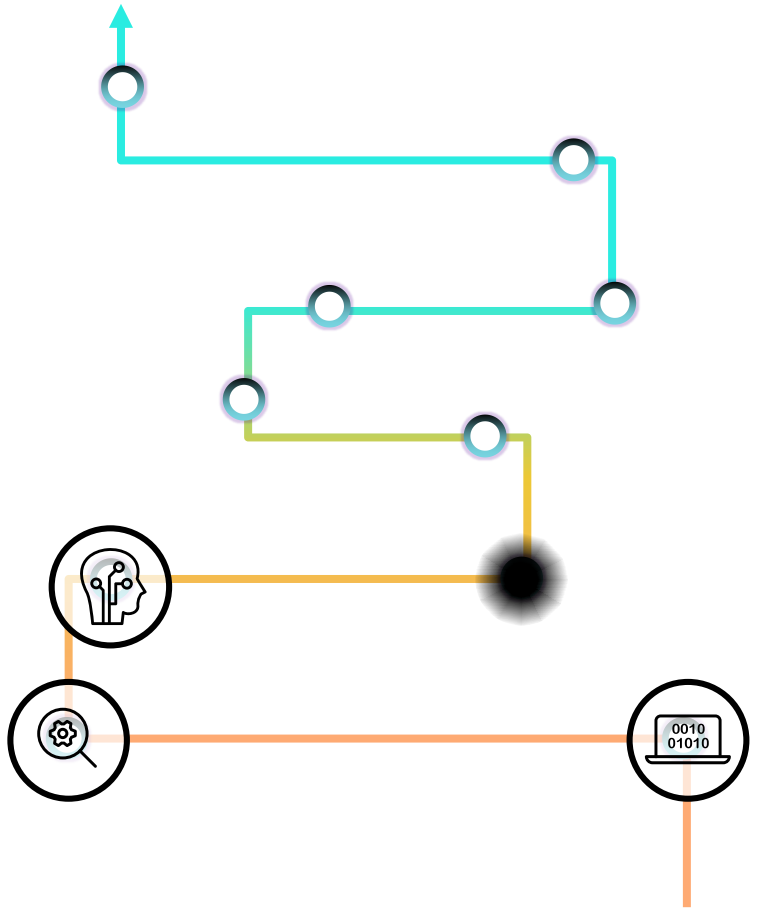


PREDICT

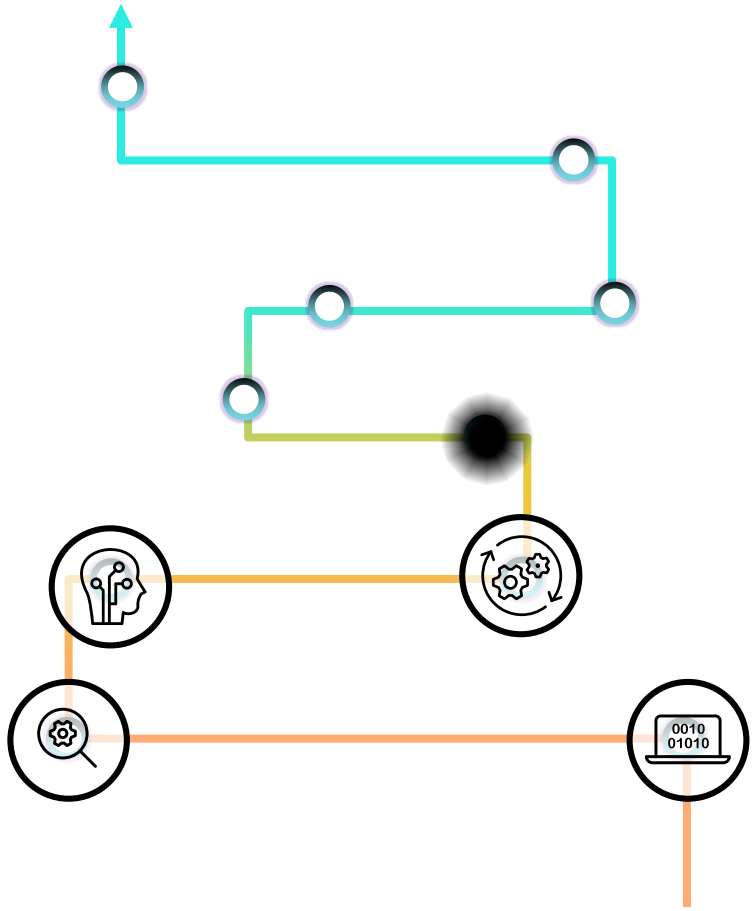




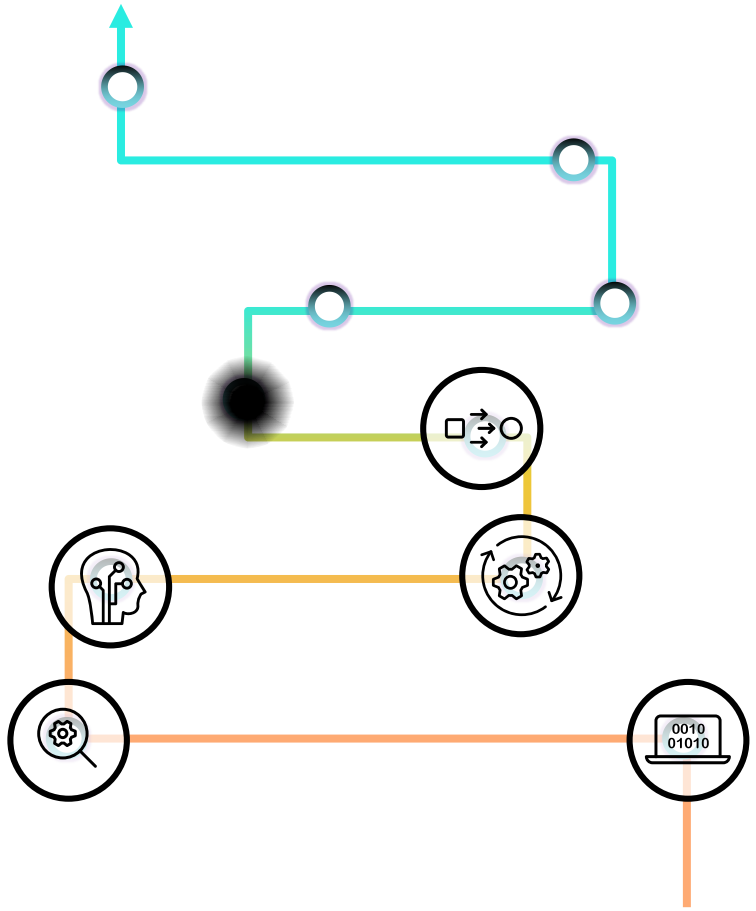
AUTOMATE



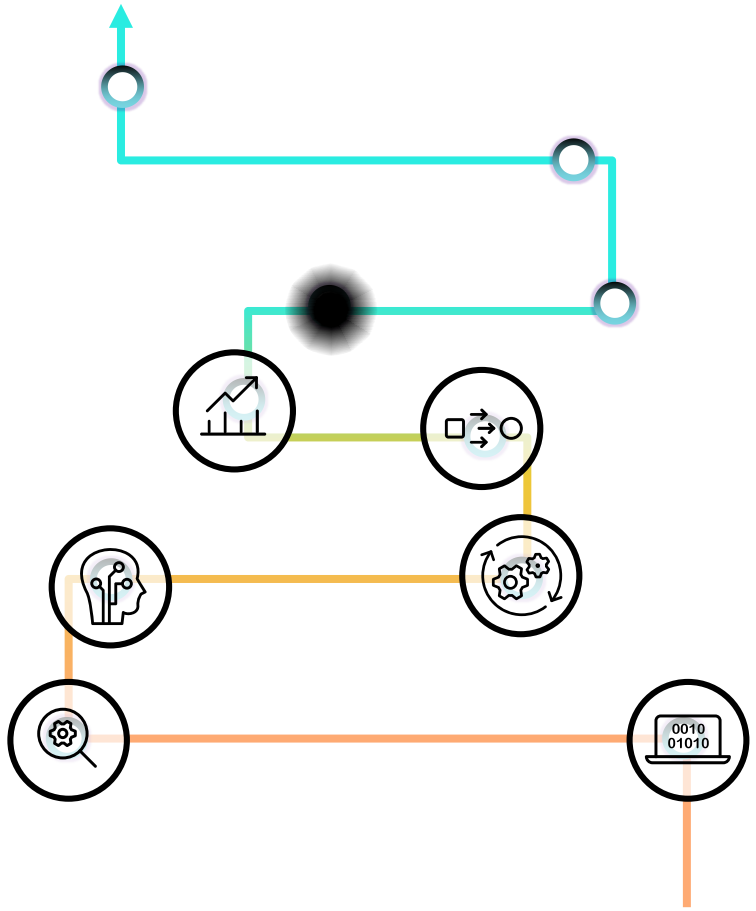
ORCHESTRATE



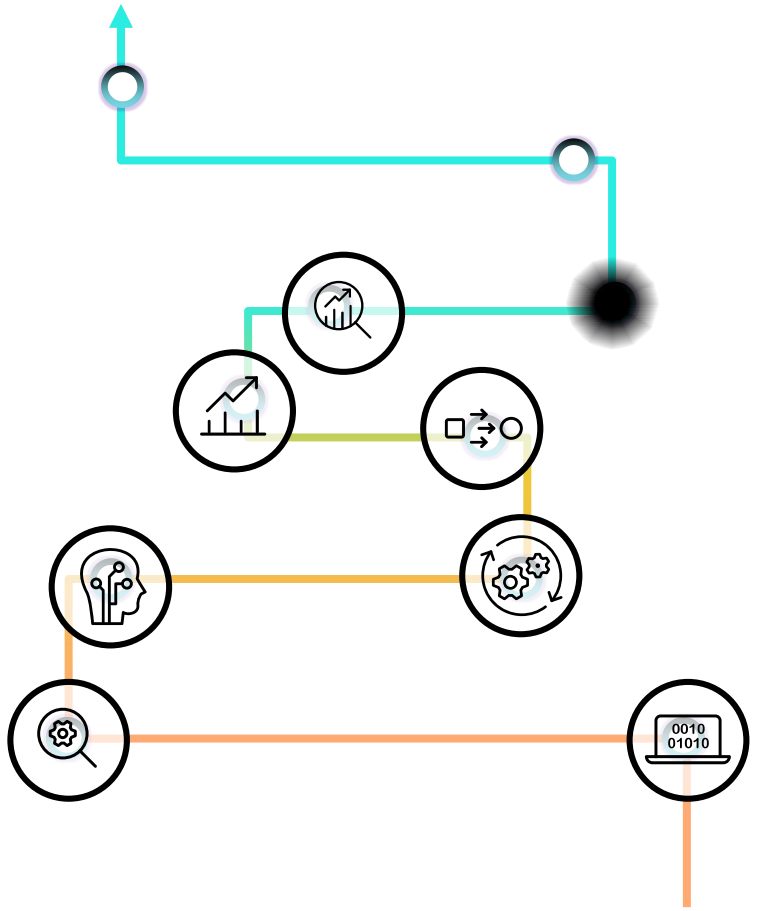
RECOMMEND



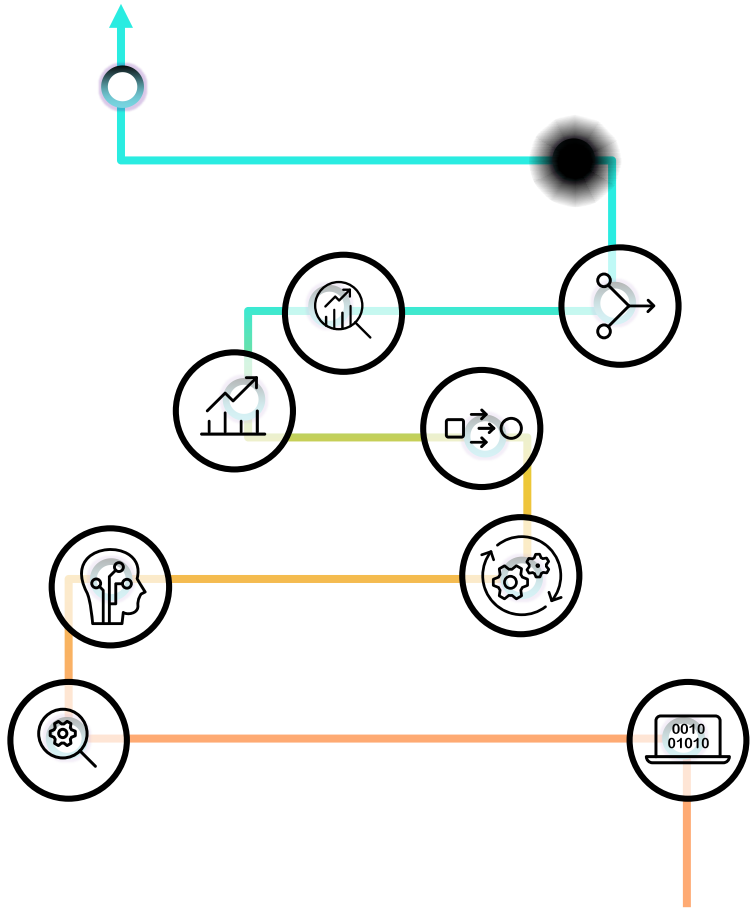
INVESTIGATE



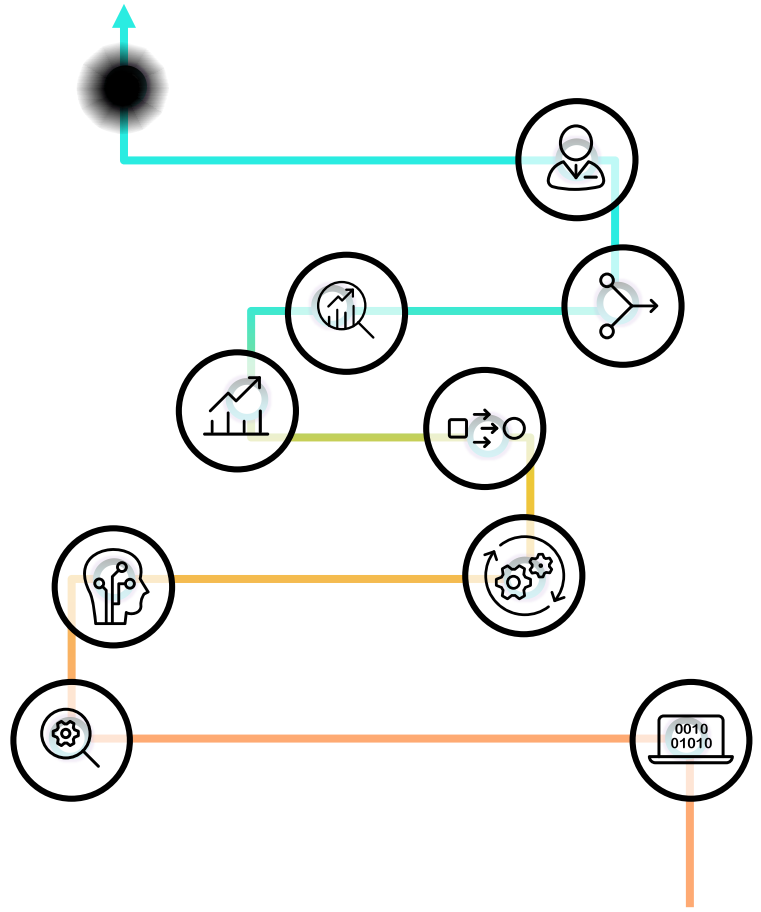
COLLABORATE

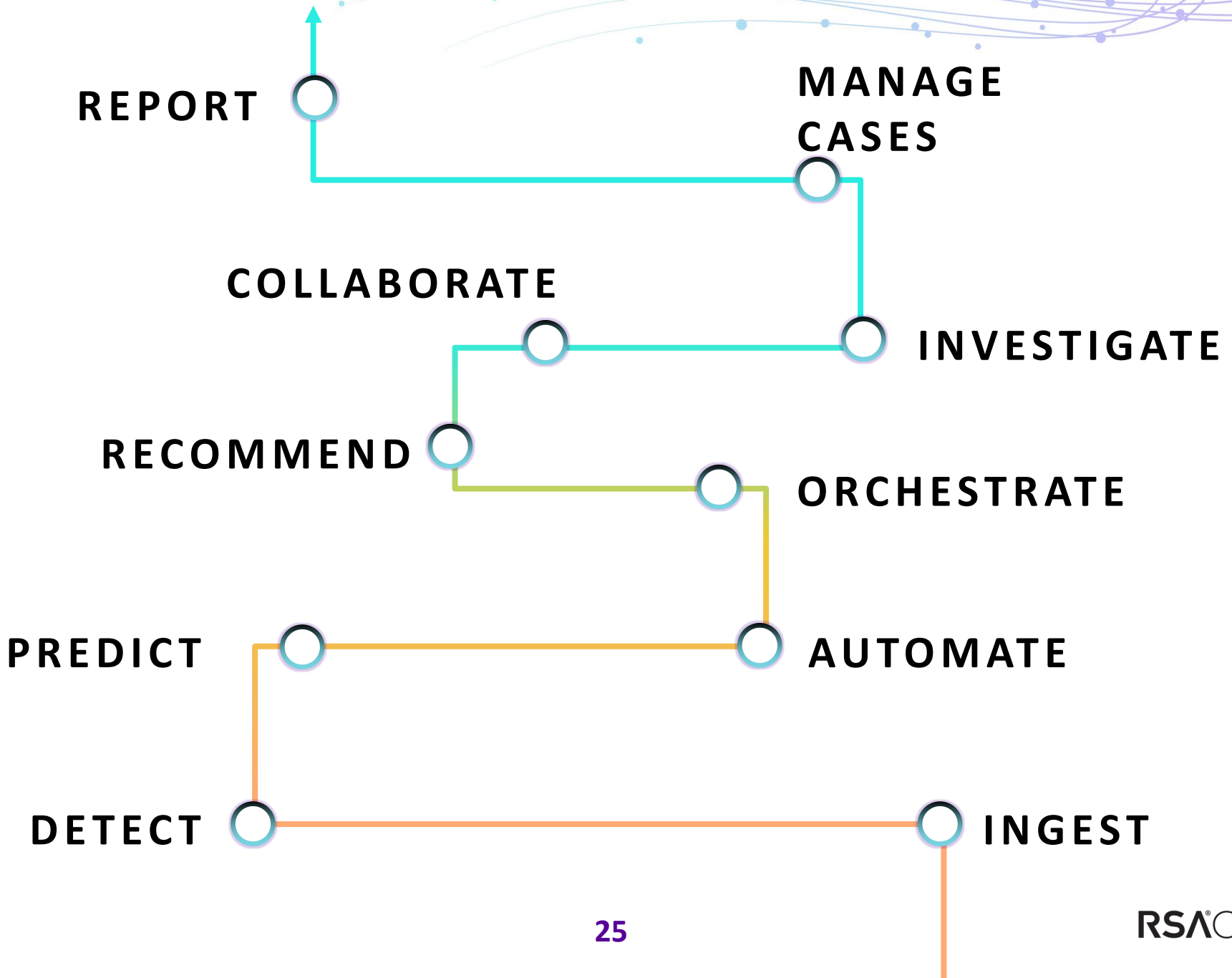


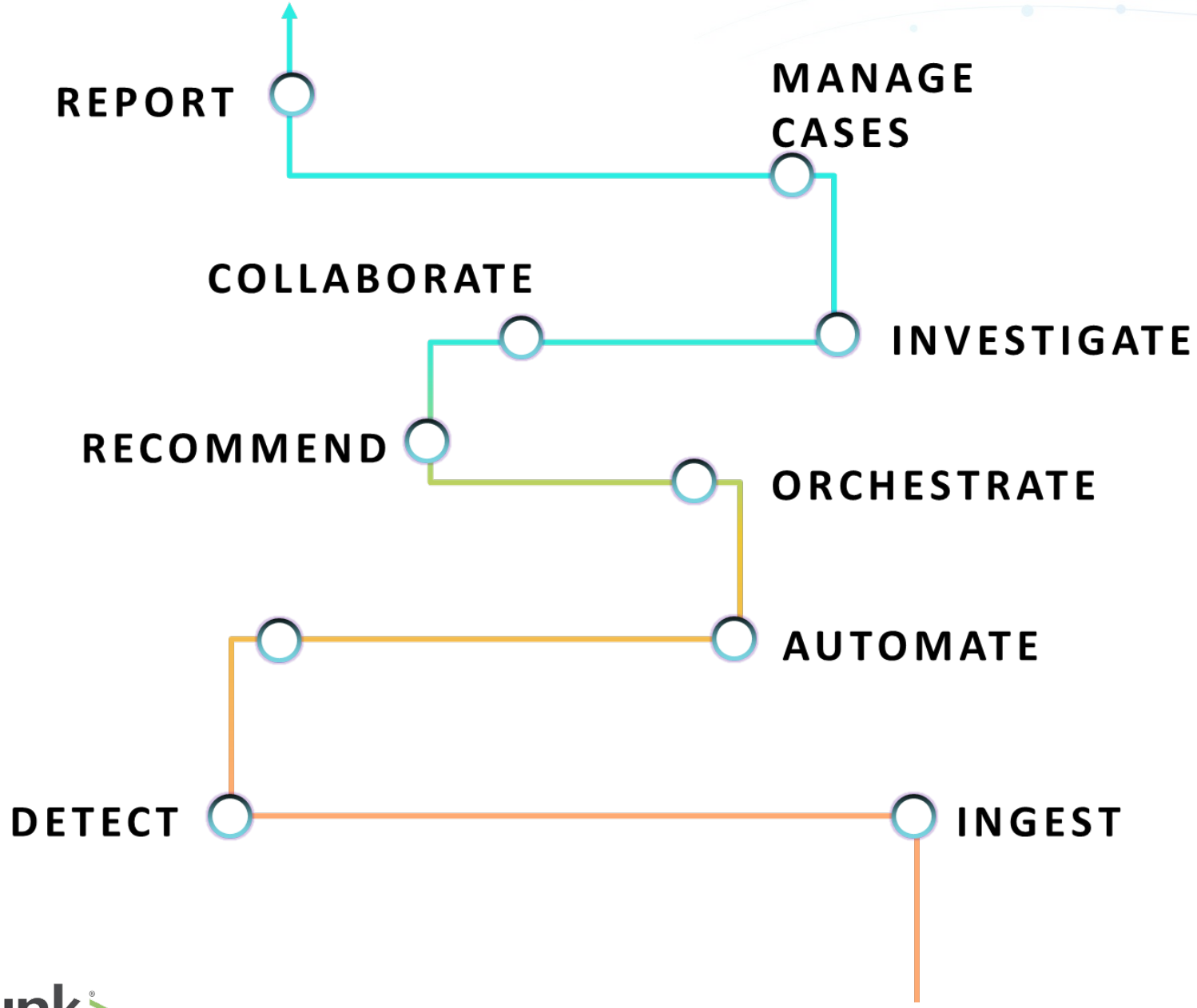
MANAGE CASES



REPORT




REPORT
MANAGE CASES
COLLABORATE
INVESTIGATE
RECOMMEND
ORCHESTRATE
PREDICT
AUTOMATE
DETECT
INGEST

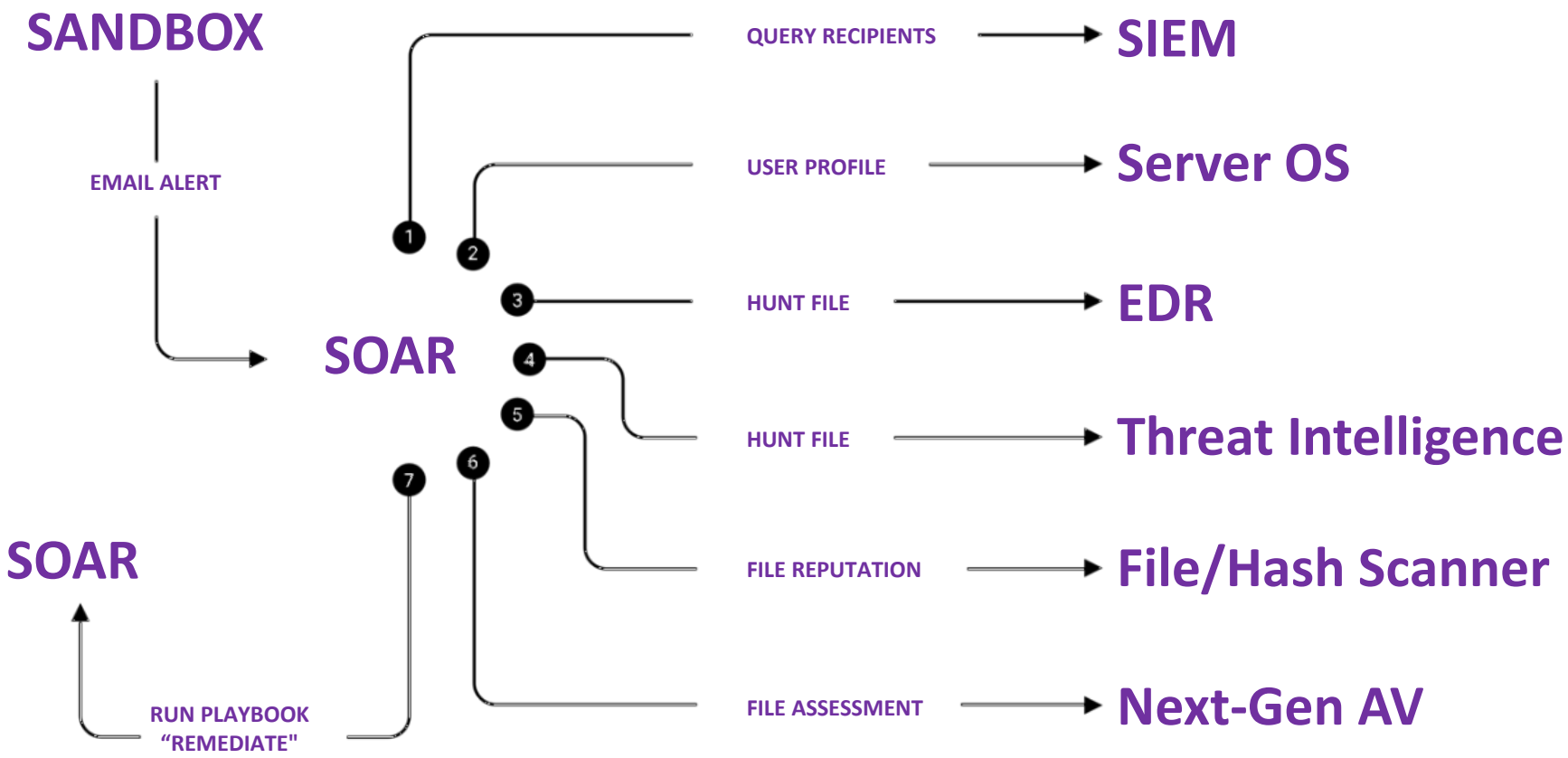


Artificial Intelligence

Machine Learning

How it Works

Automated Malware Investigation



RSAConference2019

Extending Beyond the SOC

Beyond the SOC

Fraud

Compliance

Risk Monitoring

RSAConference2019

Key Takeaways

Today We Covered…

Accelerating your detection and response workflows

Scaling your resources

Optimizing your security operations

RSAConference2019

Thank You

Oliver Friedrichs

ofriedrichs@splunk.com