

Security Orchestration & Automated Response

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



AGENDA

- 01. The Evolution of Security Orchestration and Automation
- 02. The Implementation Approach
- 03. Example Workflow
- 04. Value Delivered



Cyber Security
Orchestration &
Automation Platform

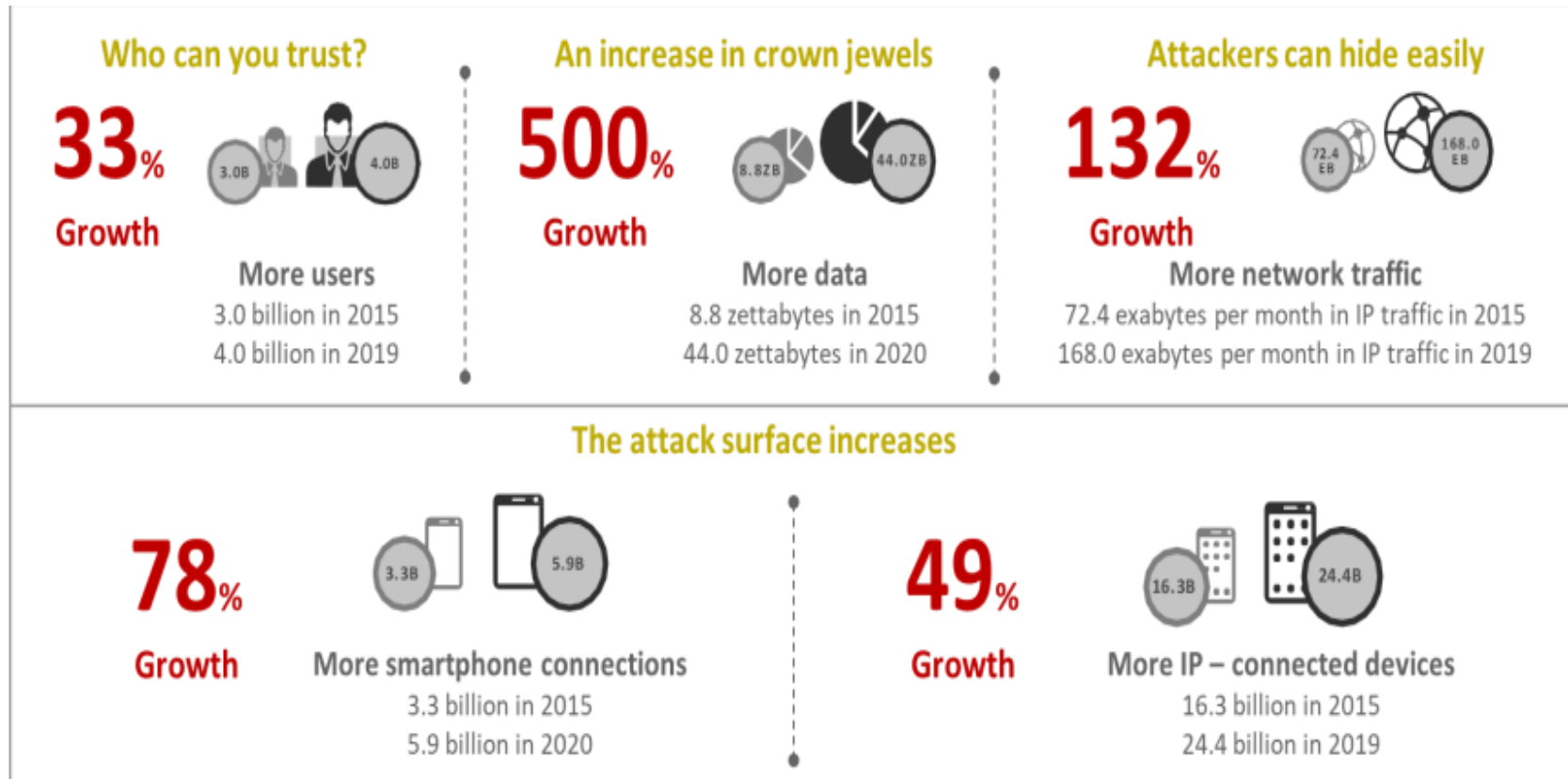
01

The Evolution of Security Orchestration and Automation

Understanding the problem

Manual security operations is increasingly becoming expensive and ineffective as the number of alerts are exponentially growing given the scale of digital transformation, accelerated volume of new threats and global wide shortage of cyber security specialists.

1. Digital Transformation is changing the technology landscape in unprecedented ways

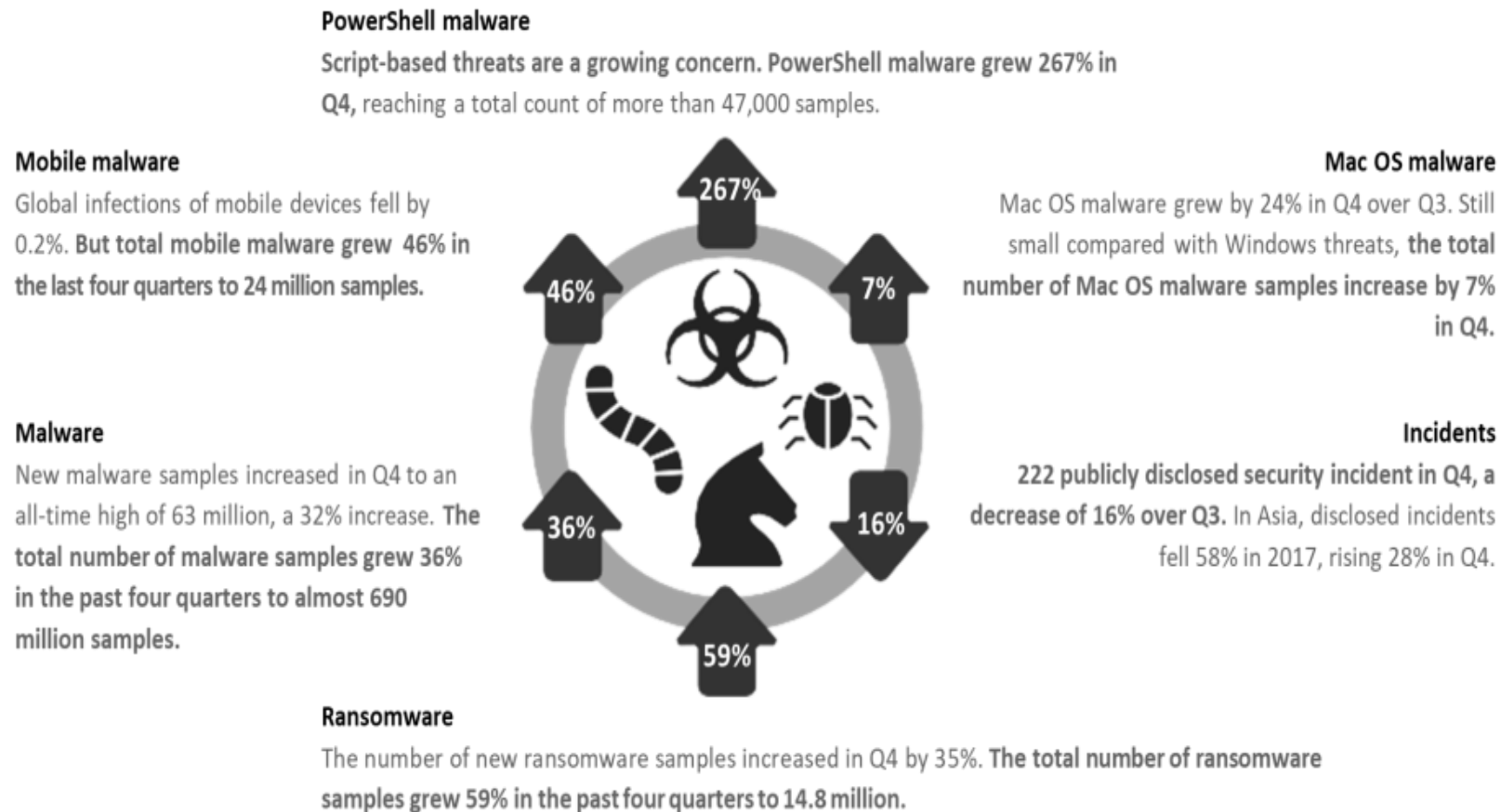


Source: ISACA

Understanding the problem

Manual security operations is increasingly becoming expensive and ineffective as the number of alerts are exponentially growing given the scale of digital transformation, accelerated volume of new threats and global wide shortage of cyber security specialists.

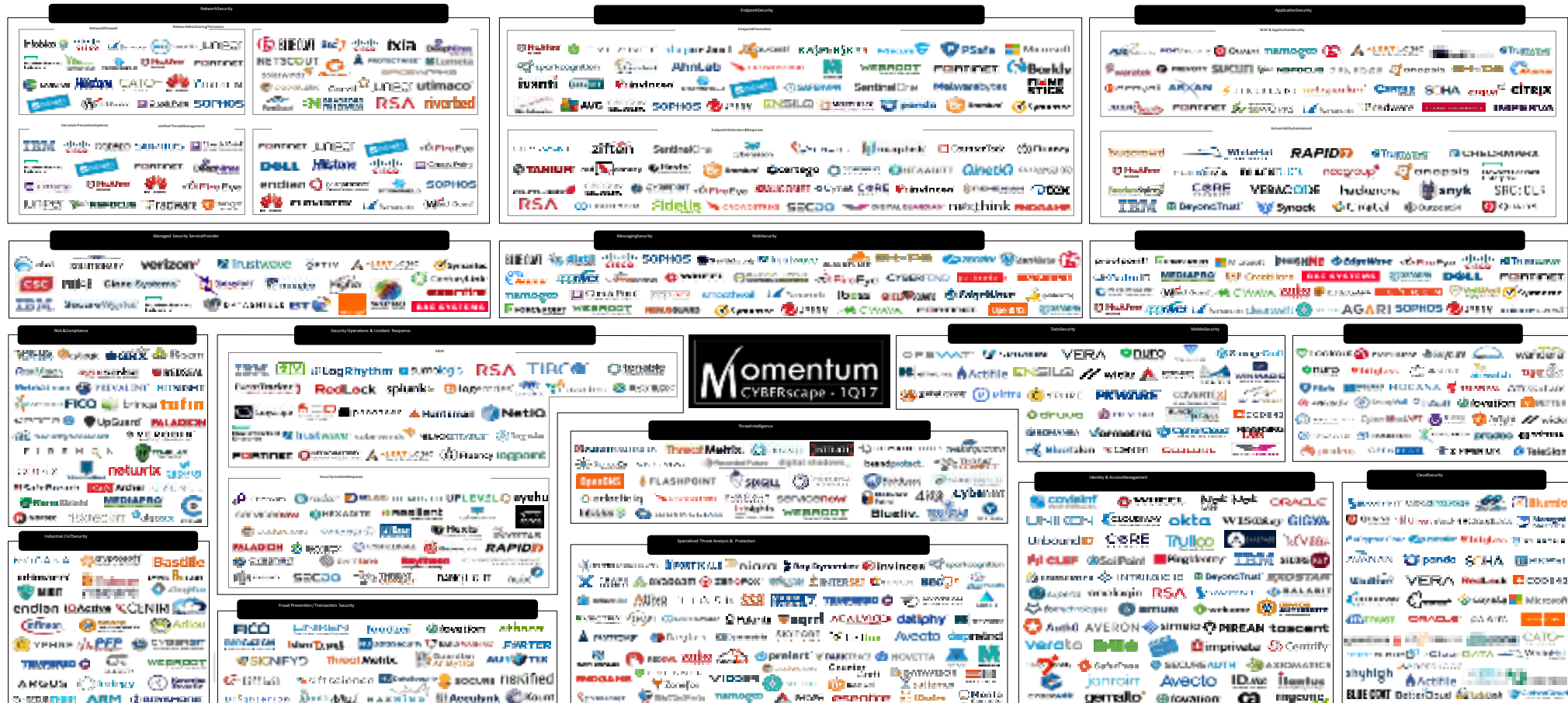
2. This growth has also generated a new level of threats - with 176 new threats every minute



Understanding the problem

Manual security operations is increasingly becoming expensive and ineffective as the number of alerts are exponentially growing given the scale of digital transformation, accelerated volume of new threats and global wide shortage of cyber security specialists.

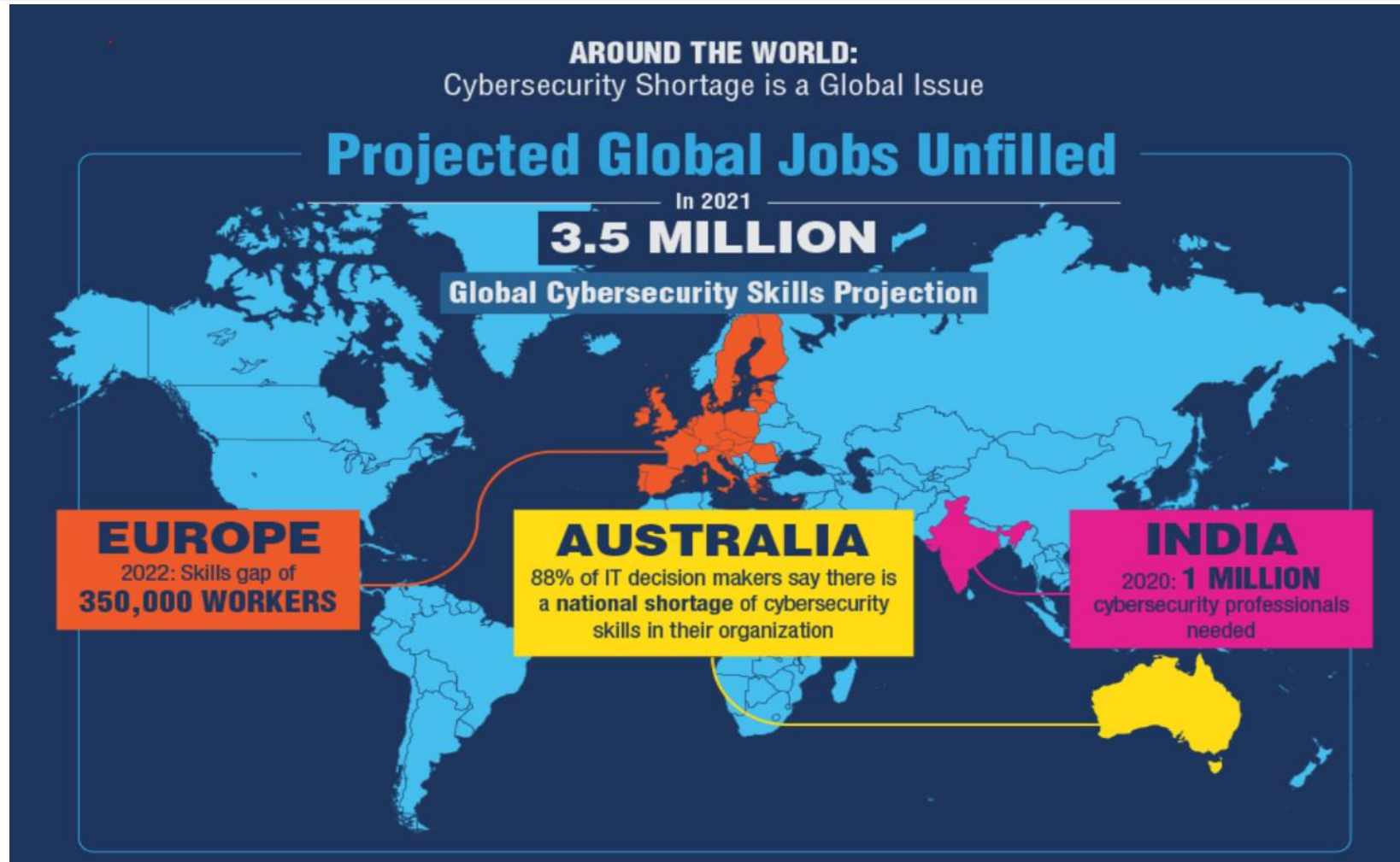
3. To manage these threats, there are now over 500 discrete vendors who are providing some form of solution



Understanding the problem

Manual security operations is increasingly becoming expensive and ineffective as the number of alerts are exponentially growing given the scale of digital transformation, accelerated volume of new threats and global wide shortage of cyber security specialists.

4. By 2020, there will be a shortage of **1 million** cyber security professionals in India



Enter SOAR : Security Orchestration, Automation and Response

Technology Convergence: convergence of 3 previously distinct technology sectors: security orchestration and automation, incident management and response, and threat intelligence.



Security
Orchestration
& Automation



Security Incident
Response
Platform



Threat
Intelligence

**SOAR : Security Orchestration, Automation
and Response**

01

Mapping Functional Components

Should-have components for SOAR solutions, and summarised capabilities within those components. The components are orchestration, automation, incident management and collaboration, and dashboards and reporting.

02

Automation

How to make machines do task-oriented “human work”

03

Orchestration

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

04

Incident management and collaboration

End-to-end management of an incident by people

05

Dashboards and reporting

Visualisations and capabilities for collecting and reporting on metrics and other information

While each component set is distinct in features, requirements, and benefits, they feed into each other in a virtuous cycle and form pieces of the complete SOAR jigsaw.

Security Orchestration & Automation (SOAR) helps address the lack of integration between technologies by providing a capability that includes:

AUTOMATION

A SOAR Platform enables you to work smarter by executing actions across your security infrastructure in seconds, versus hours or more if performed manually. Workflows may be turned in to automated playbooks, which allow for complex activities to be executed without human intervention

REPORTING & METRICS

Reporting and Metrics provide human oversight and auditing capabilities. Dashboards consolidate all critical information needed to understand the current state of your security operations. Reports provide executive level and detailed technical reporting for any event or case.

CASE MANAGEMENT

Confirmed events can be aggregated and escalated to Cases within SOAR Platform. Solutions should contain a mix of existing use case templates or the ability to customise based on your standard operating procedures, allowing you to efficiently track and monitor case status and progress.

VISUAL PLAYBOOK EDITOR

Both developers and non-developers would be able to construct and customize complex playbooks based on specific use cases. While constructing graphically, the SOAR platform generates supporting code behind the scenes in real-time.

ORCHESTRATION

A SOAR Platform's should support APIs, enabling you to connect and coordinate complex workflows across your team and tools. Powerful abstraction allows you to focus on what you want to accomplish, while the platform translates that into tool-specific actions.

ALERT MANAGEMENT

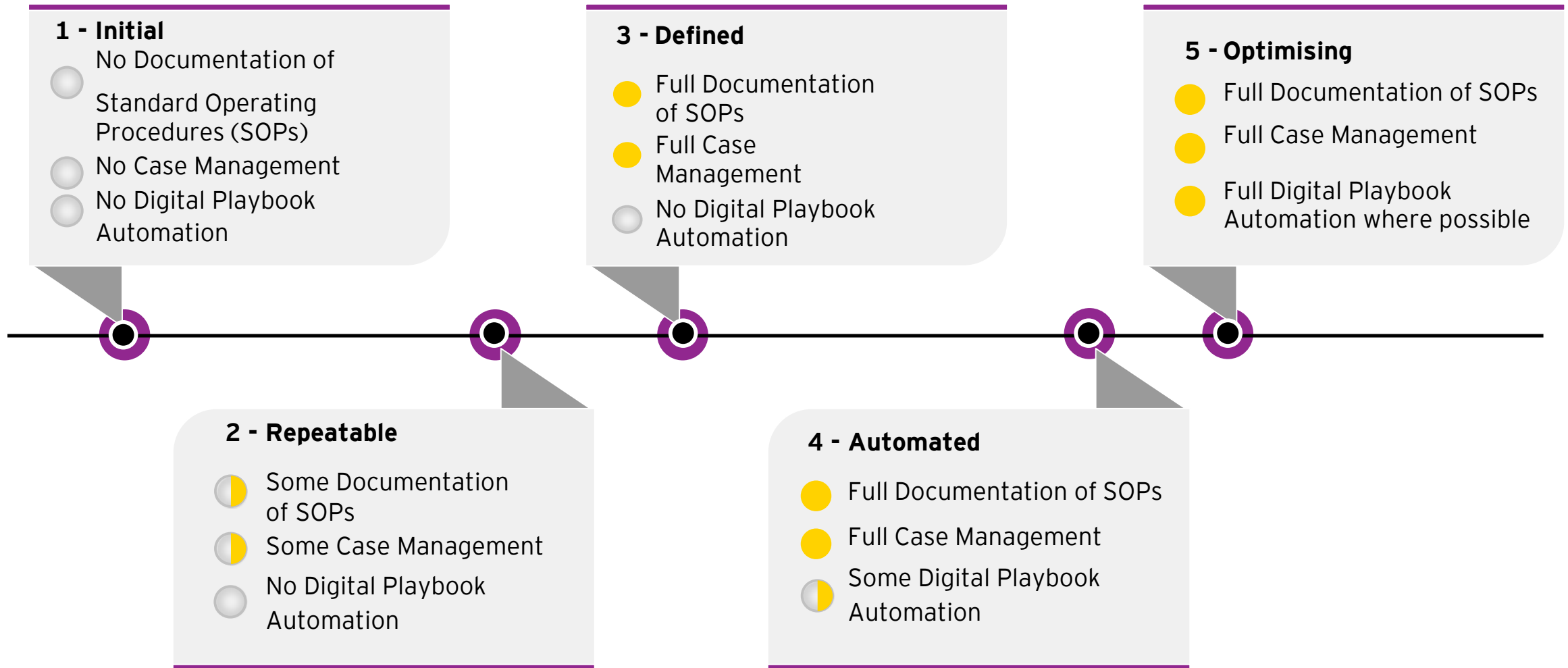
Alert management allows low-priority and false positives alerts to be eliminated before escalation, reducing the extensive procedural steps that are often prescribed for incidents or cases.

INTEGRATIONS WITH OTHER SYSTEMS

In-context integration allows you to marshal the full power of security investment with defenses that operate in unison. Integrating existing security infrastructure together allows each part to actively participate in your defense strategy.



By implementation a SOAR platform, organisations are able to significantly improve their overall security ops maturity



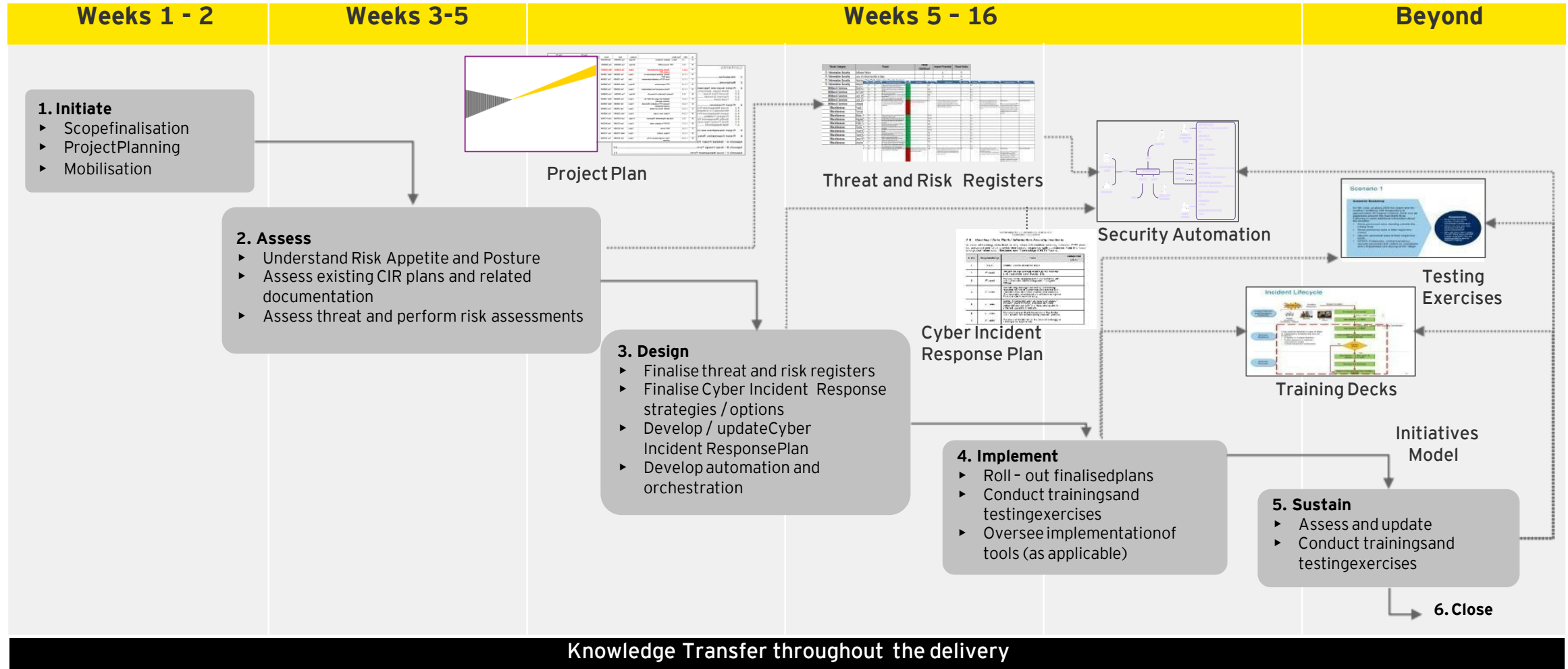


Cyber Security
Orchestration &
Automation Platform

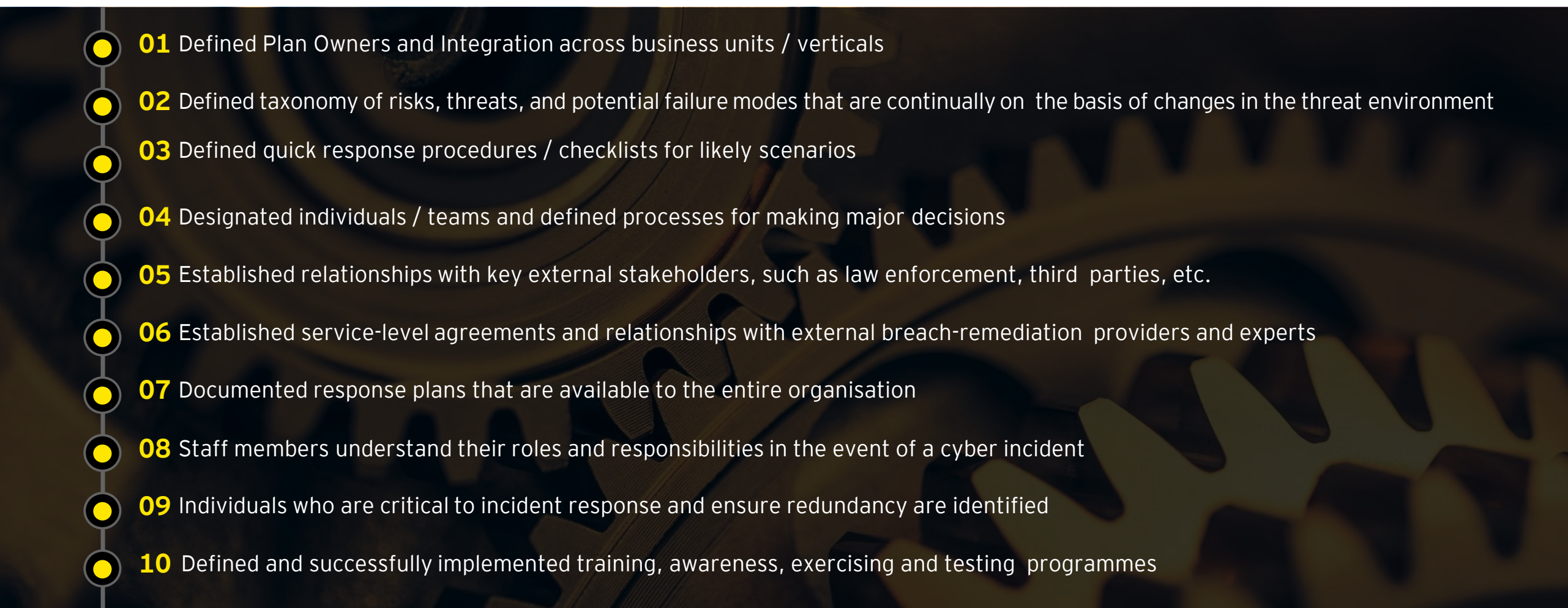
02

The Implementation
Approach

To maximise value and limit risk, we recommend that the following approach is undertaken



Characteristics of a best practice Cyber Security Incident Response Framework

- 
- **01** Defined Plan Owners and Integration across business units / verticals
 - **02** Defined taxonomy of risks, threats, and potential failure modes that are continually on the basis of changes in the threat environment
 - **03** Defined quick response procedures / checklists for likely scenarios
 - **04** Designated individuals / teams and defined processes for making major decisions
 - **05** Established relationships with key external stakeholders, such as law enforcement, third parties, etc.
 - **06** Established service-level agreements and relationships with external breach-remediation providers and experts
 - **07** Documented response plans that are available to the entire organisation
 - **08** Staff members understand their roles and responsibilities in the event of a cyber incident
 - **09** Individuals who are critical to incident response and ensure redundancy are identified
 - **10** Defined and successfully implemented training, awareness, exercising and testing programmes

Implementation Lessons Learned

Lessons Learned



- ▶ Identify particularly likely or especially damaging scenarios in order to focus initial effort on higher risk areas
- ▶ Involved appropriate teams and create top-down governance structure
- ▶ Agreement on maturity levels of process and align to automation maturity. (Don't agree to fully-automate an incomplete process)
- ▶ Build appropriate application governance layer. Most security tools will require administrator privilege and will require change approvals (this takes time!)
- ▶ Decided how you will test the functionality. Avoid triggering an action unless you have tested it

Key Dependencies



- ▶ Management support and communication plan for the stakeholders regarding the new project that will be implemented
- ▶ Availability of stakeholders to provide feedback on work products
- ▶ Complexity introduced by using two Incident Response platforms
- ▶ Accesses and required access privileges to key tools; and necessary network changes for the system integration
- ▶ Availability of connectors and its corresponding actions based on the use case
- ▶ Thorough testing of new platform upgrade packages and newly developed connectors

Cyber Security
Orchestration &
Automation Platform

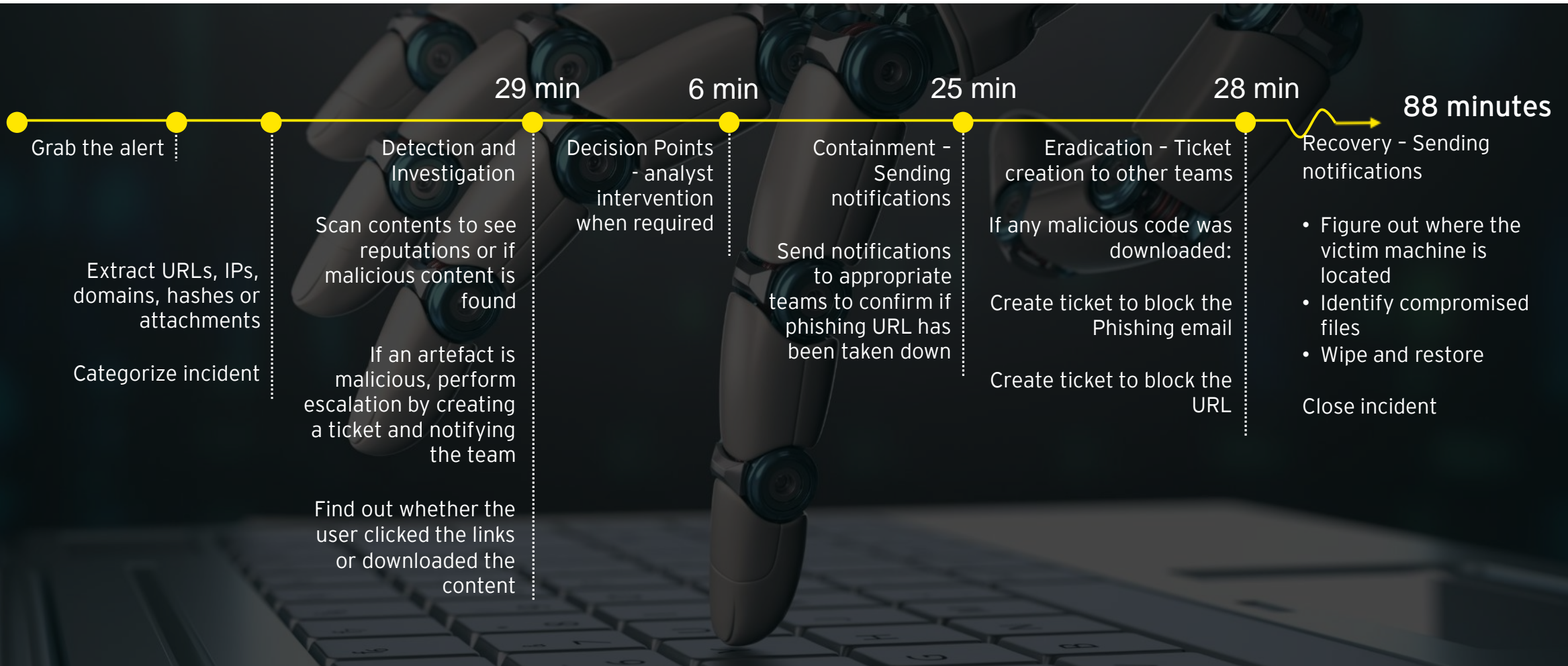
03

Value Delivered

Case Study #1

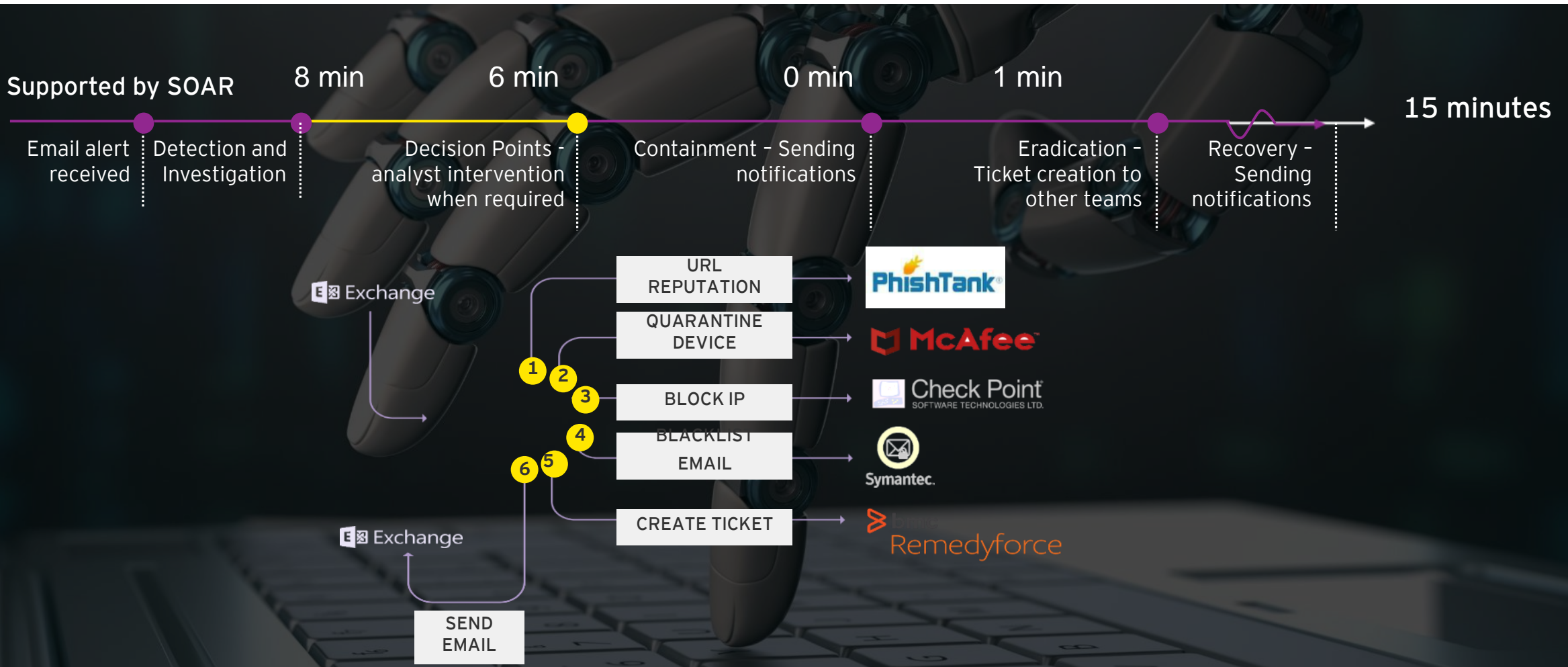
How does a SOC Analyst spend their time?

Manually Investigating a phishing attempt



Case Study #1

After Automation



Case Study #1

Automation Financial Benefits

- ▶ With an average annual salary of \$100,000 for a security employee
- ▶ Hourly rate of \$52
- ▶ Minute rate of \$0.87

\$0.87
PER MINUTE

\$26.10
PER ALERT

\$13,050
PER DAY

\$4.75m
PER YEAR

Manual Security Operations

- ▶ 30 minutes to triage, investigate, notify and respond
- ▶ Cost of each alert is \$26.10
- ▶ For an organisation with 500 alerts/day
- ▶ Cost of alerts per day is \$13,050
- ▶ With a 365 days SOC, annual cost is \$4.75m

	MANUAL		AUTOMATION	
Alert Triage	10 mins	\$8.70	Automated	\$0
Analysis	5 mins	\$4.35	5 mins	\$4.35
Escalation/Notification	5 mins	\$4.35	Automated	\$0
Response/Remediation	10 mins	\$8.70	Automated	\$0
TOTAL	30 mins	\$26.10	5mins	\$4.35

Supported with SOAR

- ▶ Reduction of time from 30 mins to 5 mins
- ▶ Cost of each alert is \$4.35
- ▶ 83% of cost reduction

83%
REDUCTION IN COST

\$4.35
PER ALERT

\$2,175
PER DAY

\$795k
PER YEAR

The implementation of a SOAR platform can provide significant tangible benefits

Business Need

The client had low incident response maturity with incidents generally taking days to weeks to resolve. In addition, with the cyber talent gap growing and generally insufficient cyber resources to be able to support operations, they recognised they needed to do something. EY was asked to:

- ▶ IB Document the client's cybersecurity incident response playbooks - a comprehensive set of instructions followed by operations to identify, contain, eradicate and review an incident
- ▶ Provide assistance to develop technical integrations with client's Incident Management solutionsM Resilient™ and Phantom Enterprise Edition™

What we did

Improved the speed of the incident response process and drove down the Mean-Time-To-Respond via:

- ▶ Improved interactions and coordination between Business, IT and Security Units
- ▶ Tailored Incident Response playbooks aligned to existing client practices. Where necessary, made recommendations that aligned practices to industry leading practice
- ▶ Integrations that automated repetitive tasks: Automation increasing the speed of the process and drove down the Mean-Time-To-Response from hours to minutes through incident response orchestration and automation.

Tangible Returns (12 months)

US\$1.1m

Dollars saved



49mon

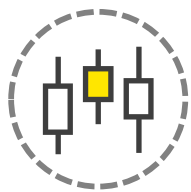
Time saved



3.39

FTE Gained





Intelligent orchestration

Accelerates and sharpens response. Human intelligence and tribal knowledge unlocked and captured in expert IR playbooks and automated enrichment that delivers critical incident insight to analysts instantly



Case management and reporting

Enables complete SOC and c-level visibility across your tools and continual IR improvement. Real-time incident dashboards and metrics that help security managers assess, measure, and improve IR capabilities and robust executive-level reporting that makes it easy to communicate with the c-suite and boardroom



Dynamic playbooks

Provides agile response that aligns to real-time incident data. Adaptive IR workflows that automatically adjust as an incident unfolds and visual drag-and-drop playbook editor that combines people, processes, and integrations



Guided response

Ensures the right person has the right information at the right time. Best practices-based incident response playbooks that guide analysts through an expert-level response and automated enrichment that provides critical incident data, enabling faster and more accurate decision making

Source: Source: https://www.resilientsystems.com/wp-content/uploads/2018/04/IBM-Resilient-Intelligent-Orchestration-data-sheet_April-2018.pdf



Resilient's Functionality





Automation

Eliminates routine tasks and enables analysts to focus on more strategic priorities. Feature-rich functional components that make automated actions reusable with minimal coding, integrations available on the IBM Security App Exchange for immediate download and use and drag-and-drop visual workflow editor that helps team quickly build IR workflows of all types - from simple to complex



Partner ecosystem and developer community

Makes building and deploying integrations faster and easier than ever. Enterprise-grade integrations with technology partners provide fast time-to-value of security investments and developer tools and documentation allows teams to quickly and easily build and deploy custom integrations

Source: Source: https://www.resilientsystems.com/wp-content/uploads/2018/04/IBM-Resilient-Intelligent-Orchestration-data-sheet_April-2018.pdf

Resilient's Functionality (contd)

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [ey.com](https://www.ey.com).

© 2018 EYGM Limited.
All Rights Reserved.

APAC no. XXXXXX

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com