



CYBER DEFENSE LIVE

Hong Kong 2018

SOAR Above Your Legacy Security Operations Center

Shashwath Hegde, CISSP
Solutions Architect, APAC, FireEye



Typical Characters in the SOC



SOC Analyst

Responsibility: Triage, investigate and respond to alerts in a timely fashion.



Security Engineer

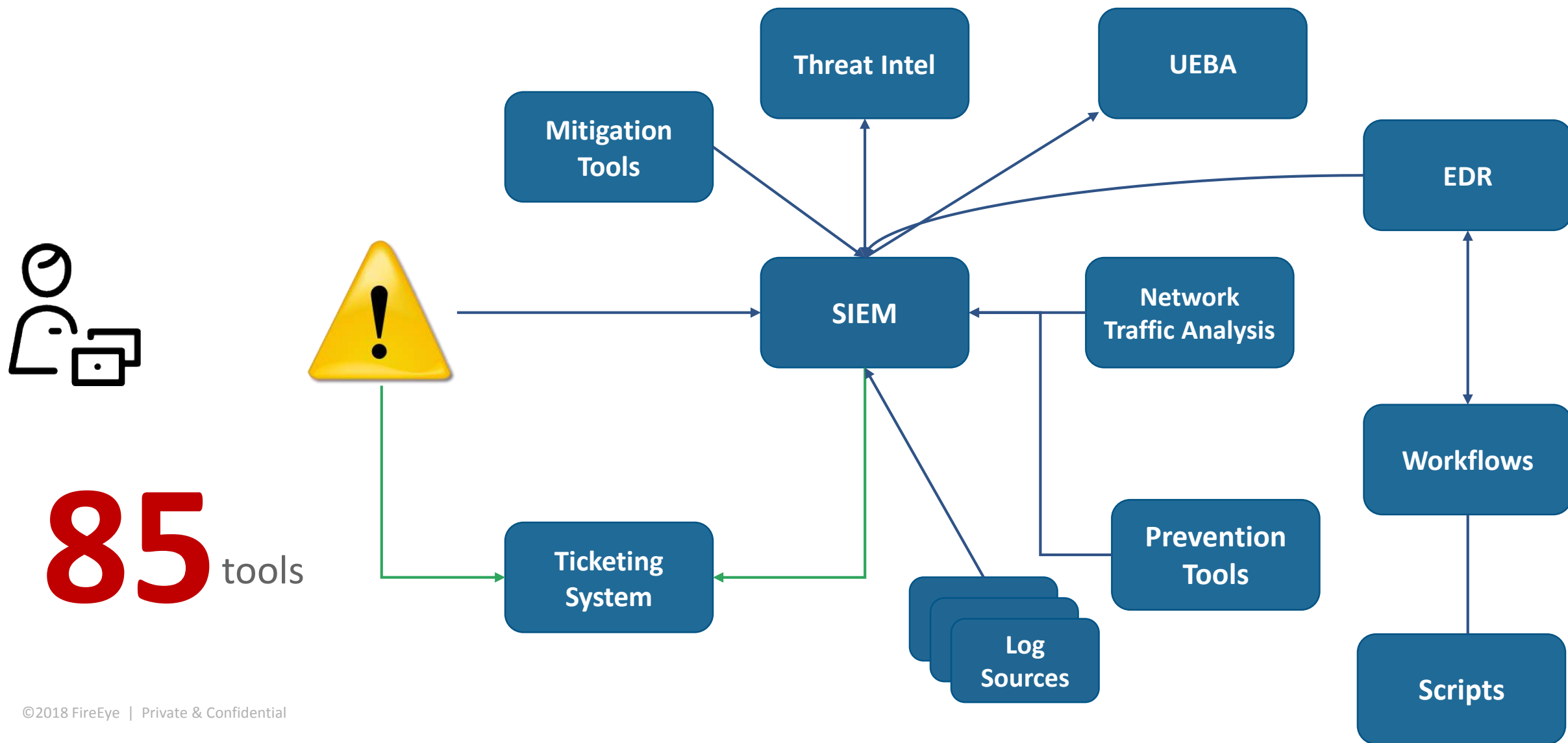
Responsibility: Supporting the SOC team with tools and scripts to help increase operational and triage efficacy.



SOC Manager

Responsibility: Implementing a security program that reduces threat exposure to the organization.

The Analyst's Day – starts with an alert



85 tools

The Analyst's Day – Objectives



Respond in time

10K alerts/day

Prioritize alerts

Triage alerts quickly

add **Contextual Intel**

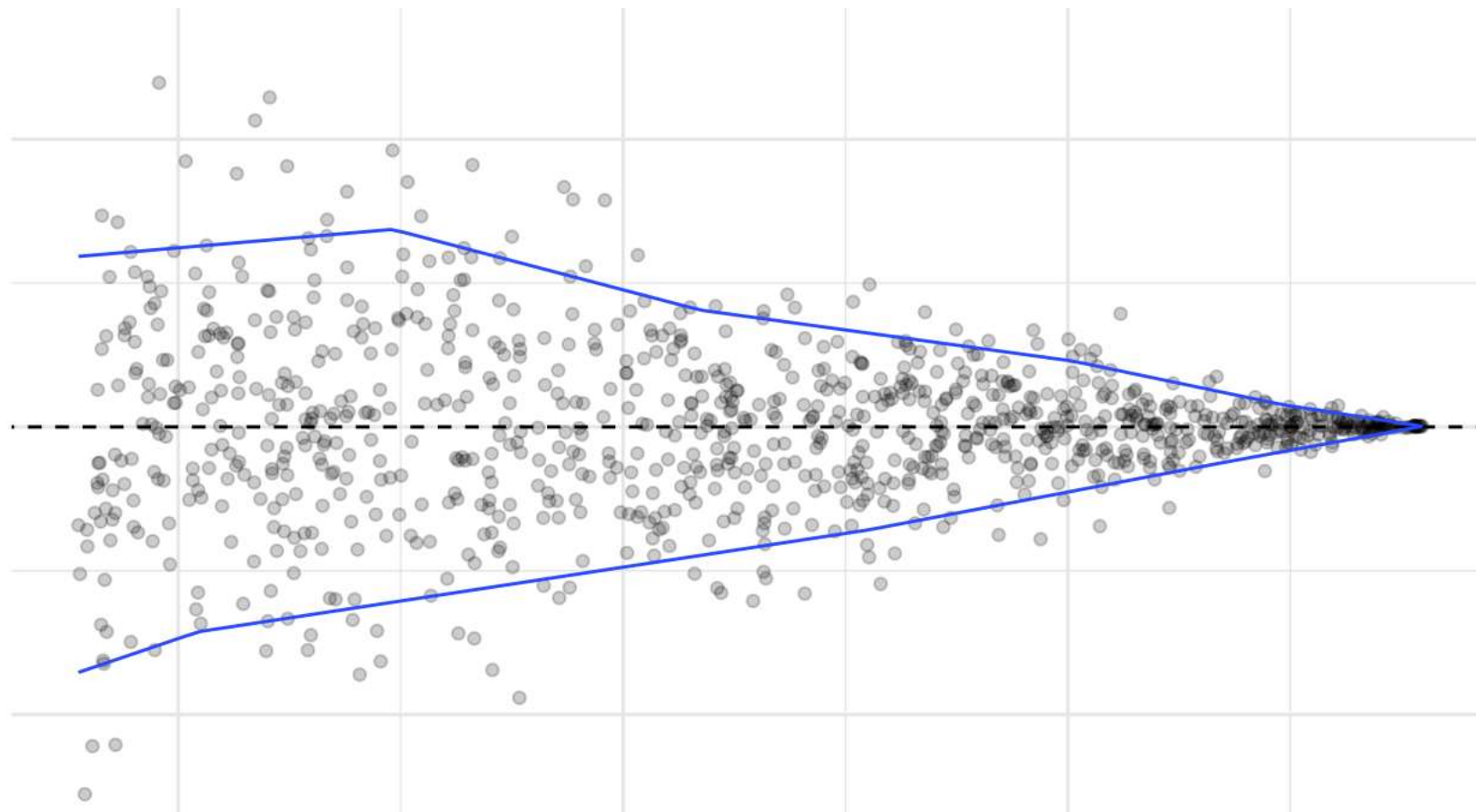
Notify stakeholders

SLA to be met

Report incidents

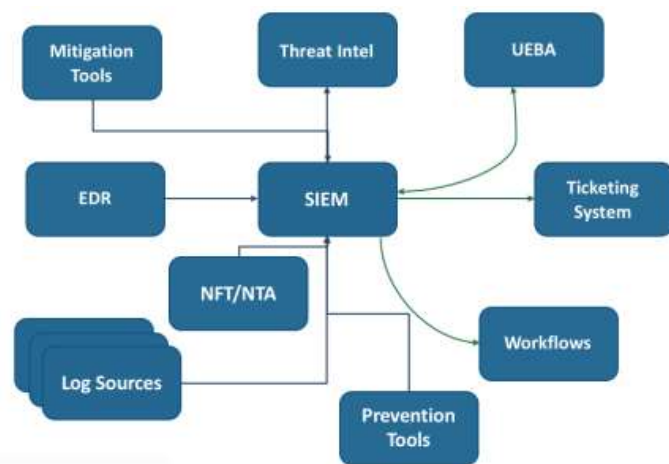
The Analyst's Day – Relevancy and Quality of Alerts

10K
alerts/day

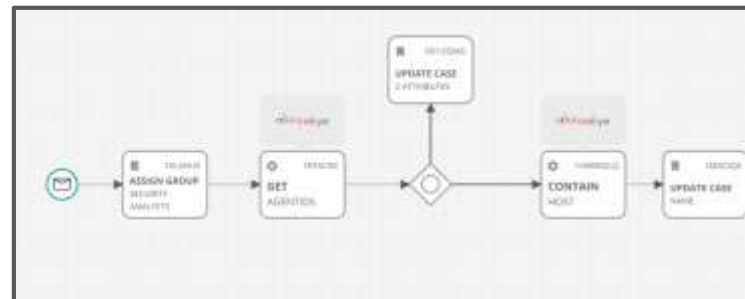


**Only Few
Alerts Matter**

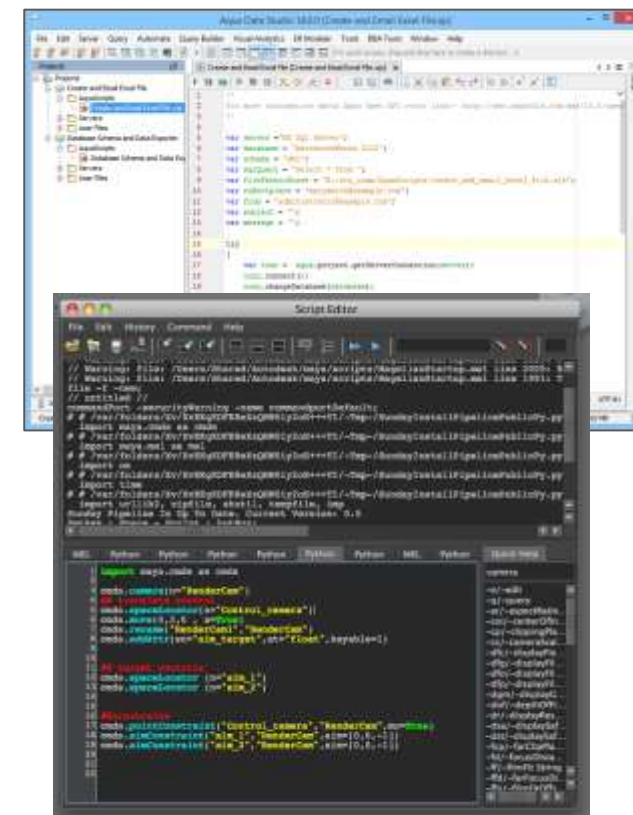
The Engineer's Day – Simplify Workflows



Current state



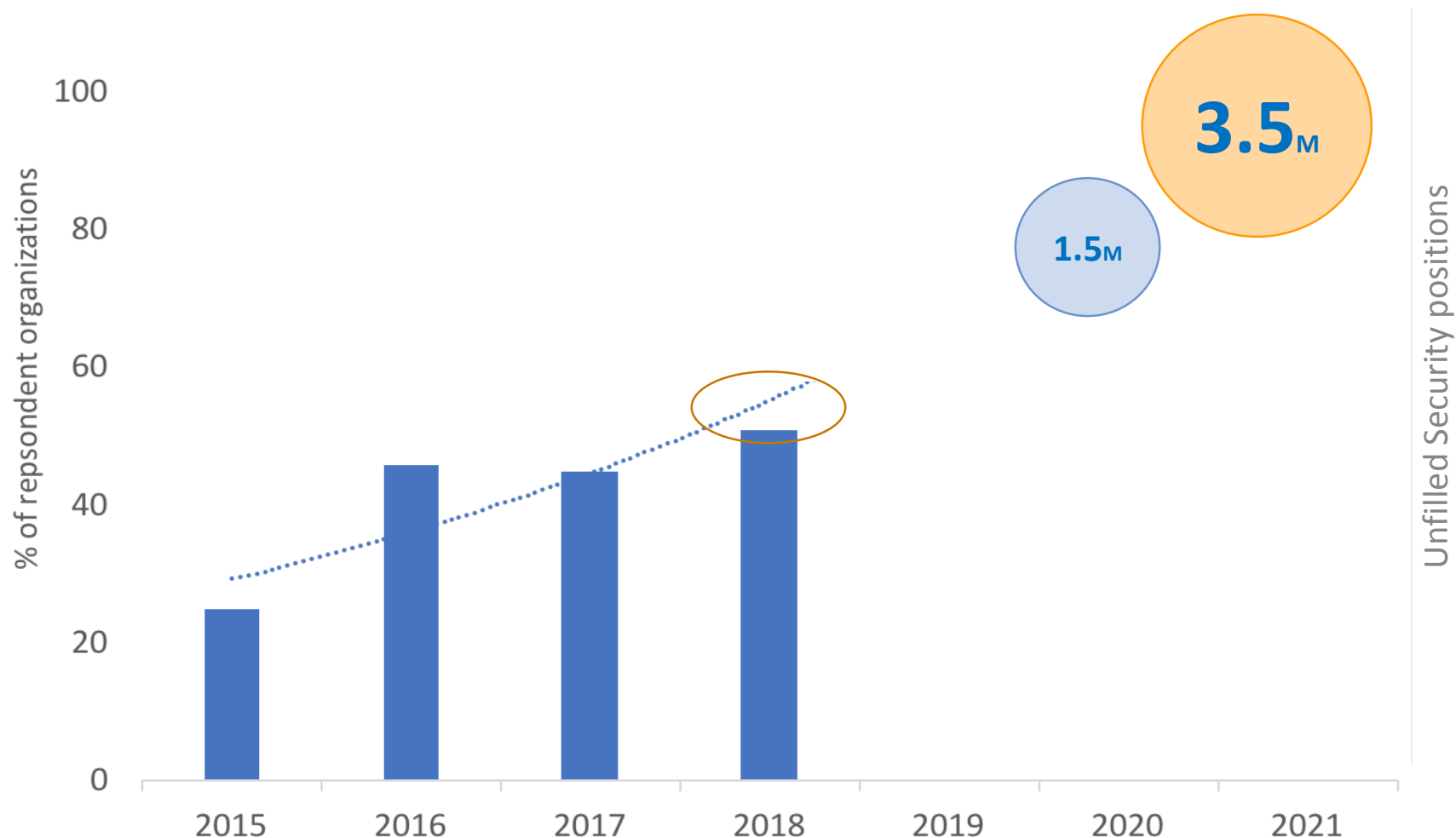
Desired state



Actual state

The Manager – New Concerns Emerge

Cyber Security Skills Shortage



Summary of Problems



Lack of visibility



Too many alerts



Limited expertise



Lack of intelligence



Too many tools

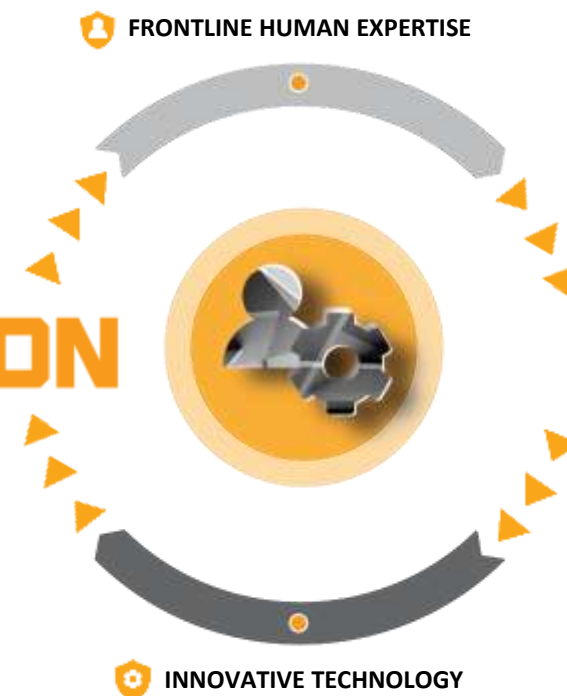


Rising costs

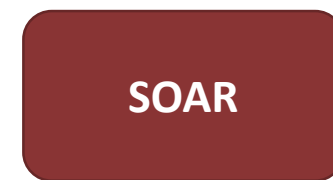
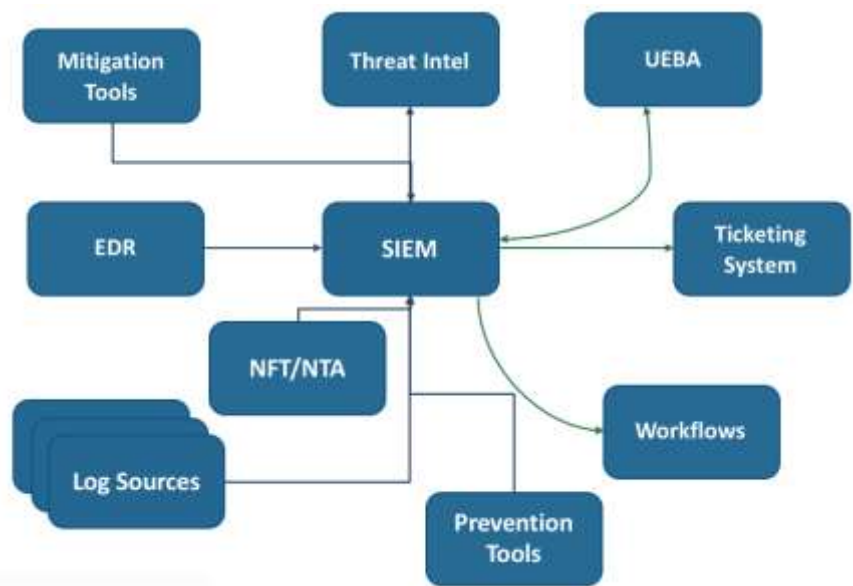
Innovation Cycle Mantra



The FireEye
**INNOVATION
 CYCLE**

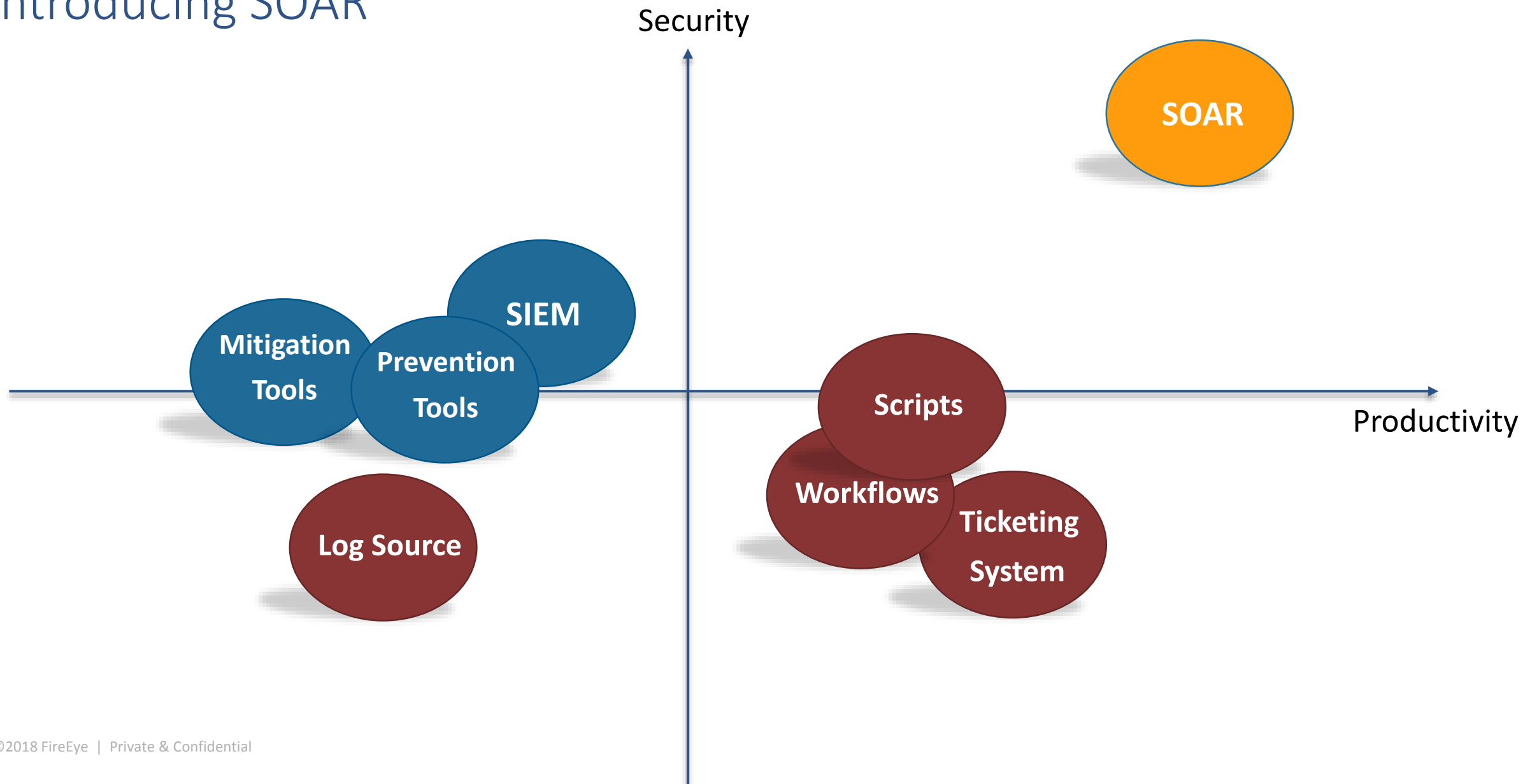


Putting it All Together

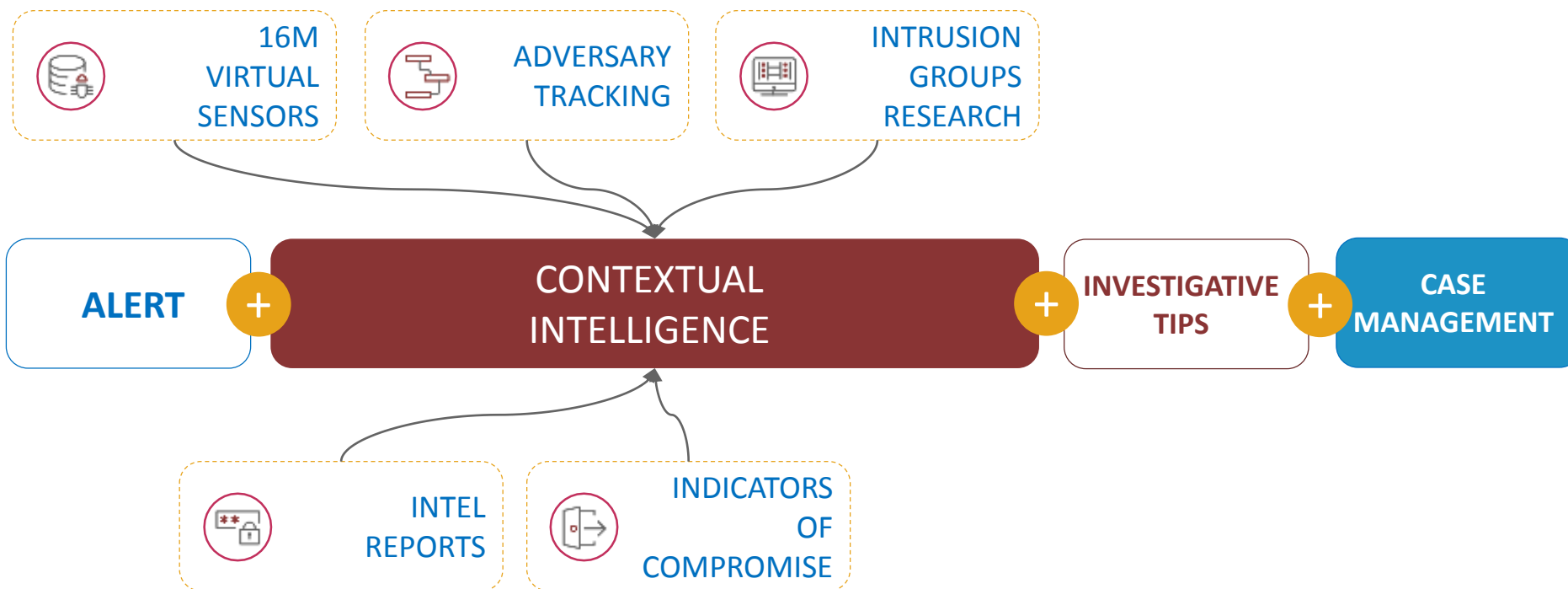
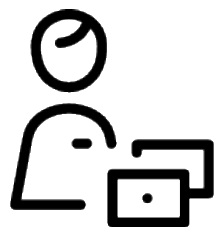


Security
Orchestration
Automation
Response

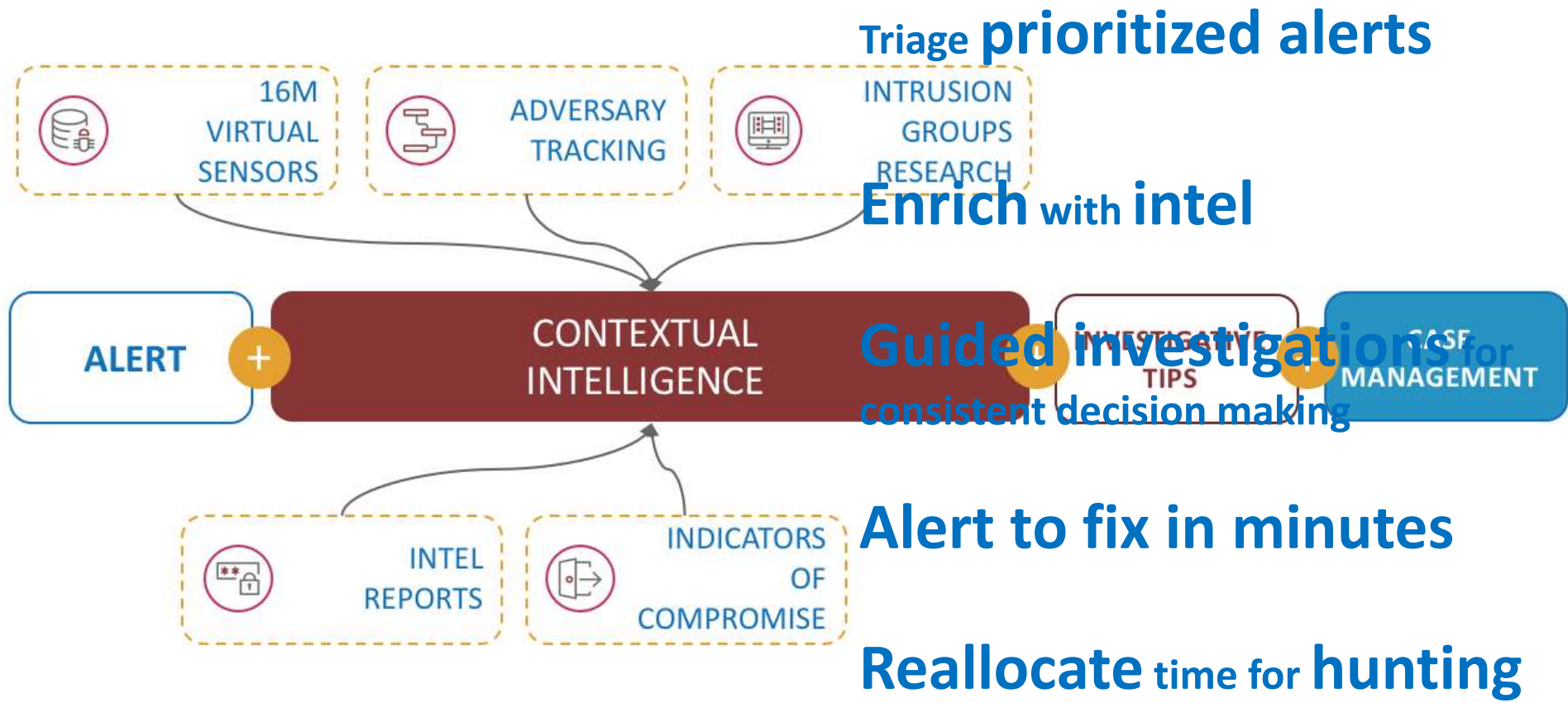
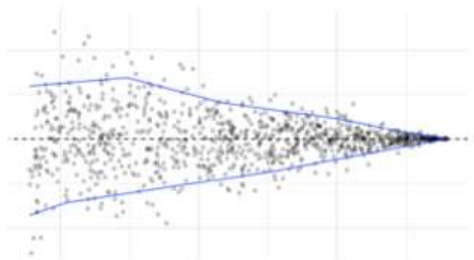
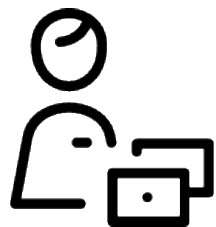
Introducing SOAR



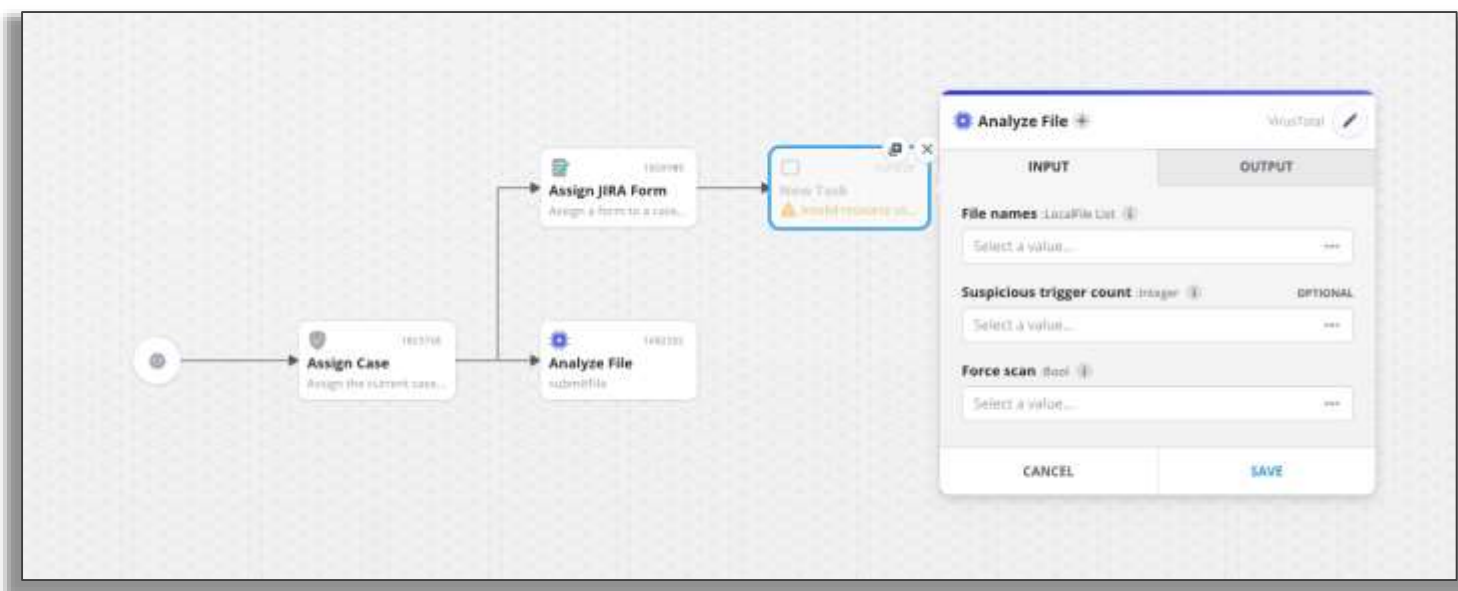
For the Analyst - Enrich Alerts to Derive Context



For the Analyst - Enrich Alerts to Derive Context



For the Engineer – Playbook Automation



Streamline repeatable manual tasks

Standardize knowledge and process management

Increase efficiency and performance of SOC analysts

For the Manager – Integrated SOC Platform



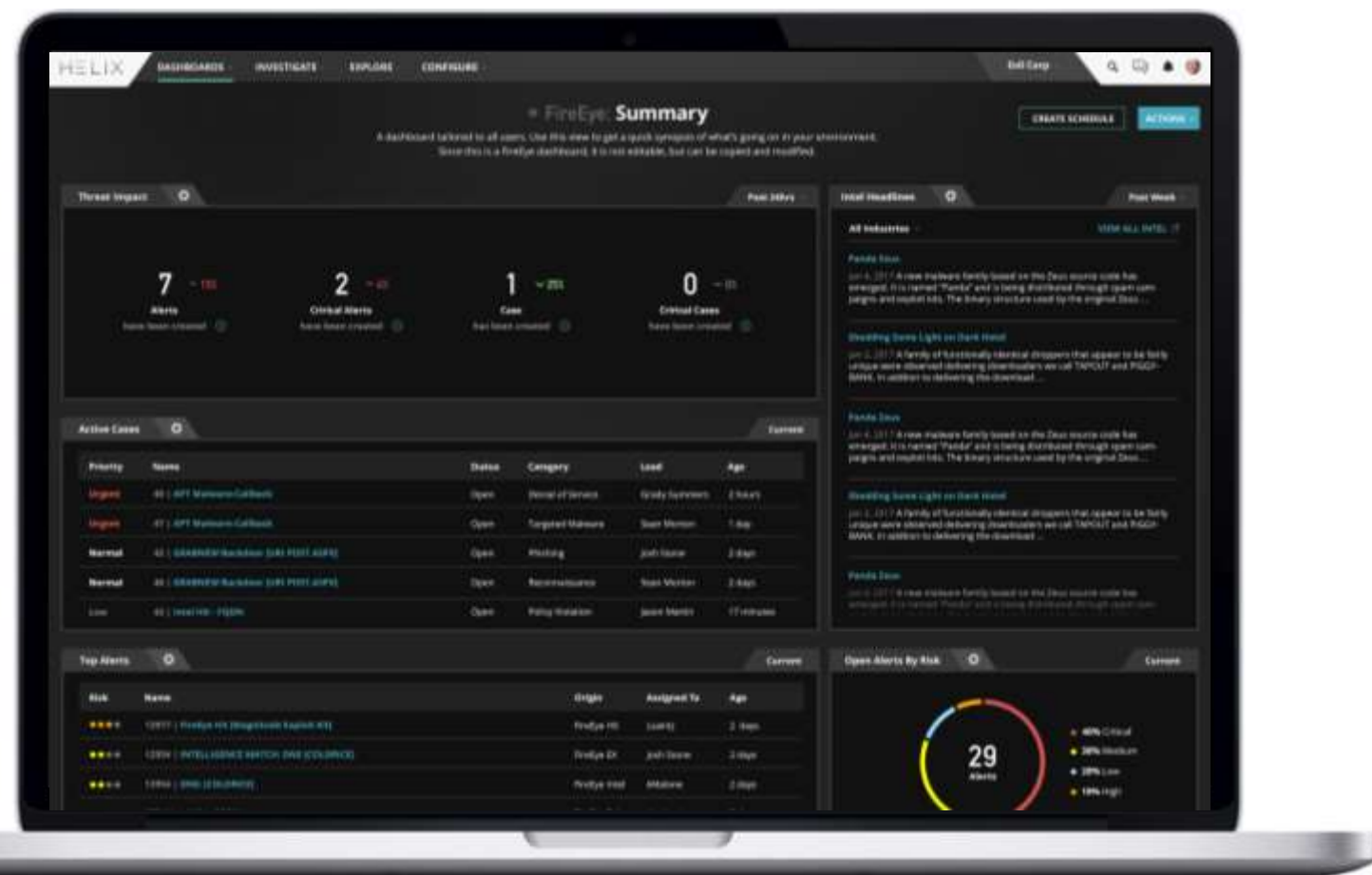
Guided investigations to address skill gap

Playbooks for predictable knowledge management

Tool consolidation via **Automation**

Orchestration for repeatable manual tasks

Dashboards for executive reporting



SOAR to New Heights with HELIX

EXPAND VISIBILITY

Across The Enterprise



INTELLIGENCE MATCHING



ANALYTICS MODULES



3RD PARTY INTEGRATIONS

IMPROVE SPEED

From Alert To Fix



CONTEXTUAL INTELLIGENCE



ORCHESTRATION



INVESTIGATIVE TIPS

STREAMLINE COSTS

Optimize & Consolidate



TOOL CONSOLIDATION



FLEXIBLE DEPLOYMENTS



TEAM EFFICIENCIES



FireEye®

Thank You

SOAR Above Your Legacy Security Operations Center

Shashwath Hegde, CISSP
Solutions Architect, APAC, FireEye