

Cyber Security Orchestration, Automation and Response



Unify Security Operations, Incident Management, Security Technology Unison
and Orchestrate Automated Responses in Real-Time

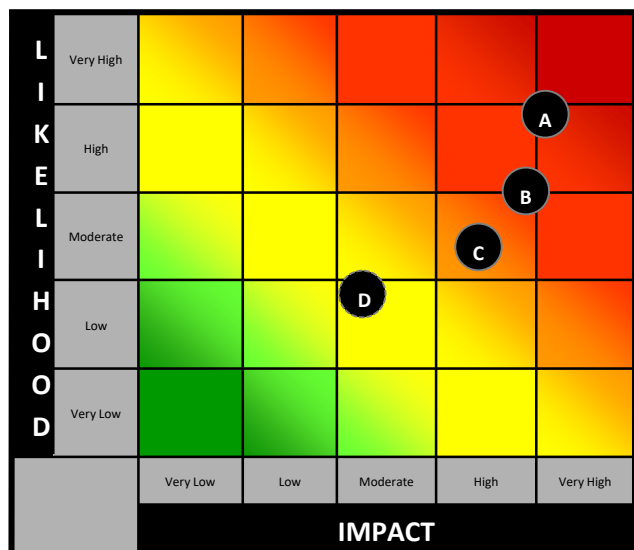
“It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.”

— Stephane Nappo

Sector threat profile

Insurance Services – Executive Summary

Insurers possess highly valuable, easily monetized data

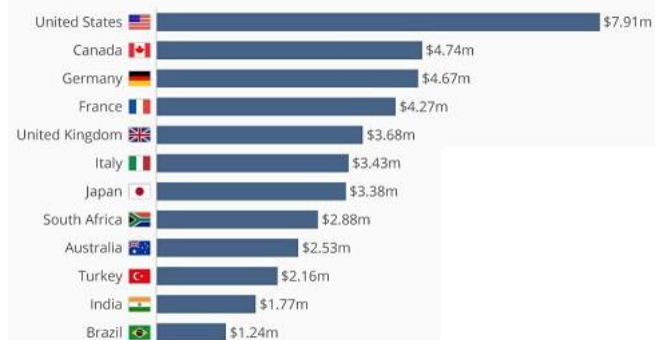


Prioritized Threat Actors

A: Cyber-criminals | B: Nation states
C: Insider threats | D: Hacktivists

Average Cost Of A Data Breach

Average total cost of a data breach by country in 2018



Growing threat to insurers

“Insurers are prime targets to be victimized given the riches of data – credit card information, medical information, and other underwriting information. It’s **not a matter of ‘if’ but ‘when’ it will happen.**”

- Computing.com

Breaches can have lasting effects

“It is easy for organizations to be reactive to cyber events and say “it will never happen to us,” but when the event does happen, it is **costly in both financial and reputational terms.** This **can directly affect the solvency of the organization** by loss of customers, share price and a potential rating downgrade..”

- EY’s publication on mitigating cyber risk for insurers

Disruptive technologies

“Make no mistake, the internet of things (IoT) **will present staunch challenges** for the insurance industry”

- Kevin Kalinich, global cyber risk practice leader, Risk & Insurance

Insurance data is valuable

“Insurance companies hold significantly more consumer data than ever, making them an **attractive target for cyberattacks.**”

- CSC Technologies

A target on multiple fronts

“Not only is the insurance sector suffering from [cyber] threats, but **insurance companies are apparently also facing threats from their competitors in the industry**, who are going after their data in **commercial espionage**, employing hacking techniques.”

- The Independent, UK

Increased federal scrutiny

Recent cyber security breaches at financial institutions and other major corporations should serve as a **wake up call for insurers to redouble their efforts to strengthen their cyber defenses** – particularly given the level of sensitive consumer information that insurers are entrusted with handling.

- New York State Department of Financial Services, *Report on Cyber Security in the Insurance Sector*

Open Source Statements

According to EY's Information Security survey:



of respondents believe their cybersecurity approach is fully meeting needs

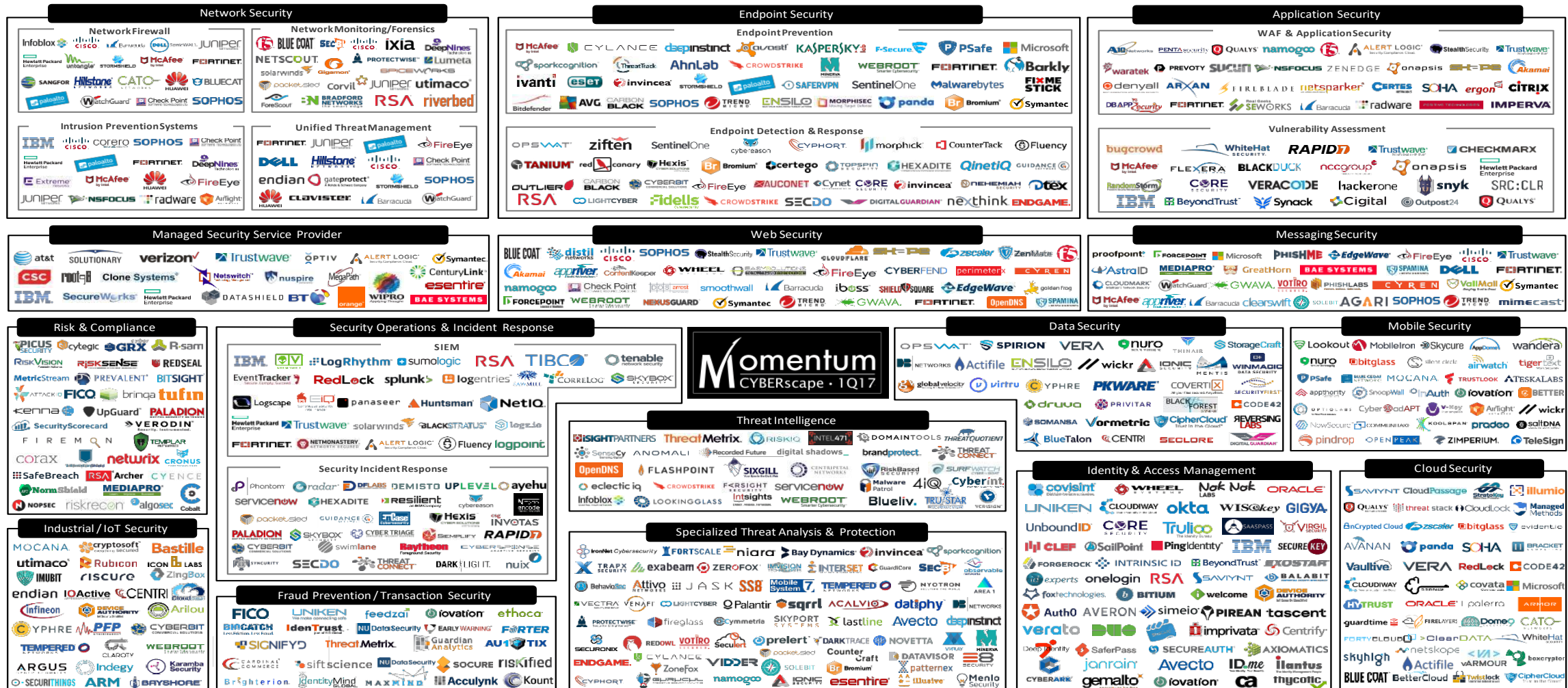


discovered "significant" incidents within their organization



did not think it was "very likely" they would be able to detect a sophisticated attack

To manage the threats, there are now over 500 discrete vendors who are providing some form of security technology



Source: <https://momentumcyber.com/docs/CYBERScape.pdf>

Security Challenges

The increase in security technologies while independently beneficial, may also impose a number of challenges



Resources

Resource *shortage* of 1 million security professionals



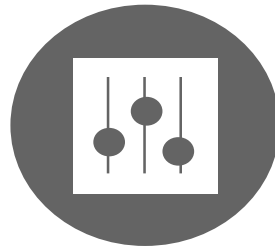
Products

Endless assembly line of point products



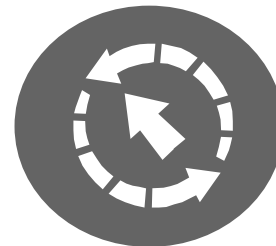
Alerts

Escalating volume of *security alerts*



Static

Static independent controls with *no orchestration*



Speed

Time taken to contain incident still exceeding time taken to compromise



Costs

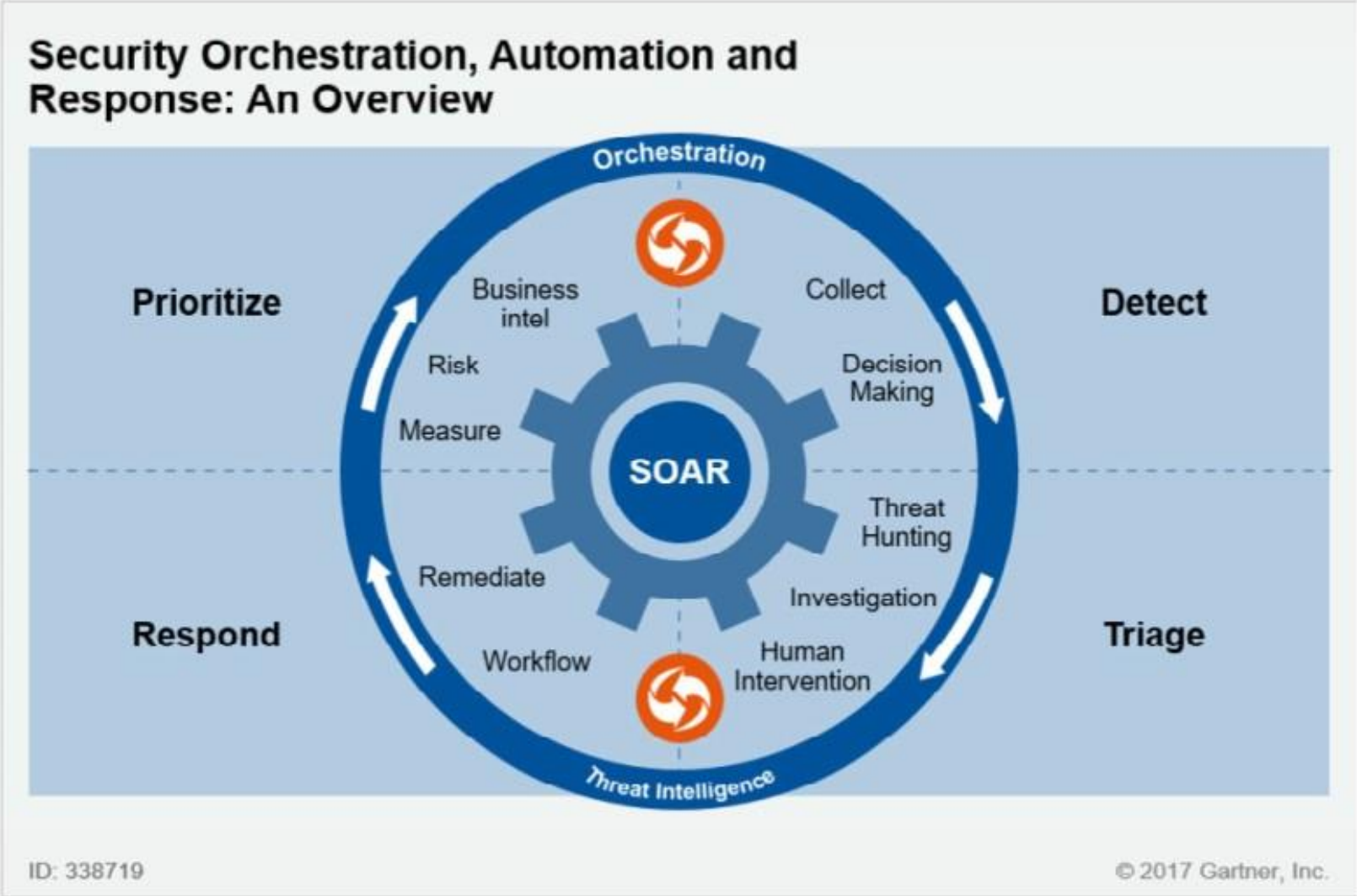
Costs *continue to increase*

The Role of Security Orchestration and Automation



Enter SOAR : Security Orchestration, Automation and Response

SOAR Overview



Description and Functional Components

Orchestration — How different technologies (both security-specific and non-security-specific) are integrated to work together

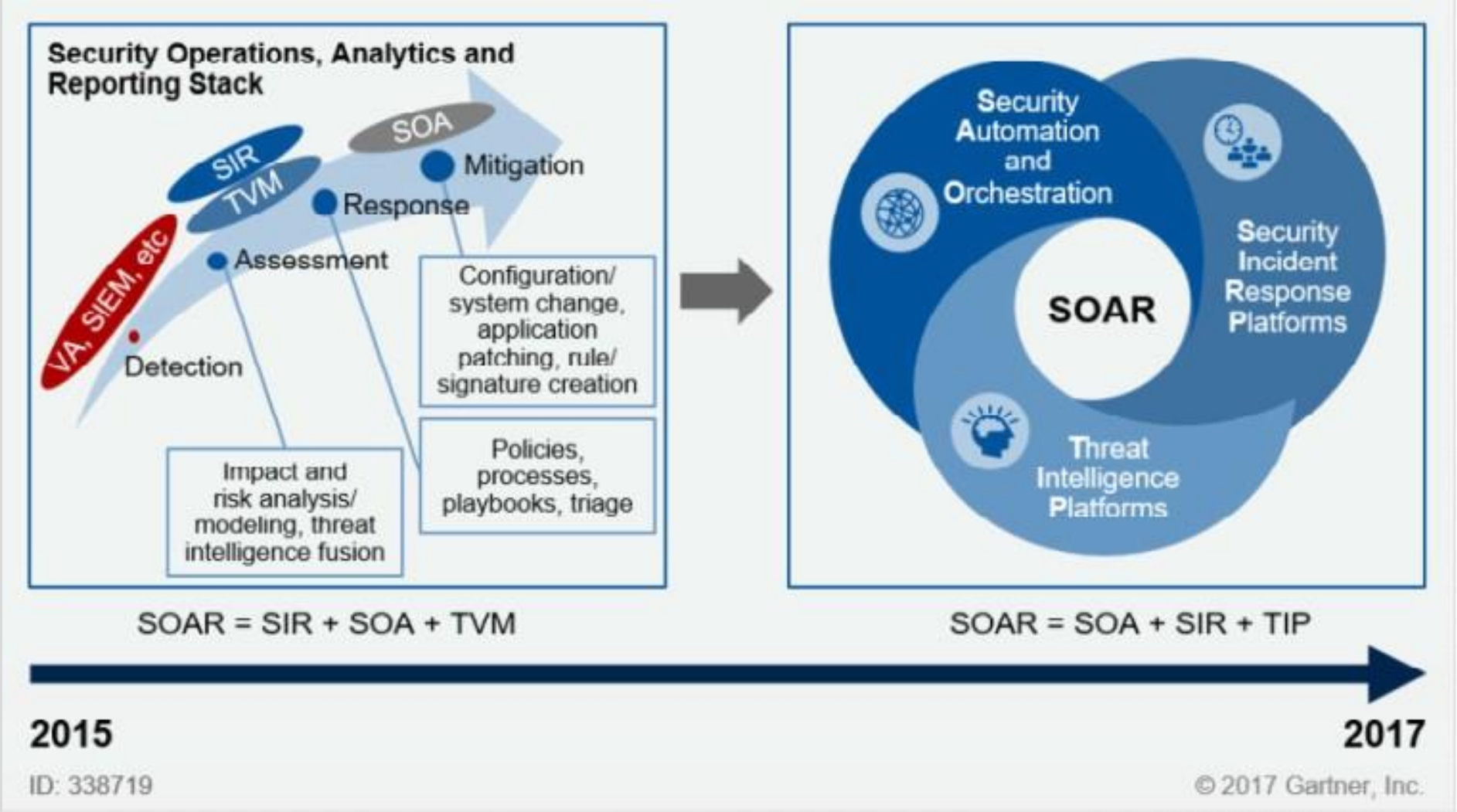
Automation — How to make machines do task-oriented "human work"

Incident management and collaboration — End-to-end management of an incident by people

Dashboards and reporting — Visualizations and capabilities for collecting and reporting on metrics and other information

Enter SOAR : Security Orchestration, Automation and Response

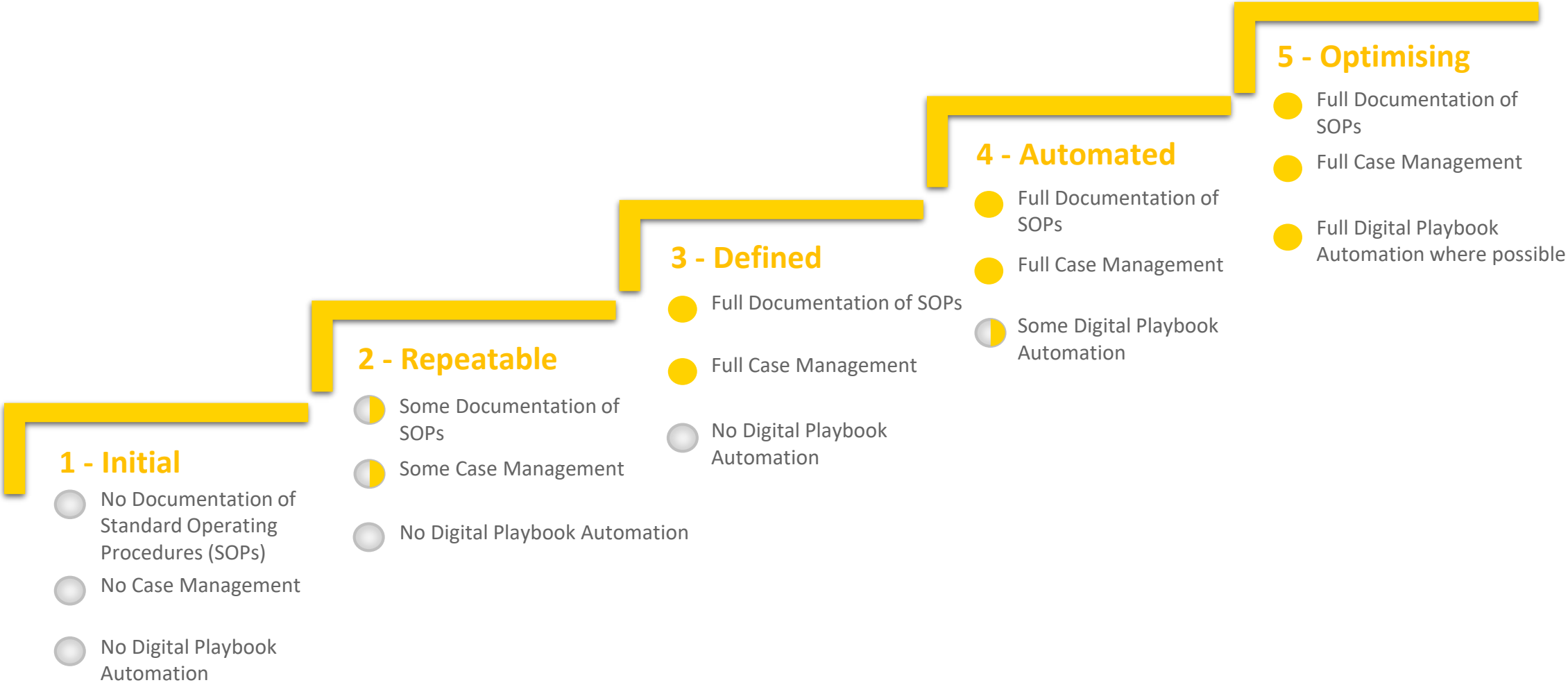
Convergence of SOAR Tools



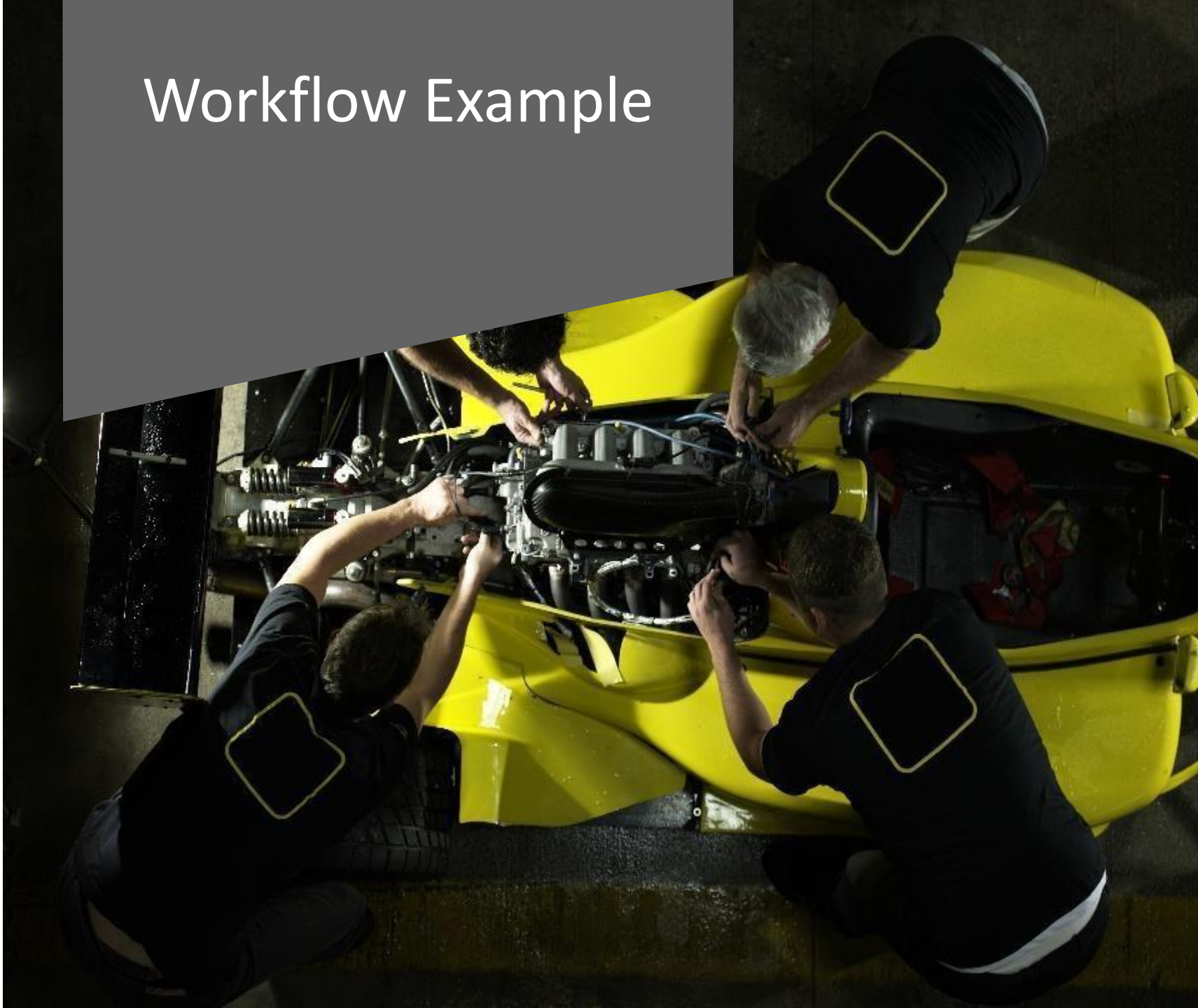
Source: Gartner (November 2017)

SOAR Benefits

Improving Security Ops Maturity

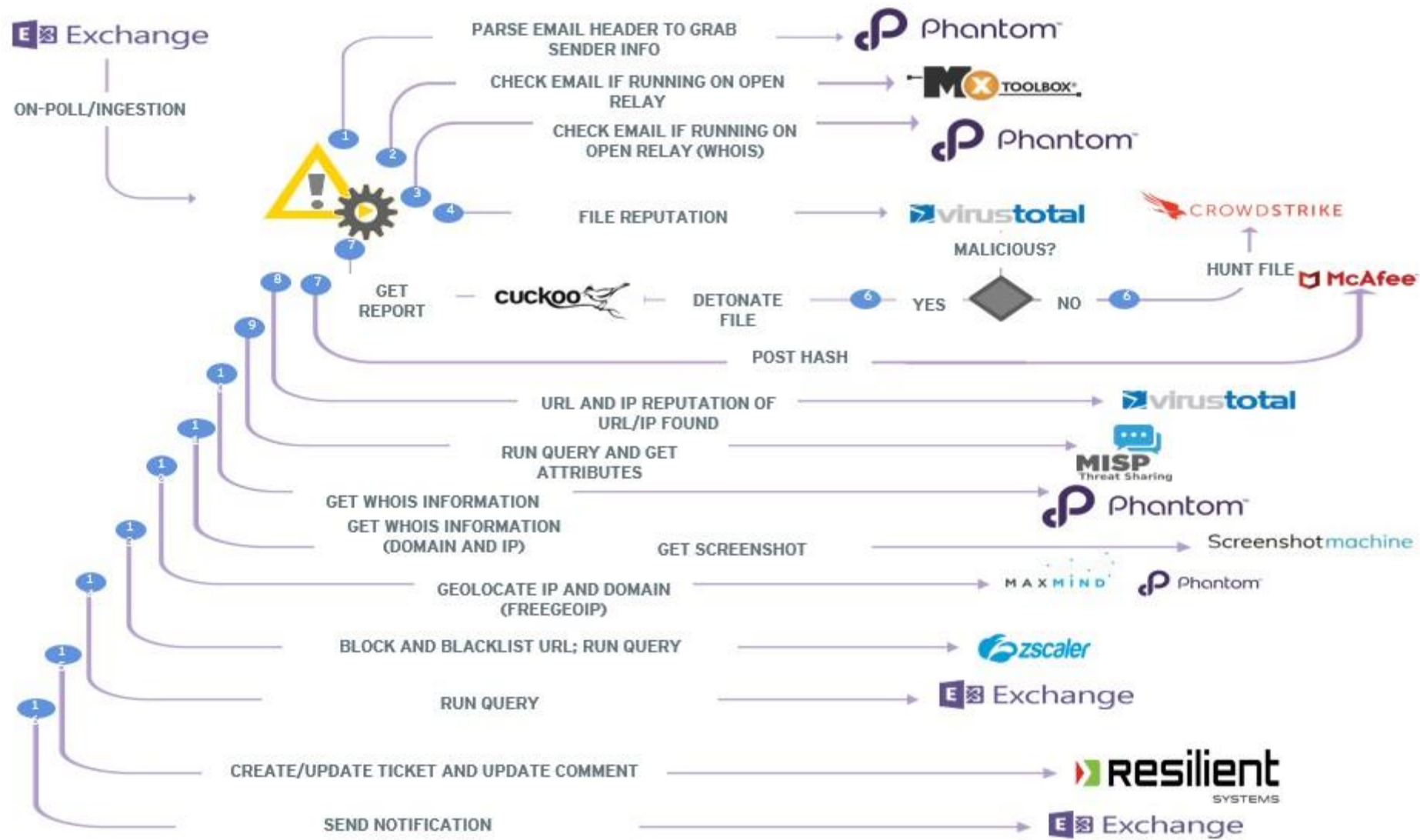


Workflow Example



Phishing Use Case

Automated workflow



Benefits Realization

Measuring your ROI

TABLE 1: Cost to Process Suspected Phishing Emails	
Key Data	
Number of Suspected Phishing Emails / Day	45
Estimated Time Required to Manually Process Each Suspected Phishing Email	90 Minutes
Average Hourly Salary: Tier-1 SOC Analyst ¹	\$39.65
Computations	
Daily Cost to Process Suspected Phishing Emails	\$2,676
Annual Cost to Process Suspected Phishing Emails ²	\$695,760

Source: Measuring the economic impact of Security Automation and Orchestration

Measuring your ROI

TABLE 2: Cost to Process Suspected Phishing Emails with Burst Activity	
Key Data	
Number of Suspected Phishing Emails / Day – Normal Conditions	45
Number of Additional Suspected Phishing Emails / Day – Burst Attack	255
Estimated Time Required to Manually Process Each Suspected Phishing Email	90 minutes
Average Hourly Salary: Tier 1 SOC Analyst ¹	\$39.65
Computations	
Daily Cost to Process Additional Suspected Phishing Emails – Burst Attack	\$15,171
Annual Cost to Process Suspected Phishing Emails – Burst Attack ³	\$363,984
Annual Cost to Process Suspected Phishing Emails – Normal Conditions ⁴	\$695,815
Total Annual Cost to Process Suspected Phishing Emails	\$1,059,744

¹ Source: https://www.glassdoor.com/Salaries/security-analyst-salary-SRCH_KO0,16.htm

² Five-day work week assumed.

³ Two burst attacks per month assumed.

⁴ From Table 1

Case Study: Insurer ROI

SOAR Implementation

Technology Integrations	Use Cases	Cost and Productivity Savings
Email	<ul style="list-style-type: none">▶ Automated email ingestion from various sources: Phishing mailbox, MSSP and CrowdStrike▶ Email communication triggered from Resilient through Phantom▶ Customised templates and recipients	<div>US\$1m</div> <div>Dollars saved (annual cost)</div>
Ticketing System	<ul style="list-style-type: none">▶ Automated polling and parsing of tickets▶ Ticket creation in ServiceNow triggered from Resilient through Phantom	<div>US\$72k</div> <div>Dollars saved (annual cost)</div>
EDR	<ul style="list-style-type: none">▶ IOC alerts automatically assigned to Incident Response team▶ CrowdStrike scenario ingestion▶ Host Status check in CrowdStrike using Phantom playbook	<div>US\$72k</div> <div>Dollars saved (annual cost)</div>
SIEM	<ul style="list-style-type: none">▶ Instantly escalate QRadar events to IBM Resilient to invoke response workflows, enrichment and remediation actions▶ Prepopulated incident ticket with information from the QRadar offense	Single pane of glass dashboard to access current data easy and fast

“My message for companies that think they haven’t been attacked is: “You’re not looking hard enough”.

– James Snook