



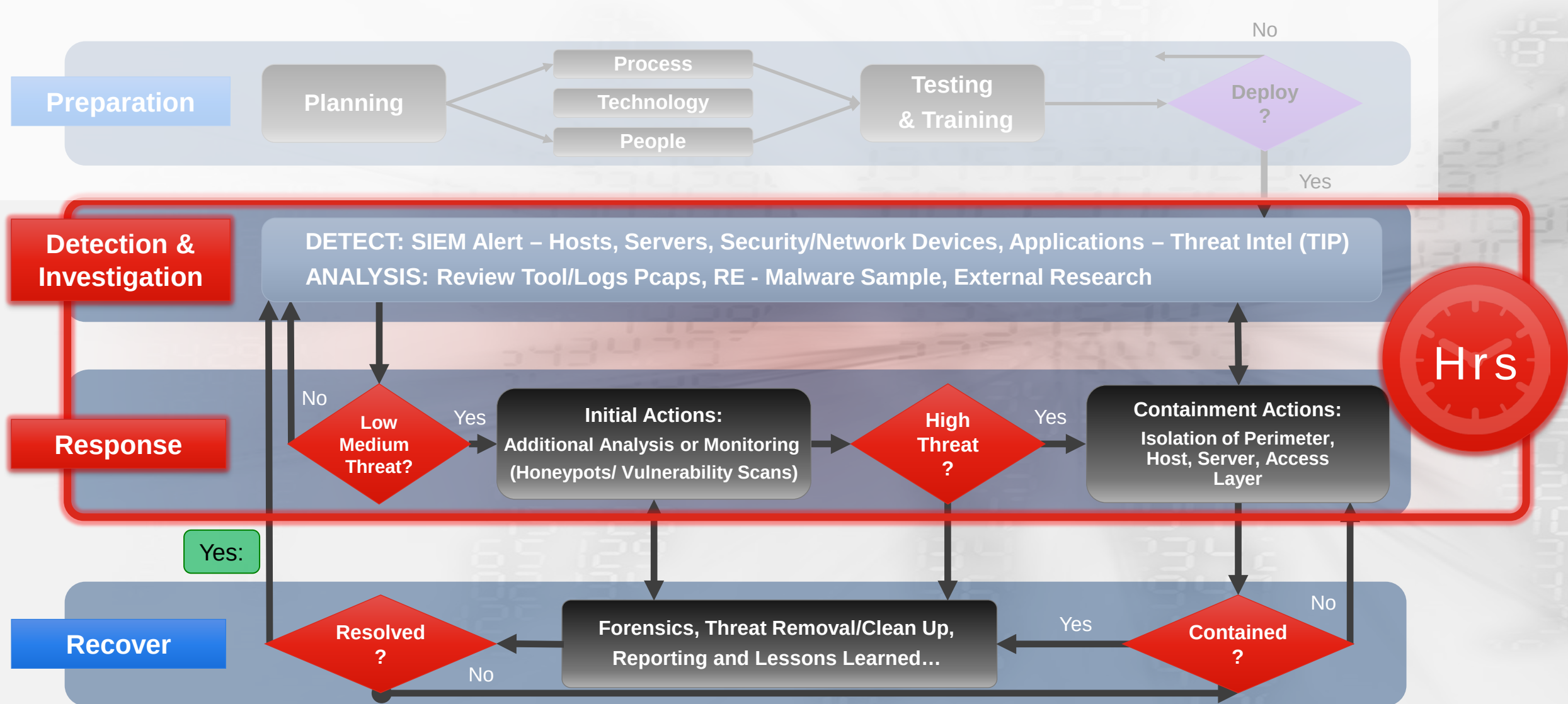
Adaptívne zabezpečenie pre SOC tímy, orkestrácia, automatizácia a reakcia

Peter Kocik

Team Leader Systems Engineering CEE

pkocik@fortinet.com

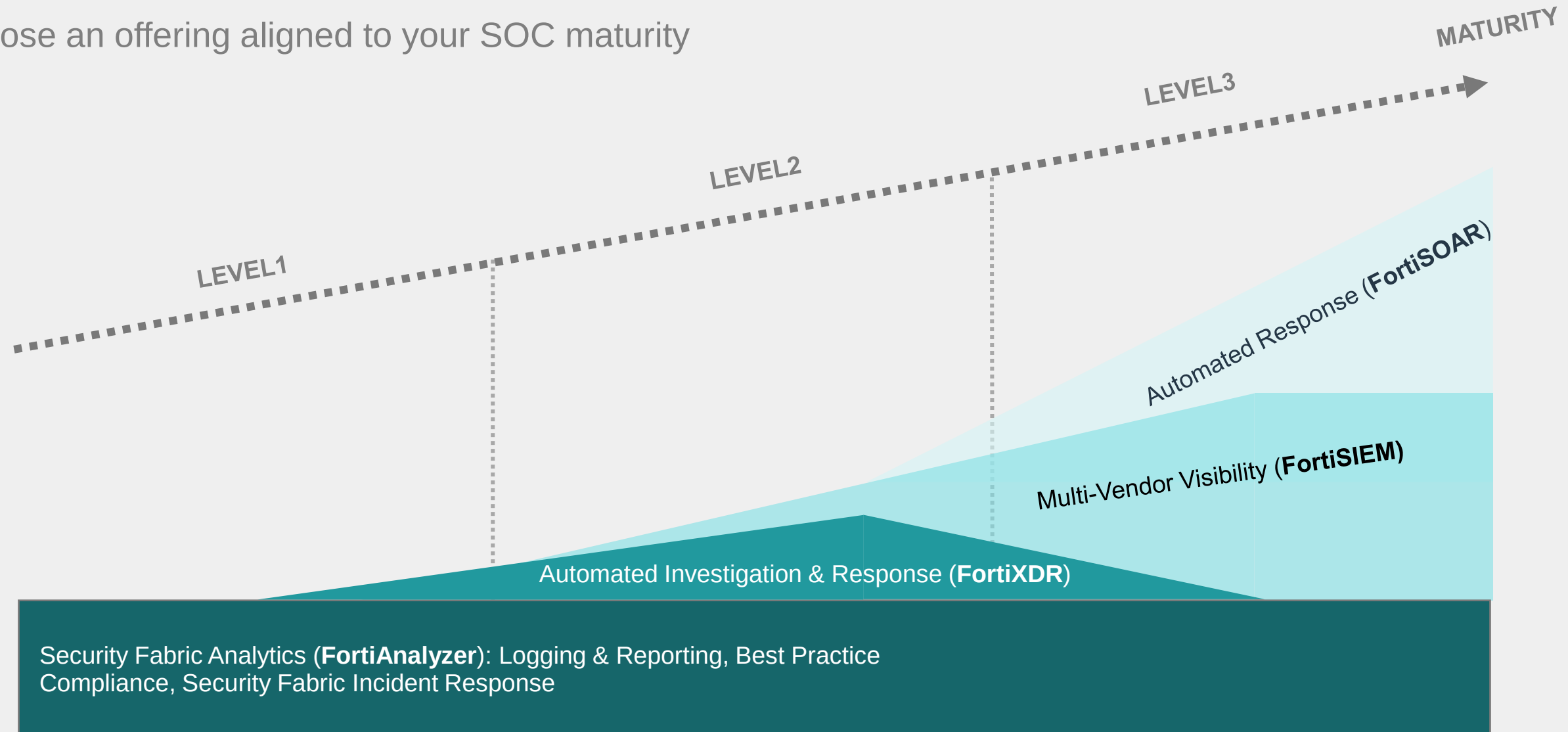
Incident Response Process





Simplify Security Operations

Choose an offering aligned to your SOC maturity



What Complexities are Driving FortiSOAR Demand

Security Operations Struggling To Keep Pace

Rise in Ransomware

“Two thirds of organizations report being targeted by ransomware. More than half brought in an incident response service and reported the incident to law enforcement.”

Fortinet, Global Ransomware Survey, 2021



Point Product Complexity

Eighty percent of organizations currently or plan to pursue a vendor consolidation strategy. 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio.

Gartner, Top Security and Risk Management Trends, 2021



Alert Overload

“70% of respondents say their home lives are being emotionally impacted by their work managing threat alerts. 51% feel their team is being overwhelmed by the volume of alerts.”

Security Magazine, 70% of SOC Teams are Overwhelmed by Alert Volume, 2021



Scarcity of Cyber Skills

“57% of organizations have been impacted by the global cybersecurity skills shortage. Among those, 62% said that the skills shortage has increased the workload on existing staff; and 38% said that the skills shortage has led to employee burnout and employee attrition.”

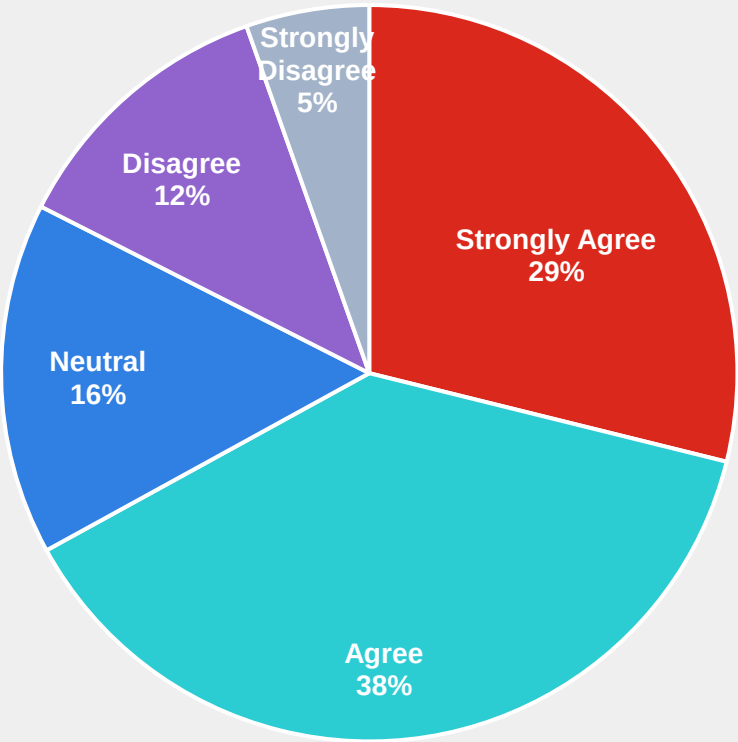
ESG and ISSA, The Life and Times of Cybersecurity Professionals, 2021



FortiSOAR Customers Implementing Consolidation Strategies

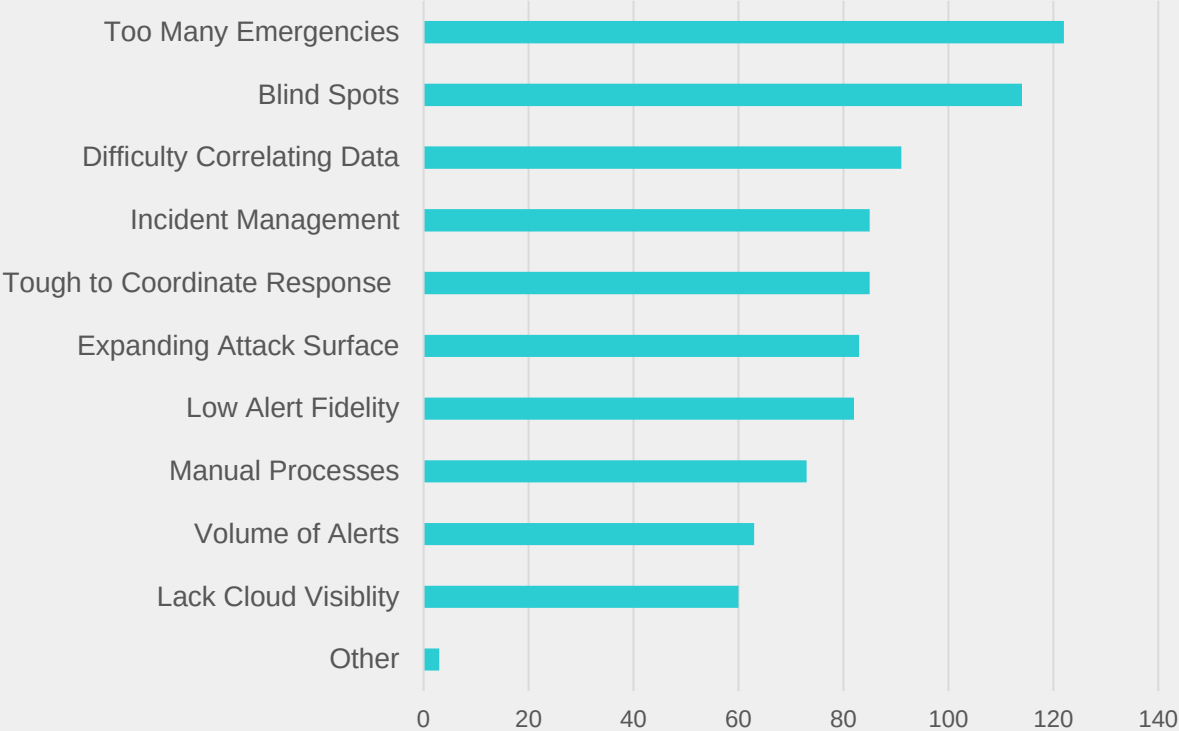
Point Product Complexity

My organization manages threat detection and response using an assortment of disconnected security tools.



67% of organizations use disconnected security tools

Which of the following would you say are your organization's biggest challenges regarding threat detection/response?



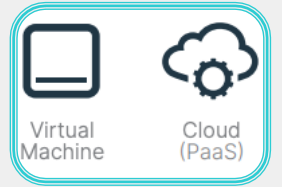
Challenged by constant emergencies, blind spots and data inconsistency





FortiSOAR from 1,000 ft Above

Respond 98% Faster Than Manual Operations with Orchestration & Automation



Reconnaissance

Weaponization

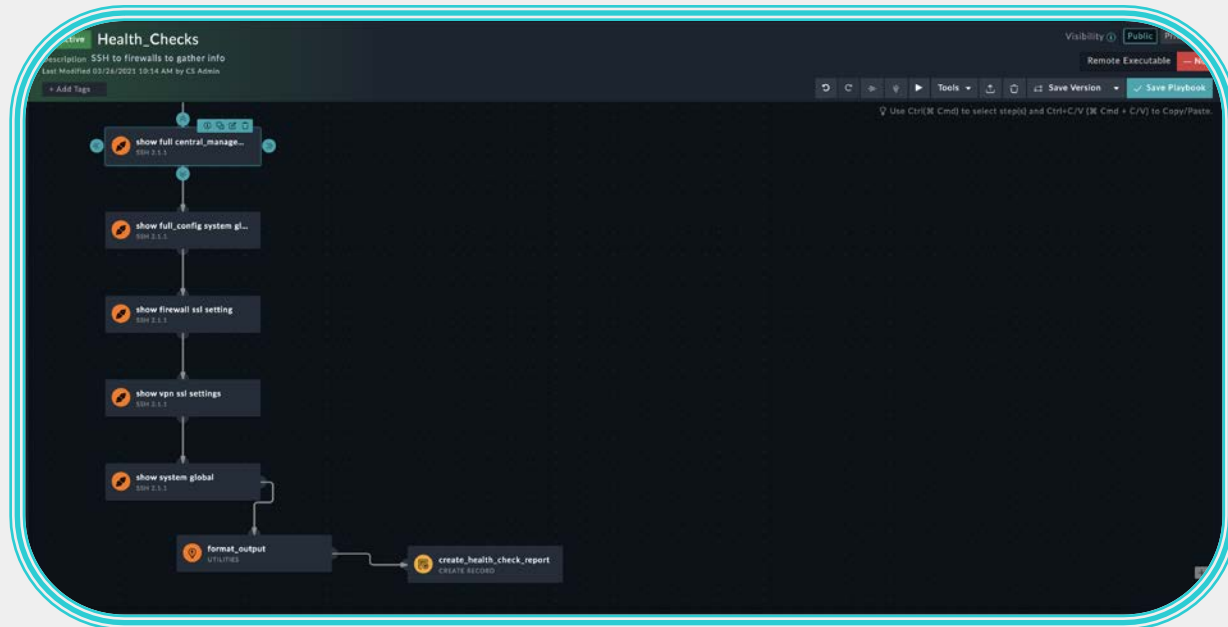
Delivery

Exploitation

Installation

Command &
Control

Action on
Objectives



Solution: FortiSOAR

- ✓ Advanced Case Management
- ✓ Integrated Threat Intelligence
- ✓ Product Adaptability
- ✓ 400 Connectors / 180+ OOTB Playbooks



Key FortiSOAR Elements (and Focus Areas)

Investigation & Response

Efficiently investigate alerts/incidents
Understand, review and manage incidents

- Crisis Response (War Room)
- Mobile Application
- Automatic tasking across multiple queues and teams

Advanced Orchestration & Automation

Easily build advanced automation to create workflows and integrate into existing tools

- AI-Based Recommendation Engine
- Playbook and Connector Builder
- Content packs
- Container in FMG/FAZ

Threat Intelligence Management

- Deep FortiGuard integration, provides unrestricted lookup and Threat Encyclopedia access within the Indicator module

Form Factors / Licensing

- VM and Cloud (Enterprise / SP Ready)
- Agnostic (Multi-Vendor)
- Multi-Tenant
- Best Practice Services

FortiSOAR in The Cloud

- Multi-tenancy support
- Flexible deployments
 - Enterprise
 - Shared tenancy
- Auto-firmware upgrade/health monitoring
- Simple licensing model

KPI Measuring & Reporting

- Quickly identify SOC KPI's (MTTR, analyst time savings) and reporting for audits, leadership etc

Role-Based Access Control

Built-in visual dashboard enabling easy creation of dashboards specific to a role in and outside the SOC

- Control access to connector actions, configurations and Playbook
- Concurrent Model



Unified Incident Response Management

1

Standardize E2E Control

FortiSOAR unifies people, processes & data from all detection / alert sources into a singular module

2

Cohesively Take Action

Orchestrate, automate, & respond with all of your existing tools in-real-time

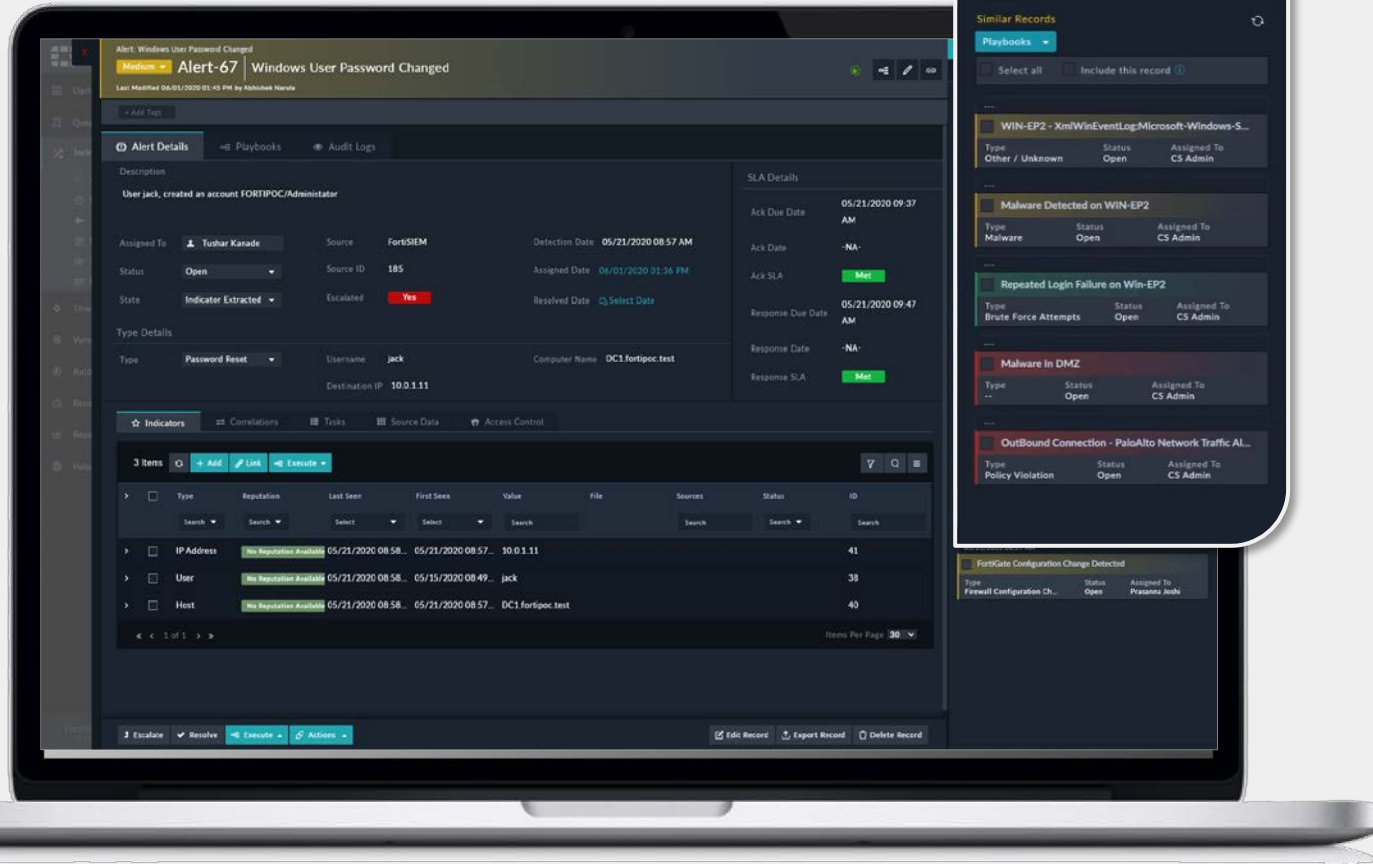
3

Visualize & Manage Seamlessly

Visualize to map, manage Incidents & easily build automated workflows



Alert Triage Automation



1

Streamline Investigations

AI-driven prioritization that dynamically detects false positives, and automatically group similar alerts and incidents to present a consolidated timeline for investigations

2

Automatically Enrich & Correlate Alerts

Reduce time spent investigating alerts through FortiSOAR's recommendation engine, that provides analysts with suggested actions, correlated alerts & critical data, enabling quick decision making

3

Proactively Respond

Control how data is processed by dictating what algorithm fits internal best practices



SOC Optimization

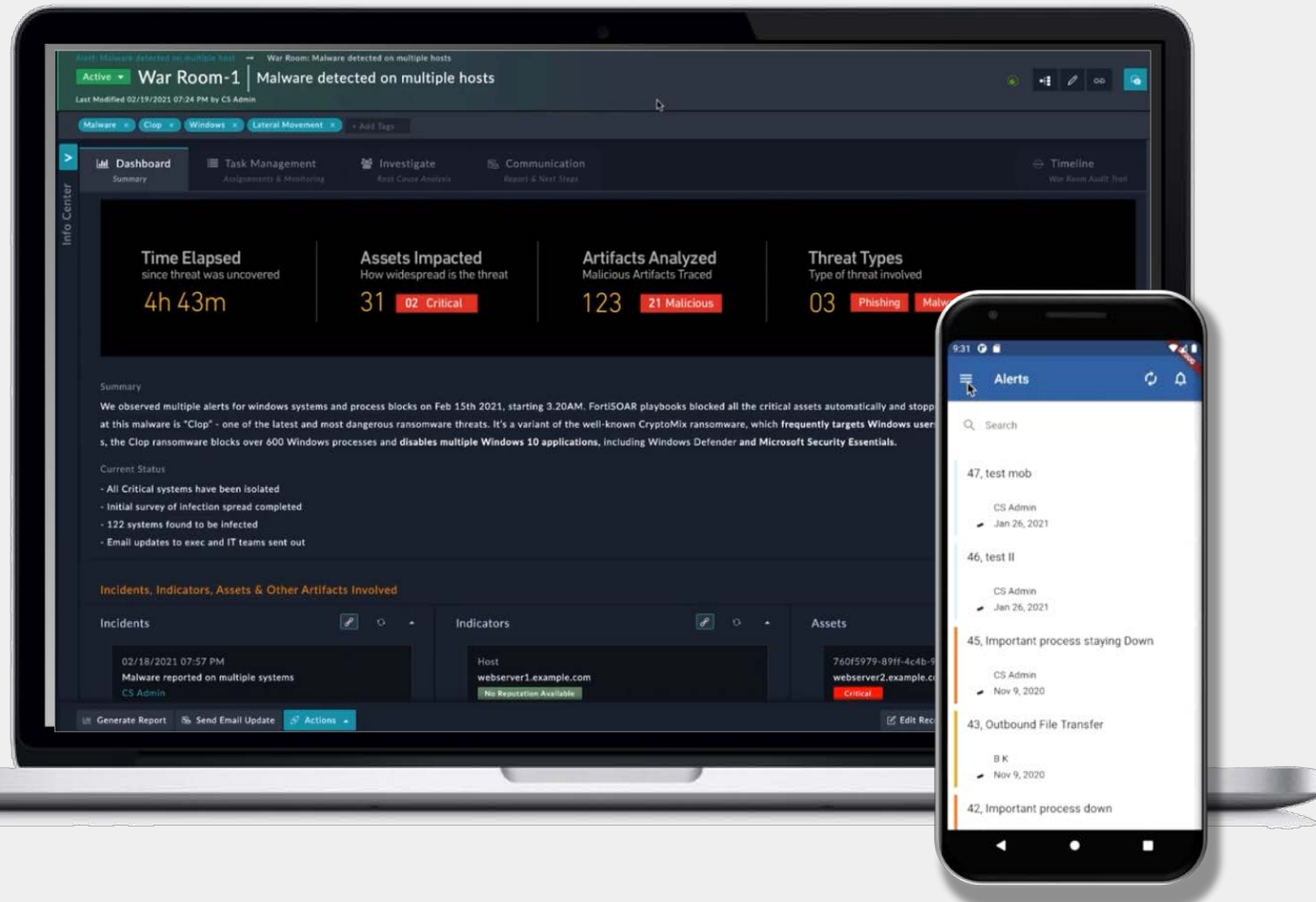
1 **Reduce TCO (Total Cost of Ownership)**
Leveraging comprehensive & easy to customize dashboards – Zero in on where processes can be automated

2 **Measure & Control SOC Success**
Monitor security operations KPIs and identify where SOC performance can be improved

3 **Jumpstart with Product Flexibility**
OOB content packs for speedy time to value and no code playbook builder for easy to scale automated workflows



SOC Cross-Collaboration



1

Get a Head with a Strong Response

If an attack occurs, a cohesive and fast response is required. FortiSOAR helps build a strong crisis response profile, while addressing the communications and skill gap

2

Expedite the Remediation Process

Using unified dashboards with incident related Metrics – time lapsed, impacted assets, threat types, & mobile application, empowers teams to address attacks instantly

3

Connect All Stakeholders

- *Concurrent user seats*
- *Real-time Communications – Conference, Messaging, and historical references*
- *Distributed Multi-Tenancy, Light weight agent, dedicated tenant*

Threat Intelligence Management

1

Integrate Threat Intelligence

Enabling analysts to focus on threat hunting without having to context switch

2

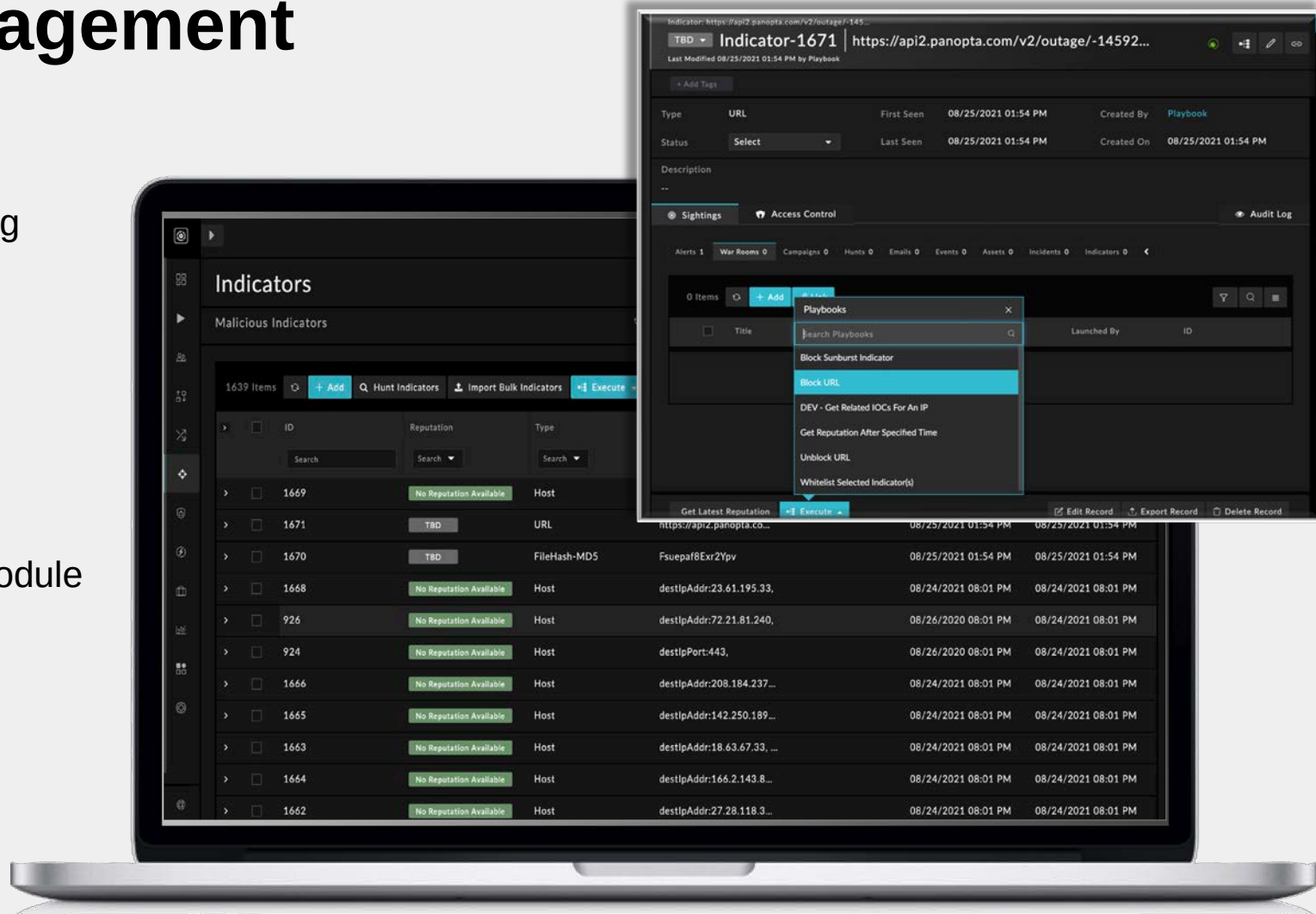
Simplified TIM

FortiSOAR's deep FortiGuard integration, provides unrestricted lookup and Threat Encyclopedia access within the Indicator module – centralizing TIM

3

Easily Hunt Threats

Automated threat hunting, execute playbooks and stop the threat proactively
Enabling analysts to focus on threat hunting without having to context switch



Phishing Investigation and Response

Automated Phishing Investigation & Response



Automated Alert Triage

- Begin Triage in FortiSOAR/notify user
- Define severity

False Positive

- Verify in Sandbox
- Check and Review representation of hostname
- Notify User/alert is automatically closed



Enrich

- Automated Indicator Extraction from email
- Identify if there are malicious Indicators



Confirmed Response

- Notify user on confirmation, block IP address, & extended investigation
- Identify all versioning of phishing email and delete
- Further investigation and confirm IOC

Manual Investigation & Response



Triggers High Alert Volume



Numerous coordination touch points



Continuous attempts

Case Study – Predtým ...

Veľká komerčná spoločnosť – internal SOC

- Existujúci SOC team: 5 analytici
- Využívajú sa free nástroje a SIEM (Qradar)
- Komplexná infraštruktúra, mnoho vendorov: Cisco, F5, Fortinet, Microsoft, Symantec ...
- ± 70 Incidentov za deň
- Niekoľko automatizovaných scenárov, zväčša manuálna investigácia
- Time to respond pri kritických incidentoch 50-60 minút

Case Study – Výber a PoC ...

- Oslovili sme všetkých významnejších SOAR výrobcov
- V rámci prvého kola sme identifikovali tých ktorí zapadali do nášho konceptu
- Technické DEMO vybratých riešení v trvaní 3-4 hodín pre každého výrobcu
- Druhé kolo výberu, do finále postúpili FortiSOAR a Cortex XSOAR
- PoC
- Tretie kolo výberu – súťaž o lepšiu cenu

Case Study – Potom ...

Business Impact

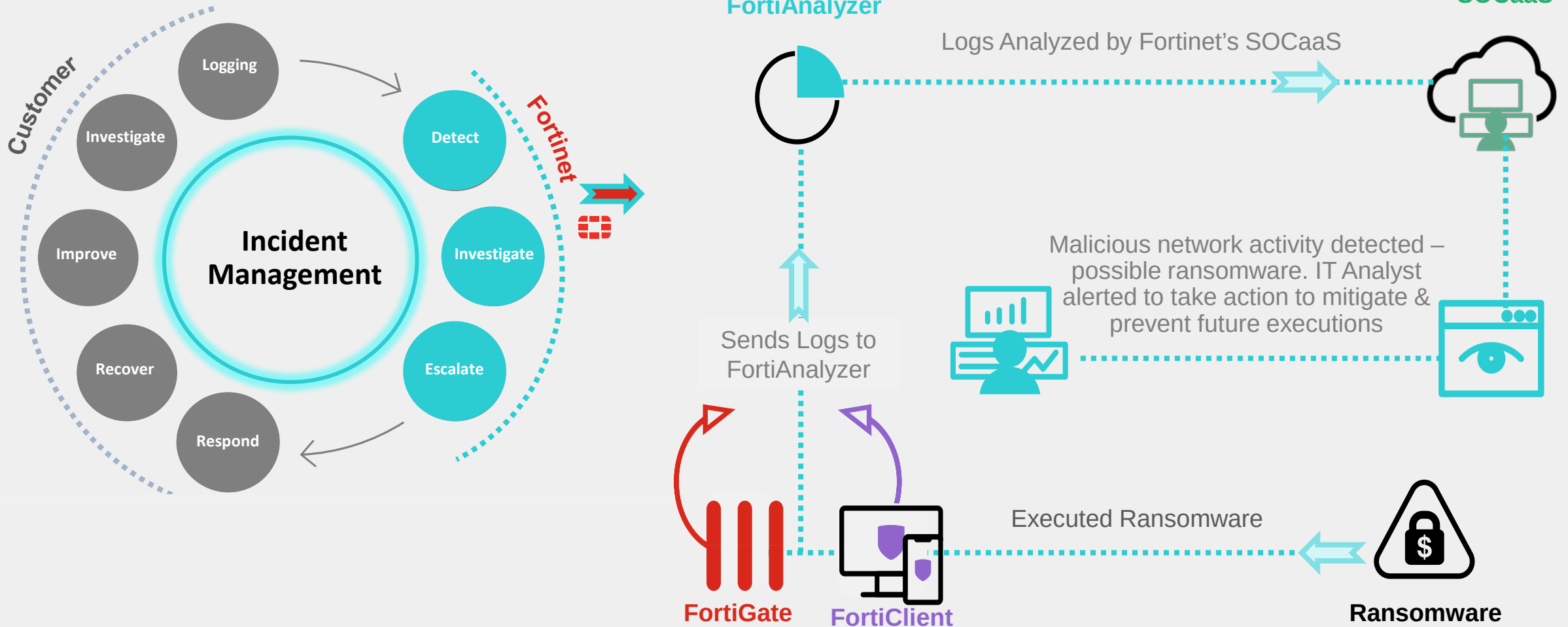
- Veľmi rýchle nasadenie do existujúceho prostredia, bezproblémová integrácia
- Zrýchlená reakcia na závažné hrozby (z 60 minút na ± 5 minút)
- Vylepšená efektivita vďaka automatizácii reakcie na low-level incidenty, tímu sa uvoľnila možnosť vykonávať strategickejšiu prácu
- Možnosť multitenancie do budúcnosti, SOC as a service

CISO: “Mať takú robustnú automatizáciu v našom SOCu, case management, playbooky a napojenia na systémy je veľkým prínosom. Naši analytici sú spokojní, vyšetrujú len to čo skutočne potrebuje ľudský pohľad. Naš tím sa už neprebúdzá uprostred noci, pokiaľ to nie je absolútne nevyhnutné.”



Fortinet's SOCaaS

Start, Build, or Offload Your SOC with 24x7 Coverage





Thank You 😊