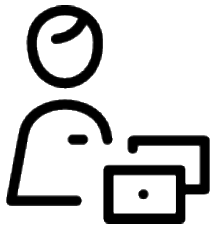
FireEye

SOAR Above Your Legacy Security Operations Center

Anthony Ng (黄献顺)

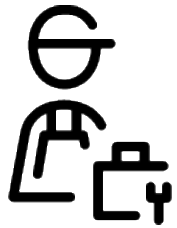
Sr. Director, Systems Engineering

Typical Characters in the SOC



SOC Analyst

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



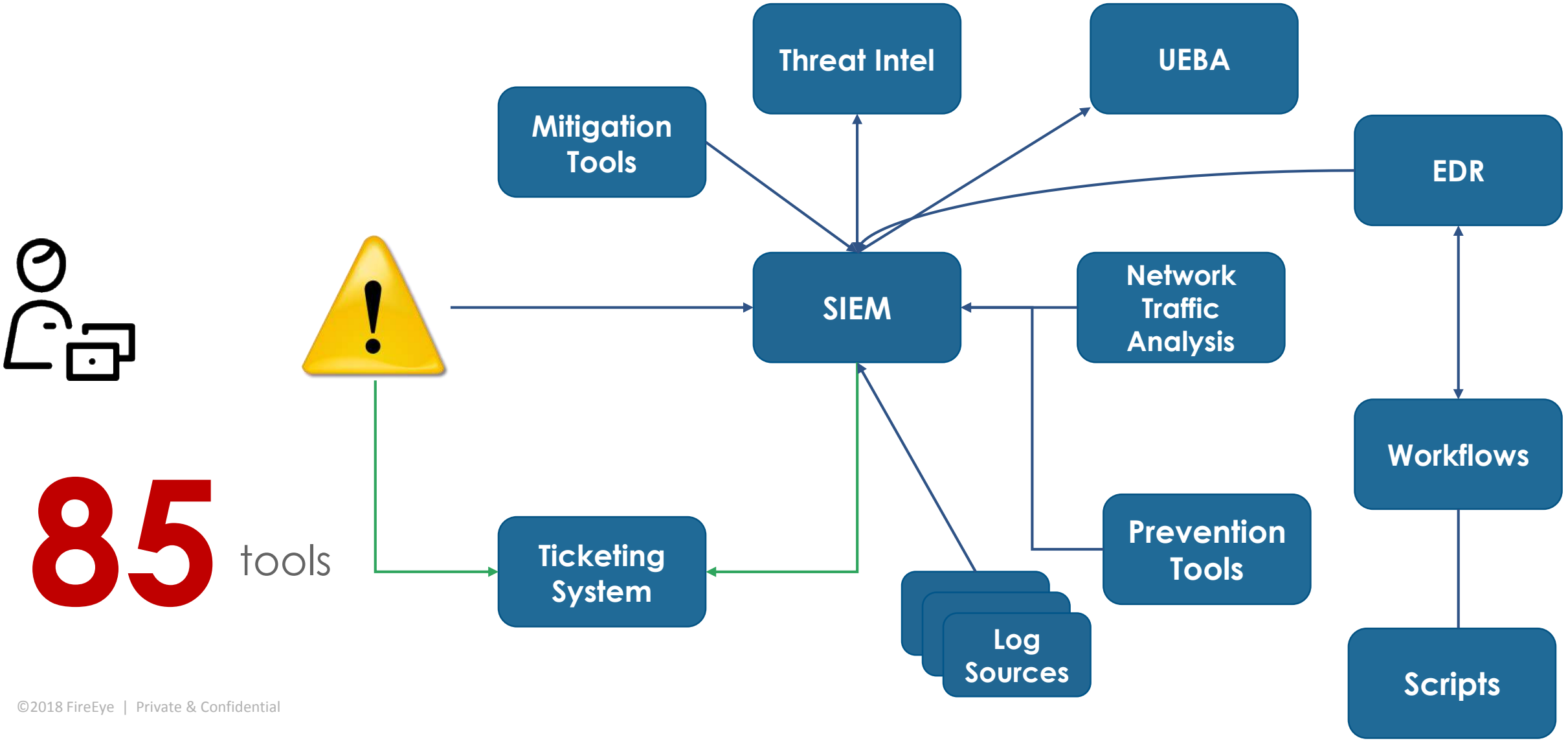
Security Engineer

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



The Analyst's Day – Objectives

Respond in time

Prioritize alerts

Triage alerts quickly

add **Contextual Intel**

Notify stakeholders

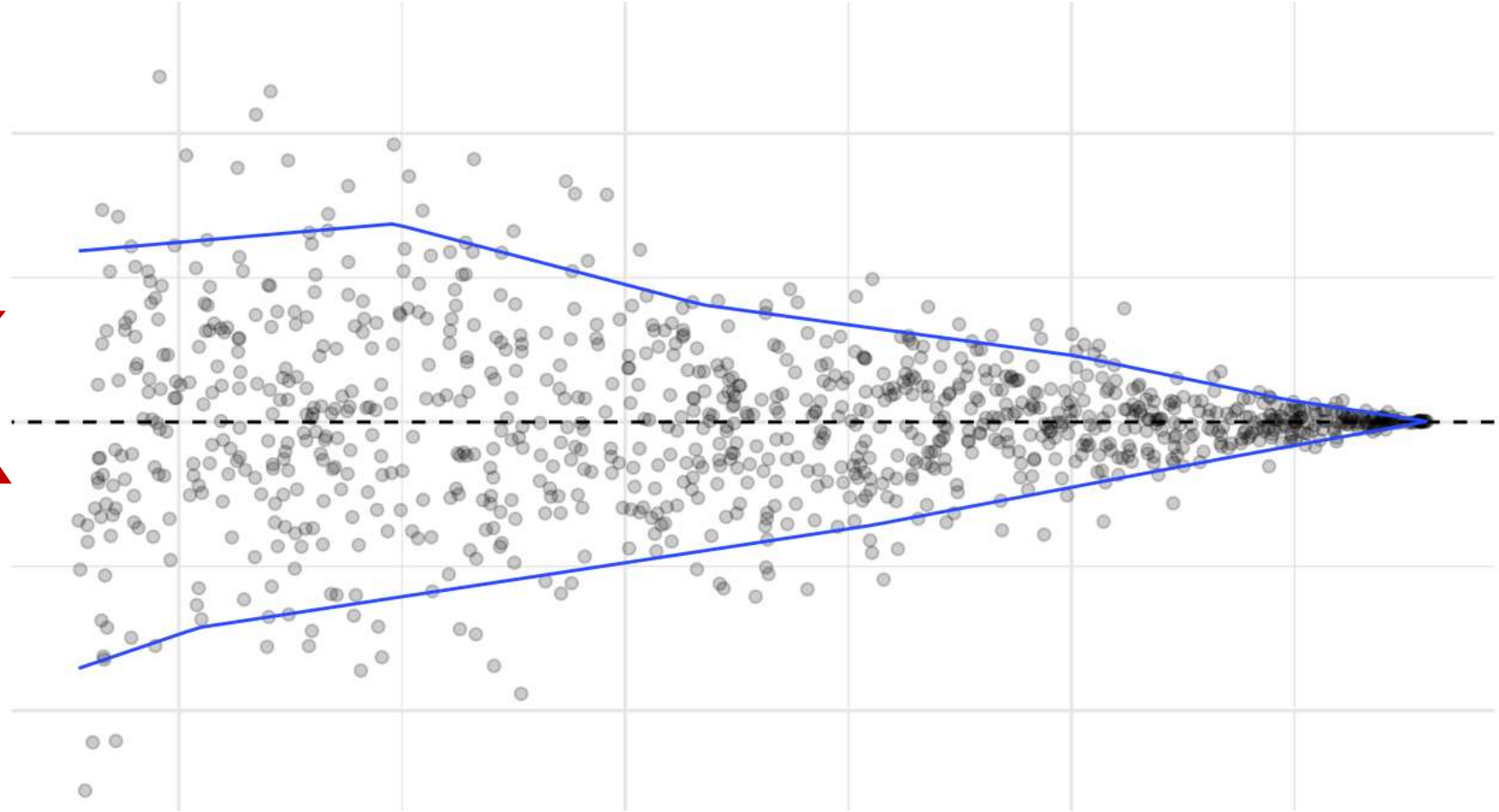
SLA to be met

Report incidents

10K alerts/day

The Analyst's Day – Relevancy and Quality of Alerts

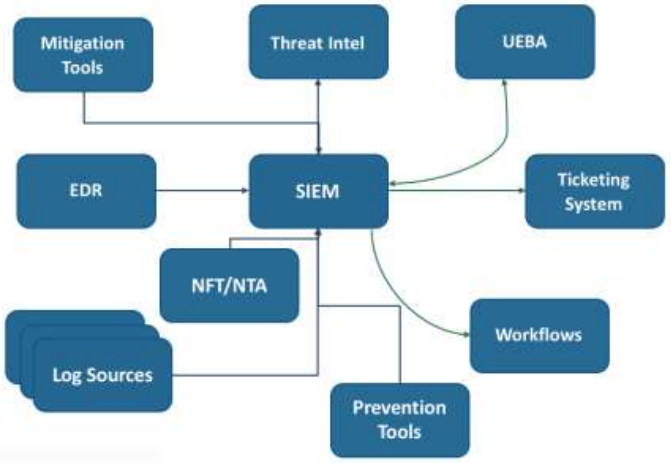
10K
alerts/day

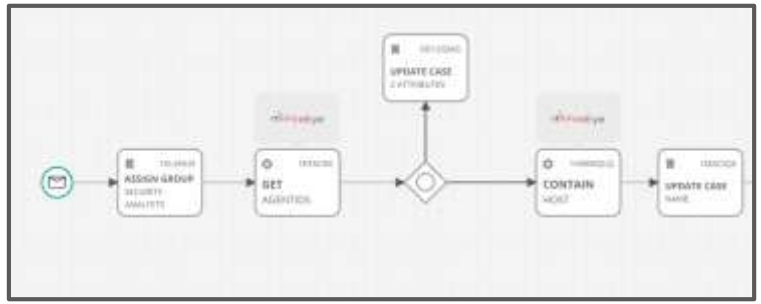


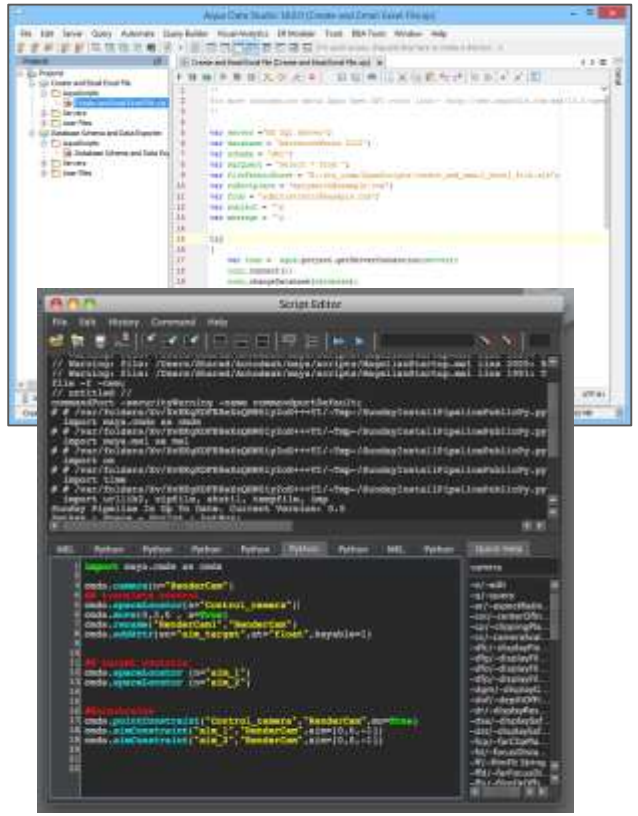
Only Few Alerts Matter

 Source: Heteroscedastic Variance

The Engineer's Day – Simplify Workflows



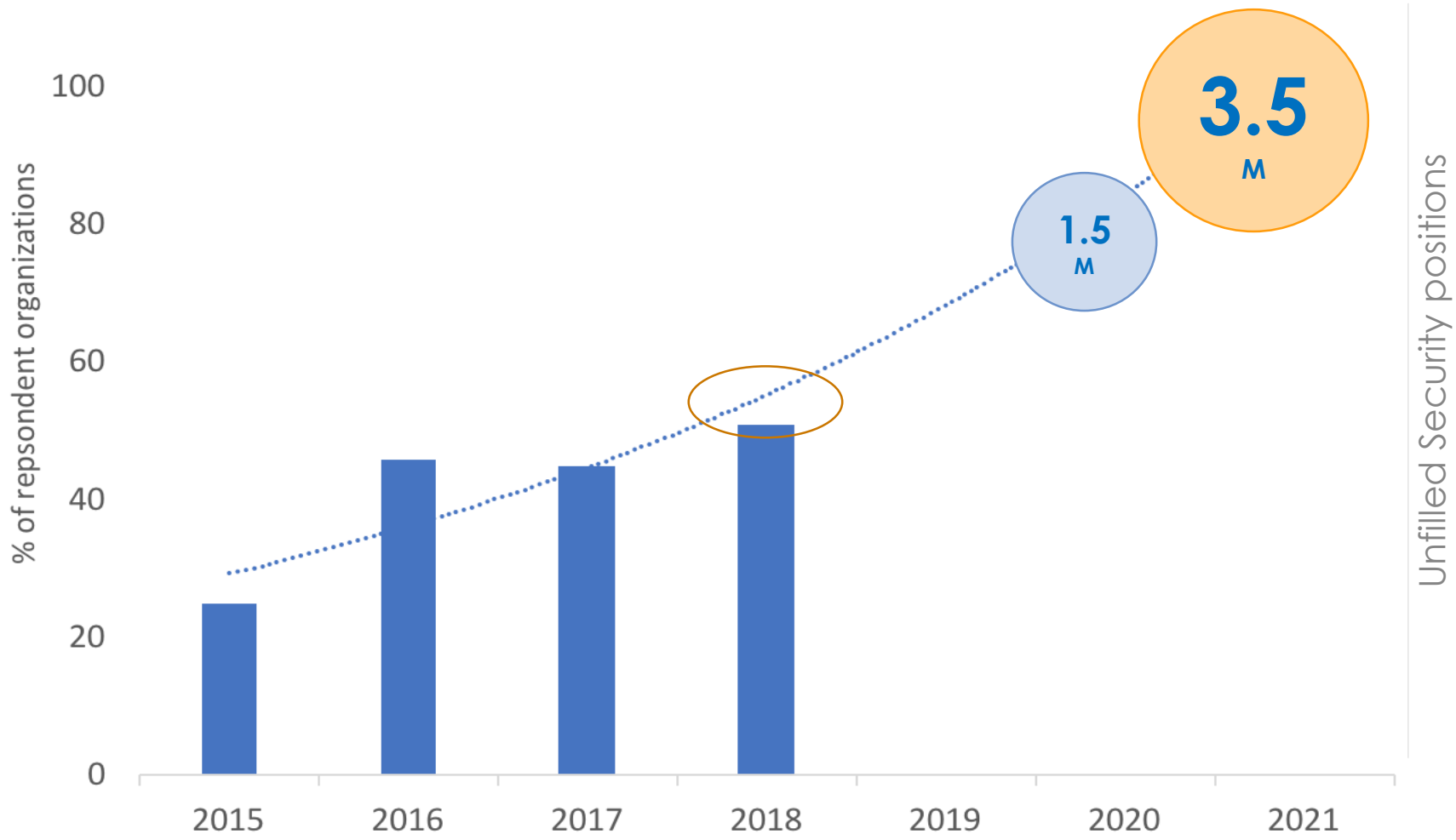




Current state **Desired state** **Actual state**

The Manager – New Concerns Emerge

Cyber Security Skills Shortage



Source: https://cybersecurityventures.com/jobs/

Source: https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html

Summary of Problems

Lack of visibility

Too many alerts

Limited expertise

Lack of intelligence

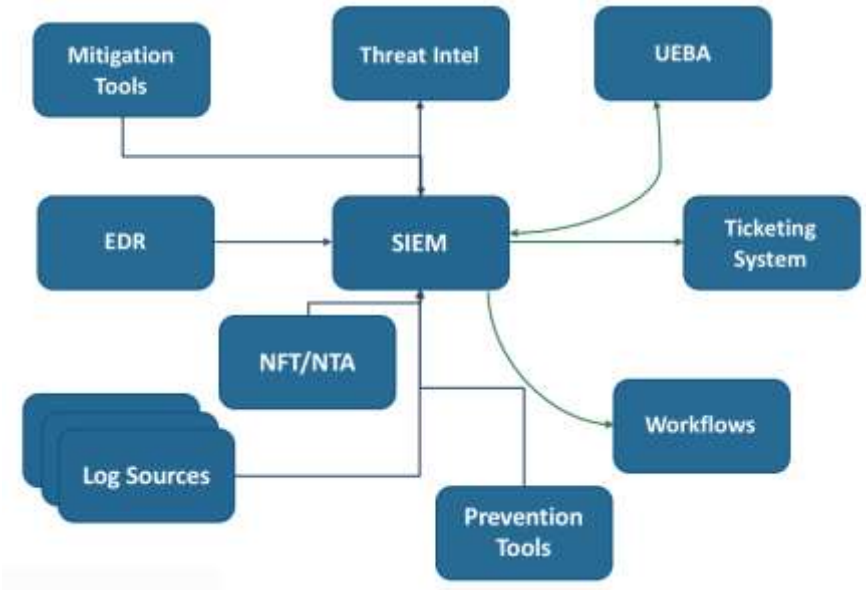
Too many tools

Rising costs

Innovation Cycle Mantra

The FireEye
INNOVATION
CYCLE

Putting it All Together

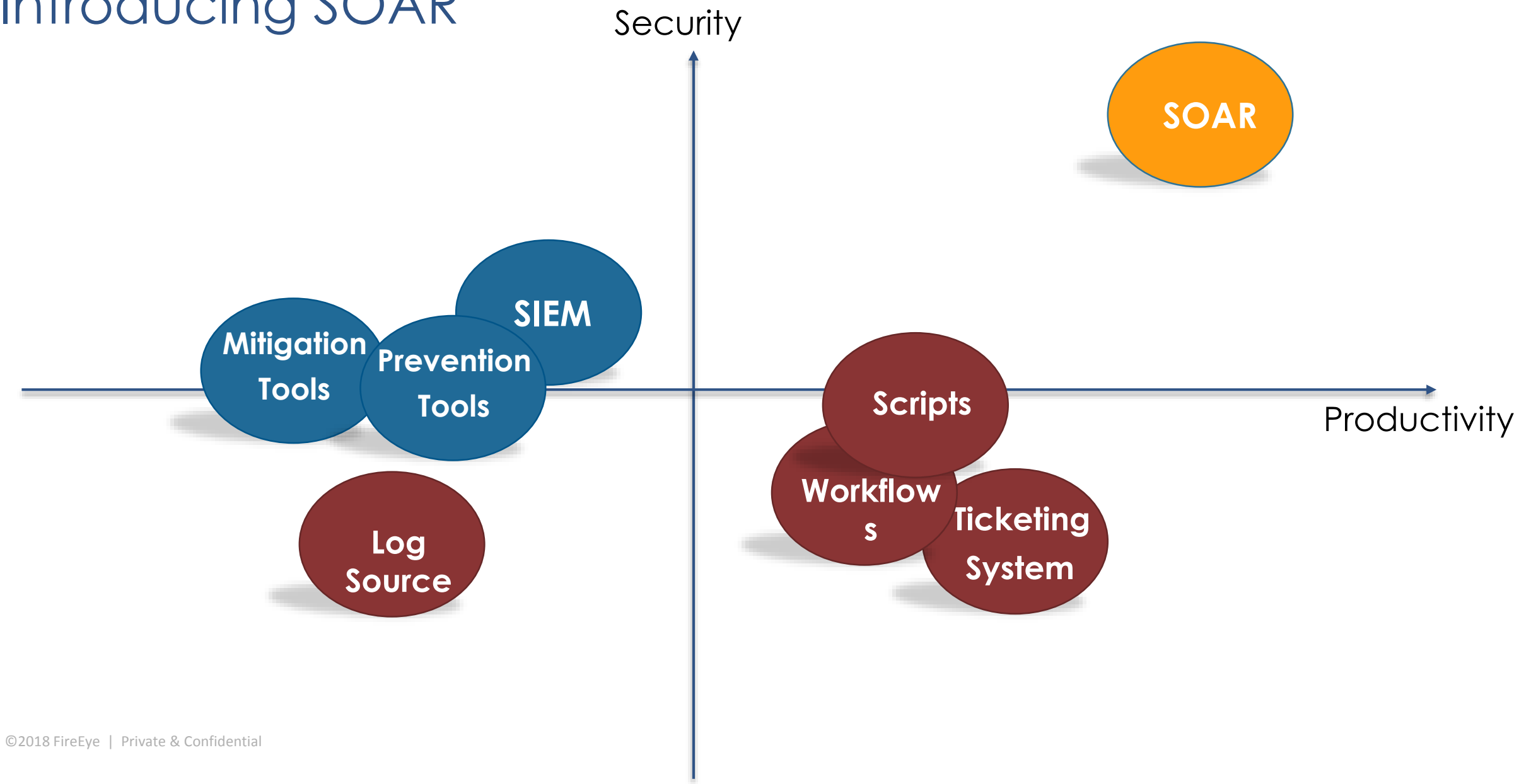


HELIX

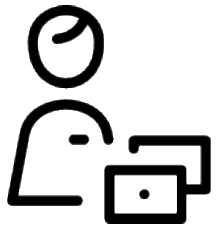
SOAR

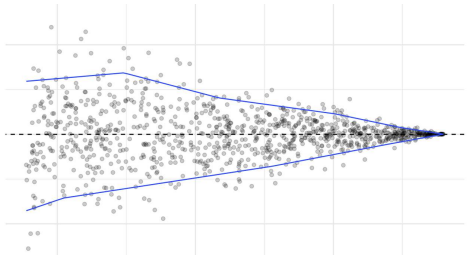
Security Orchestration Automation Response

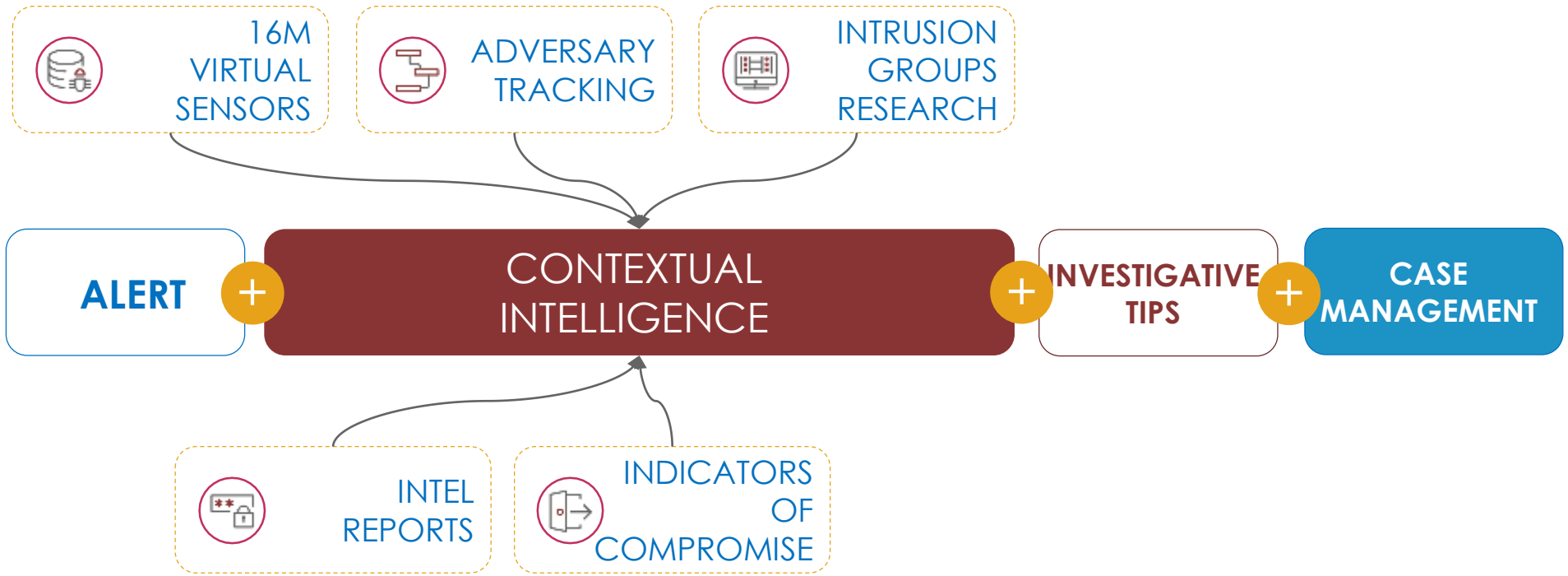
Introducing SOAR



For the Analyst - Enrich Alerts to Derive Context

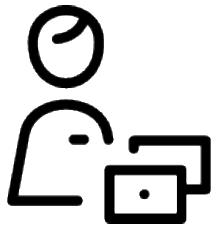






HELIX

For the Analyst - Enrich Alerts to Derive Context



Triage prioritized alerts

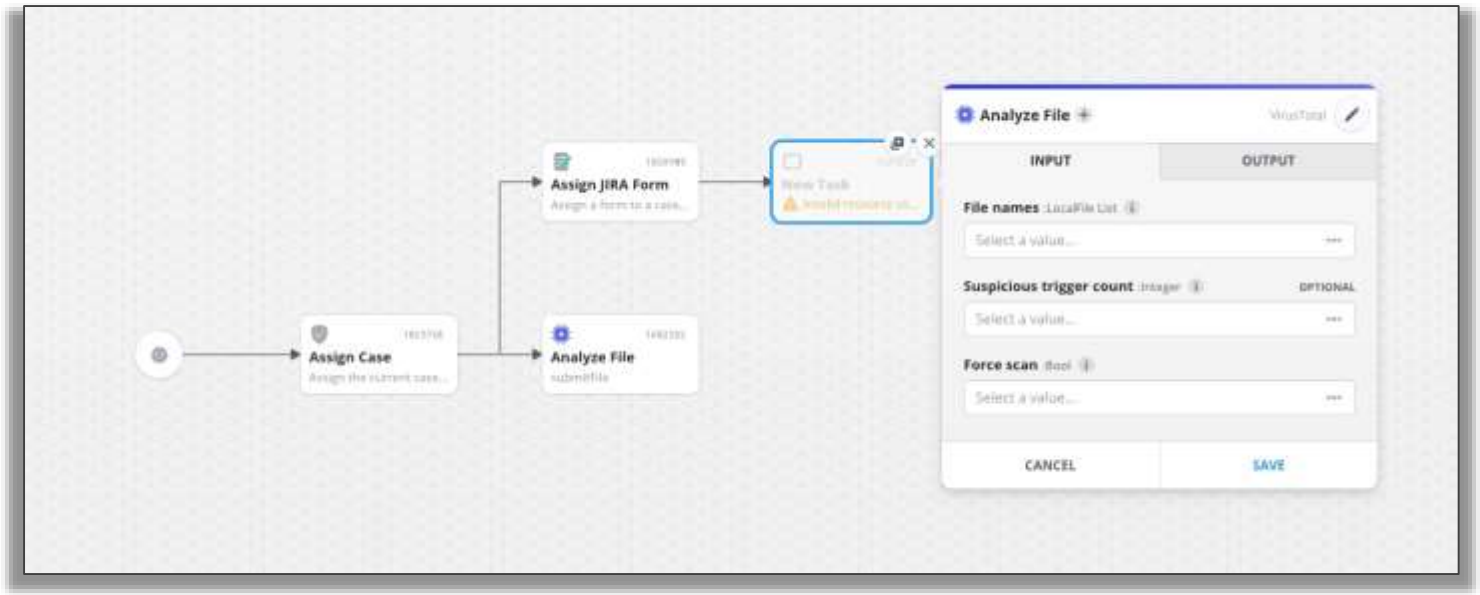
Enrich with intel

Guided investigations for consistent decision making

Alert to fix in minutes

Reallocate time for hunting

For the Engineer – Playbook Automation



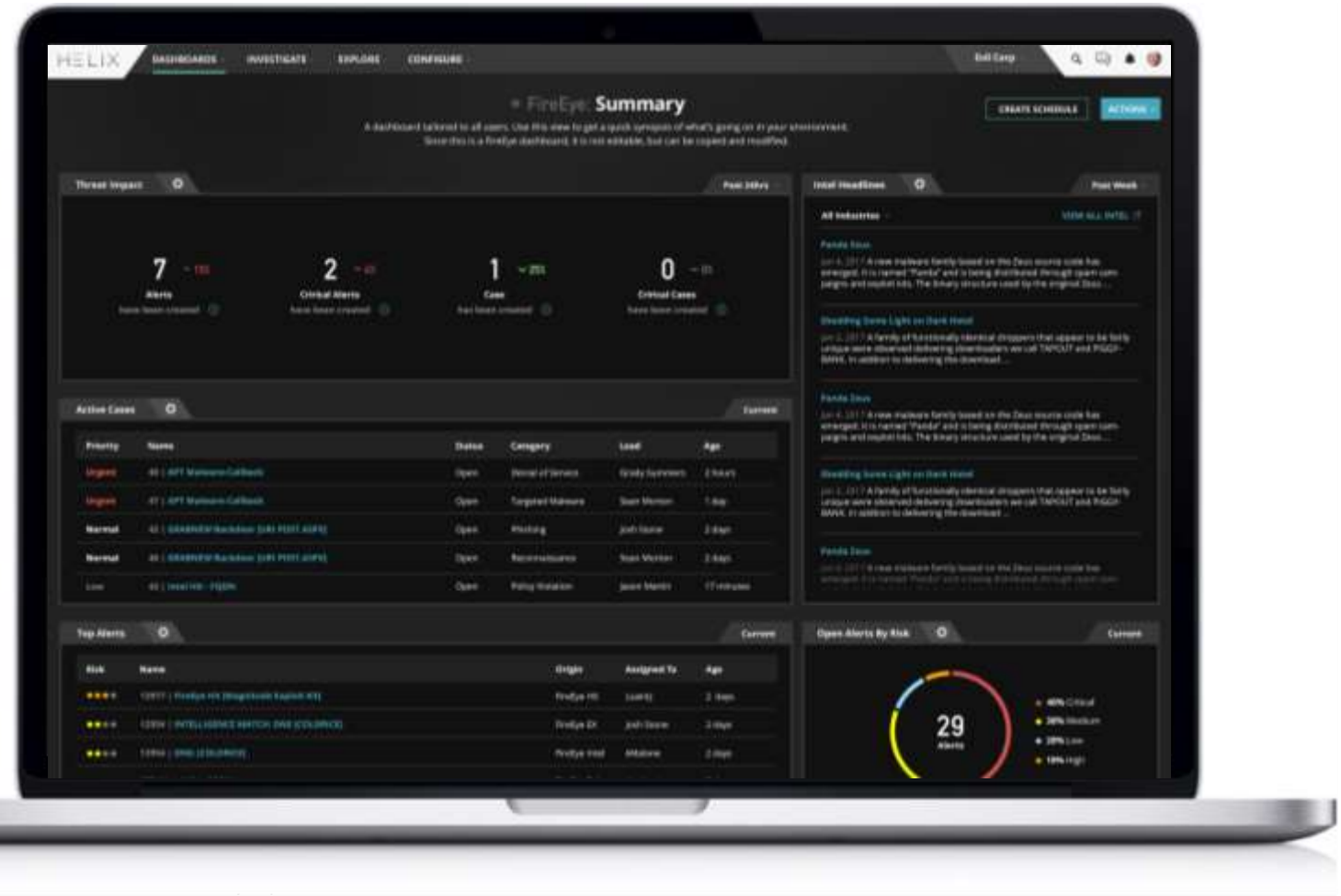
Streamline repeatable manual tasks

Standardize knowledge and process management

Increase efficiency and performance of SOC analysts

HELIX

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

HELIX

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