How Secure are Networks?

Let us start with real-life example

Mobile Operator in Korea

Threat Actor

2

MisconfiguNetwork and/or vulnerable organization assets

Initial Access (2022)

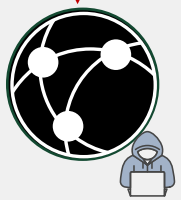
Weak/Stolen Credentials
Obsolete Systems

1

Reconnaissance

Social Engineering
Exposed Credentials

Dark Web



3

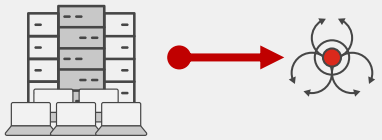
Execution

Malware Installation
System Discovery

4

Persistence

23 Systems with Malware Installed



DC

Critical Systems (HSS) containing Subscribers Personal Data

5

Lateral Movement

6

Exfiltration

27 Mill. USIMs

Reconnaissance → Initial Access & Execution → Persistence & Privilege Escalation → Lateral Movement & Exfiltration

FORTINET

Cyber-Security

Fernando Montes
Sr Regional Director Service Providers
Latin America

FORTINET

Cyber-Resilience

From Protection, to Trusted Secure Networks

Fernando Montes
Sr Regional Director Service Providers
Latin America

What is coming this year and beyond…

https://www.fortinet.com/lat/blog/industry-trends/predicciones-de-amenazas-para-2025-preparate-para-ciberataques-mas-grandes-y-audaces

Telco Operators are Prime Targets for Attacks

Critical Infrastructure in any country

Stop the network, stop the country

Data of millions of subscribers

Large cash flow, target to raise money within hours

Telco Attack attempts

Source: https://www.fortiguard.com/

Telco/Carrier Threat Landscape

Global Threats Detected
243.02bn

IPS

Exploit Techniques Detected
8.23bn

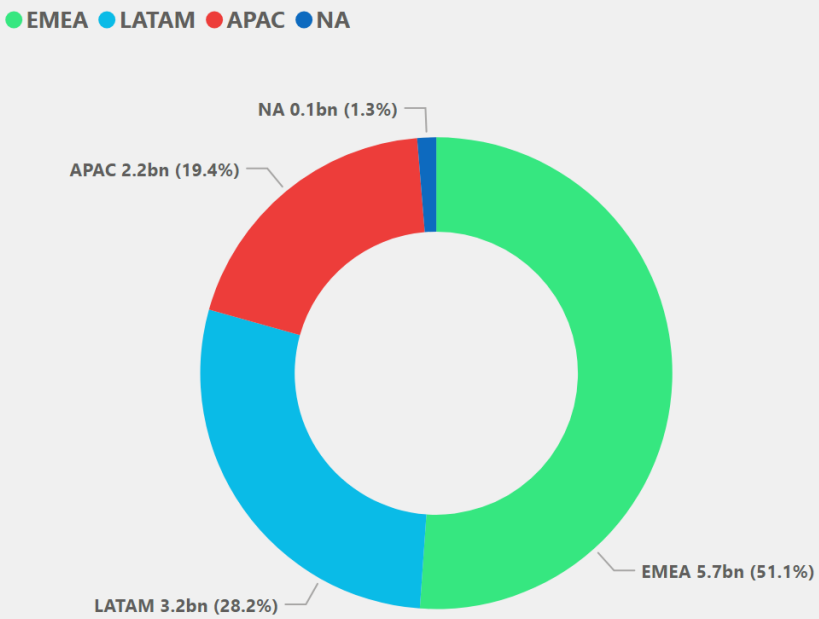
AV

Malware Distribution Detected
190.39M

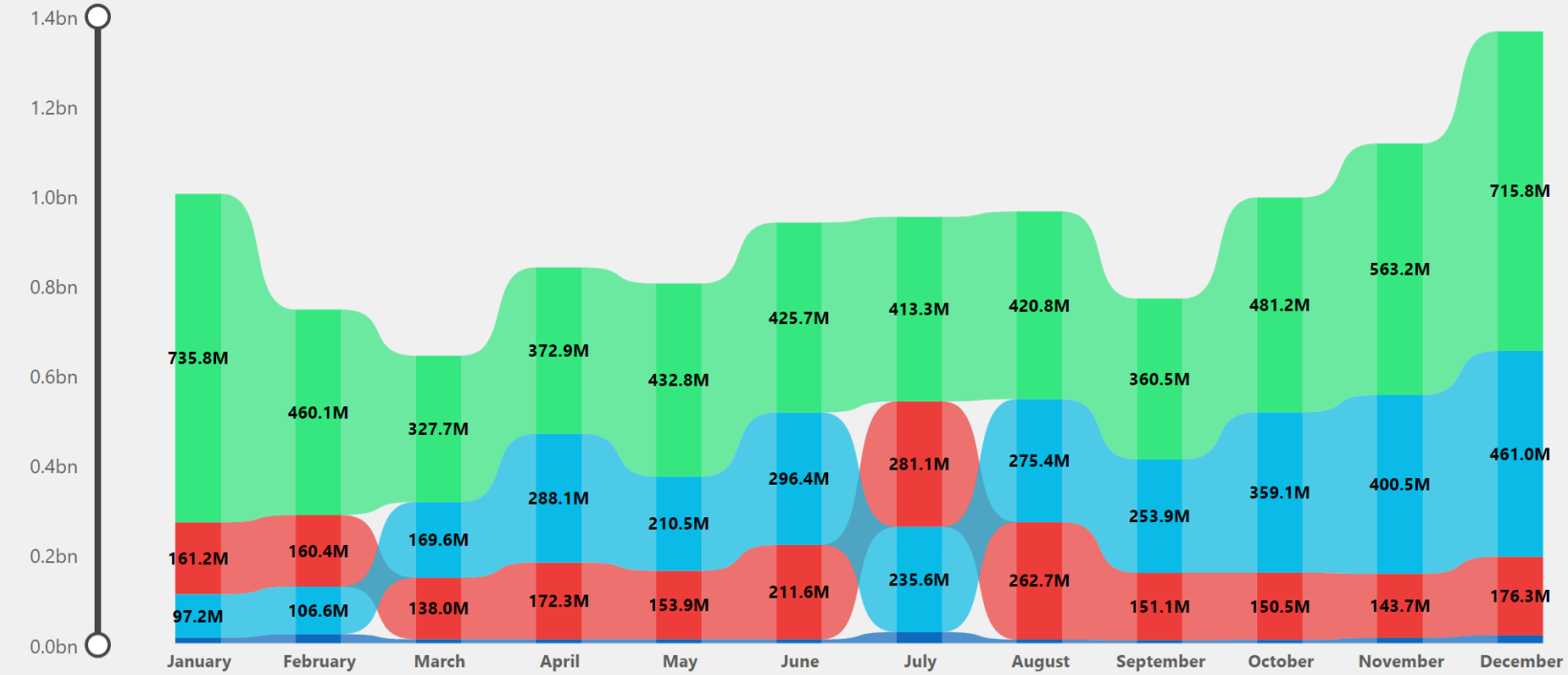
C2

Botnet Activity Detected
882.26M

Malicious Activity Distribution by Region



Behavioral Trend Analysis by Region



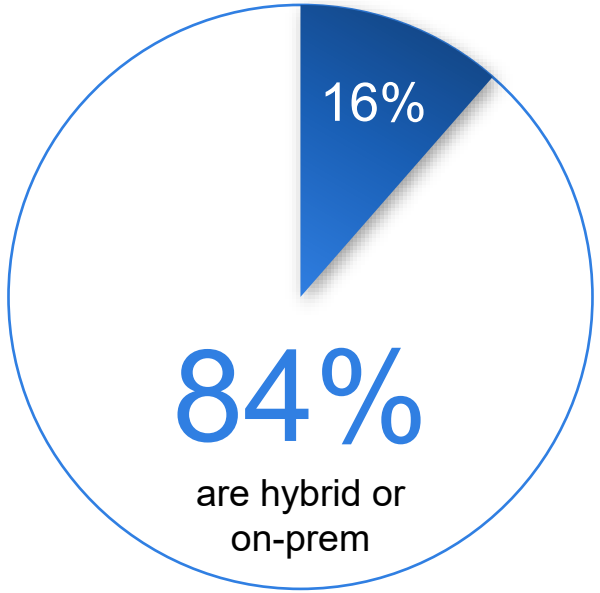

Users
Network
Business
Resilient Platform
AI


Users
Network
Business
Resilient Platform
AI

Telco Workforce is Hybrid

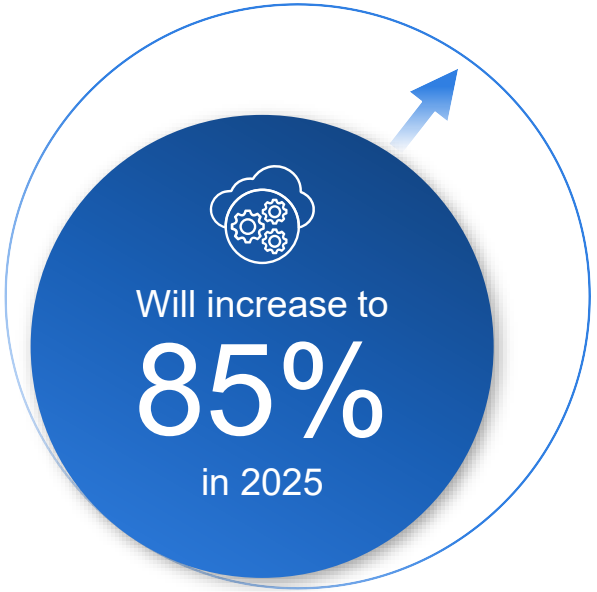
Managing Hybrid Workforce

Only **16%** of companies are fully remote



Growing Cloud Adoption

Up to **70%** of companies use SaaS apps today



Journey to Zero Trust

Sources saasacademy.com | forbes.com | virtualizationreview.com

Step-1: Secure Hybrid Access with Zero Trust

Principle

Zero Trust

Architecture

SASE

Customer Benefits

Improve user experience

Improve secure access

Product

SD-WAN

Telco Office / Point of Sales

SSE Cloud Service

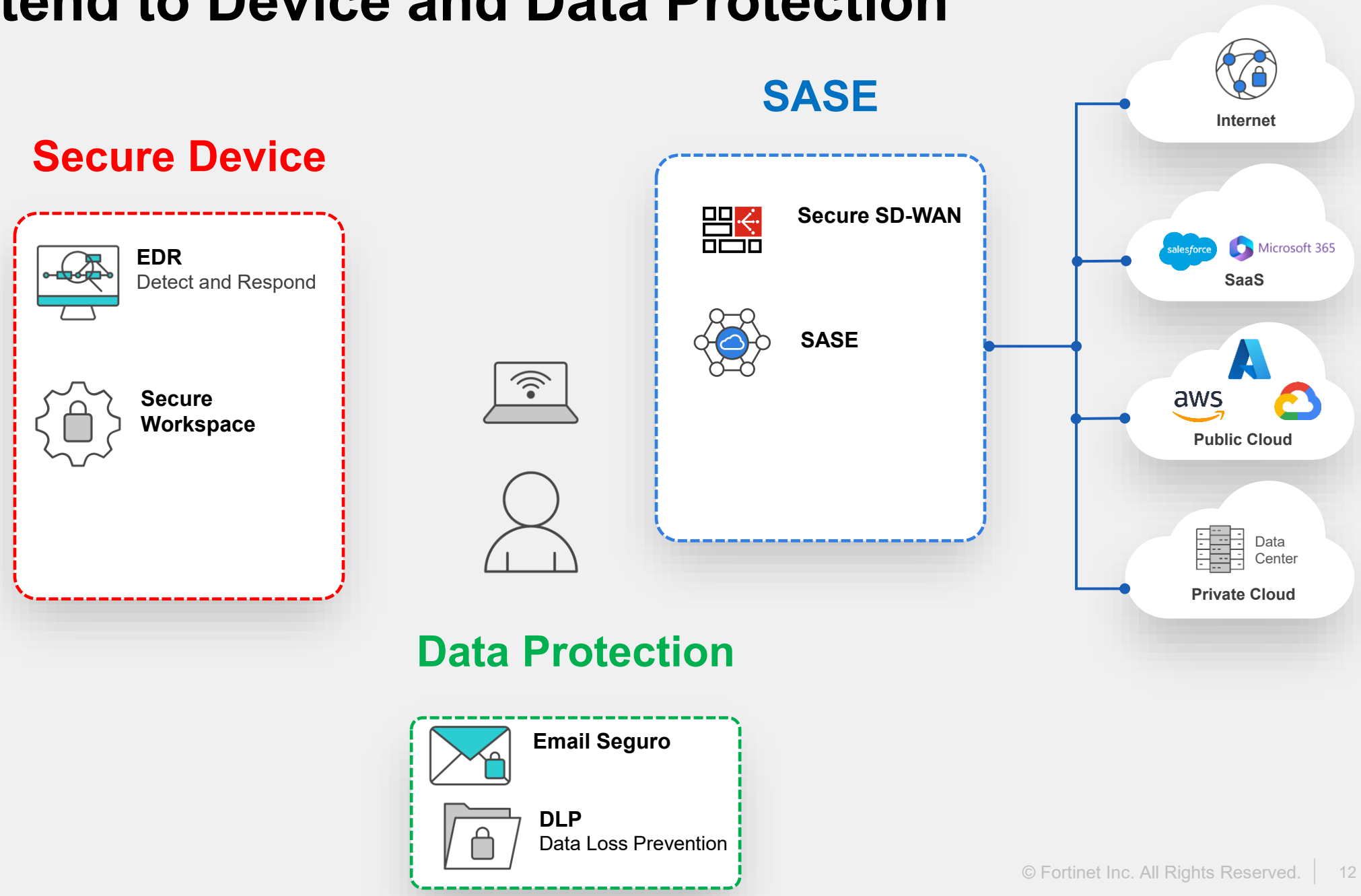
Secure Private Access (ZTNA)

Secure SaaS access (CASB)

Secure Internet Access (SWG/FWaaS)

- **SWG = Secure Web Gateway / FWaaS = Firewall-as-a-Service**, which protect users and devices from web-based threats.
- **ZTNA = Zero Trust Network Access**, providing secure, identity-based access with explicit control. Can also be sold standalone.
- **CASB = Cloud Access Security Broker**, which ensures secure access to SaaS applications and safeguards sensitive data.

Step-2: Extend to Device and Data Protection



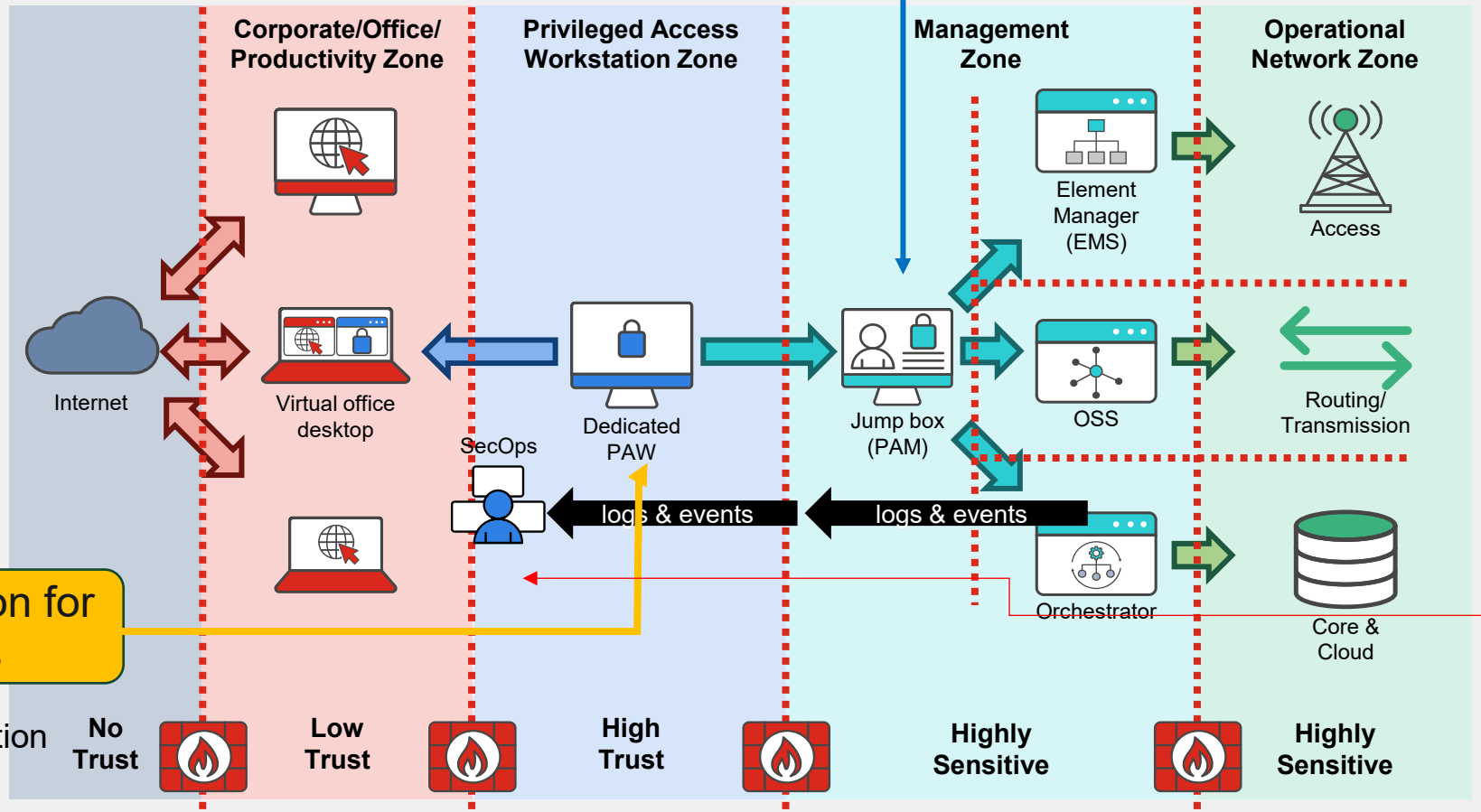
Step-3: Super-Users & Administration

2 Secure Access to Management

1 Isolate different Segments

Privilege Access **(PAM)** + **ZTNA**
Multi-Factor Authentication **(MFA)**
Rol Based Access Control **(RBAC)**

Segmentation FW



3 Dedicated Workstation for Privilege access

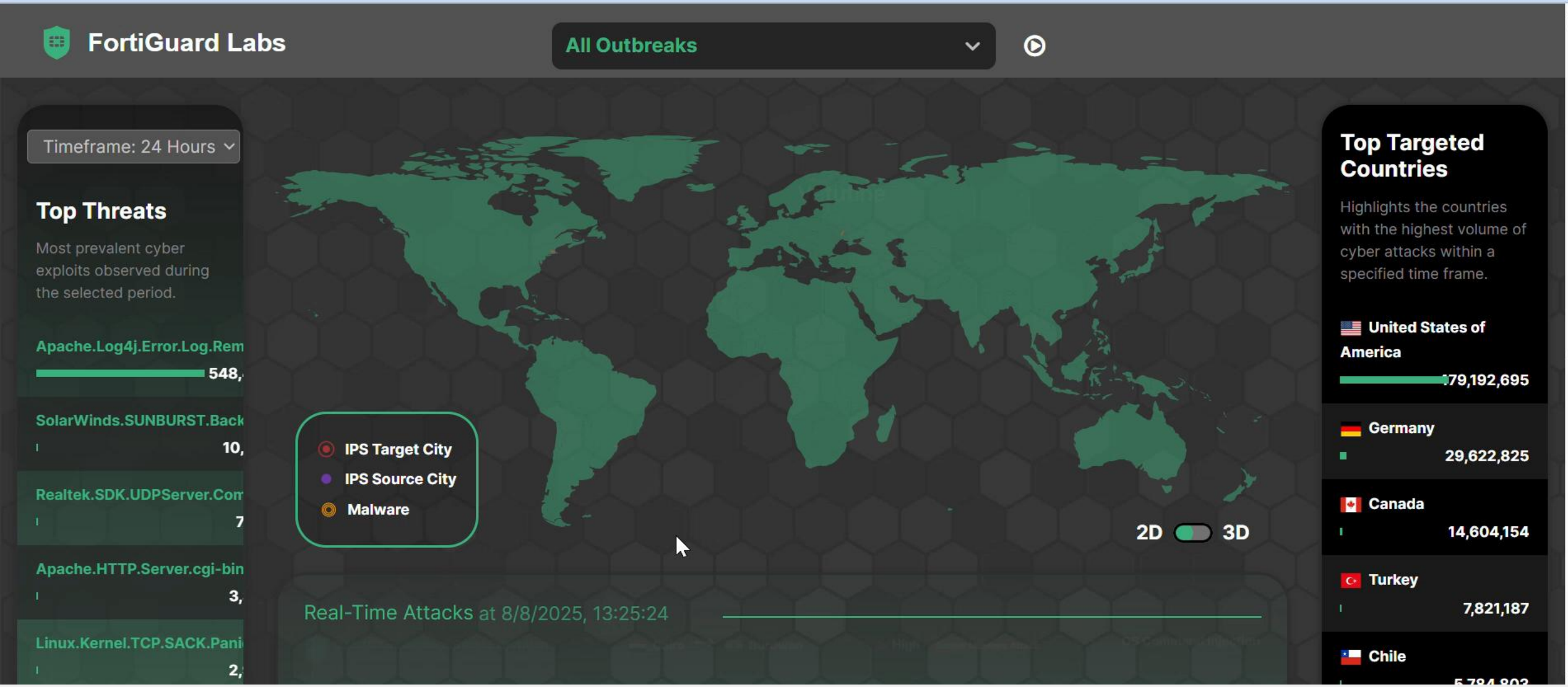
With Remote Browser Isolation **(RBI)**

4 SoC with AI

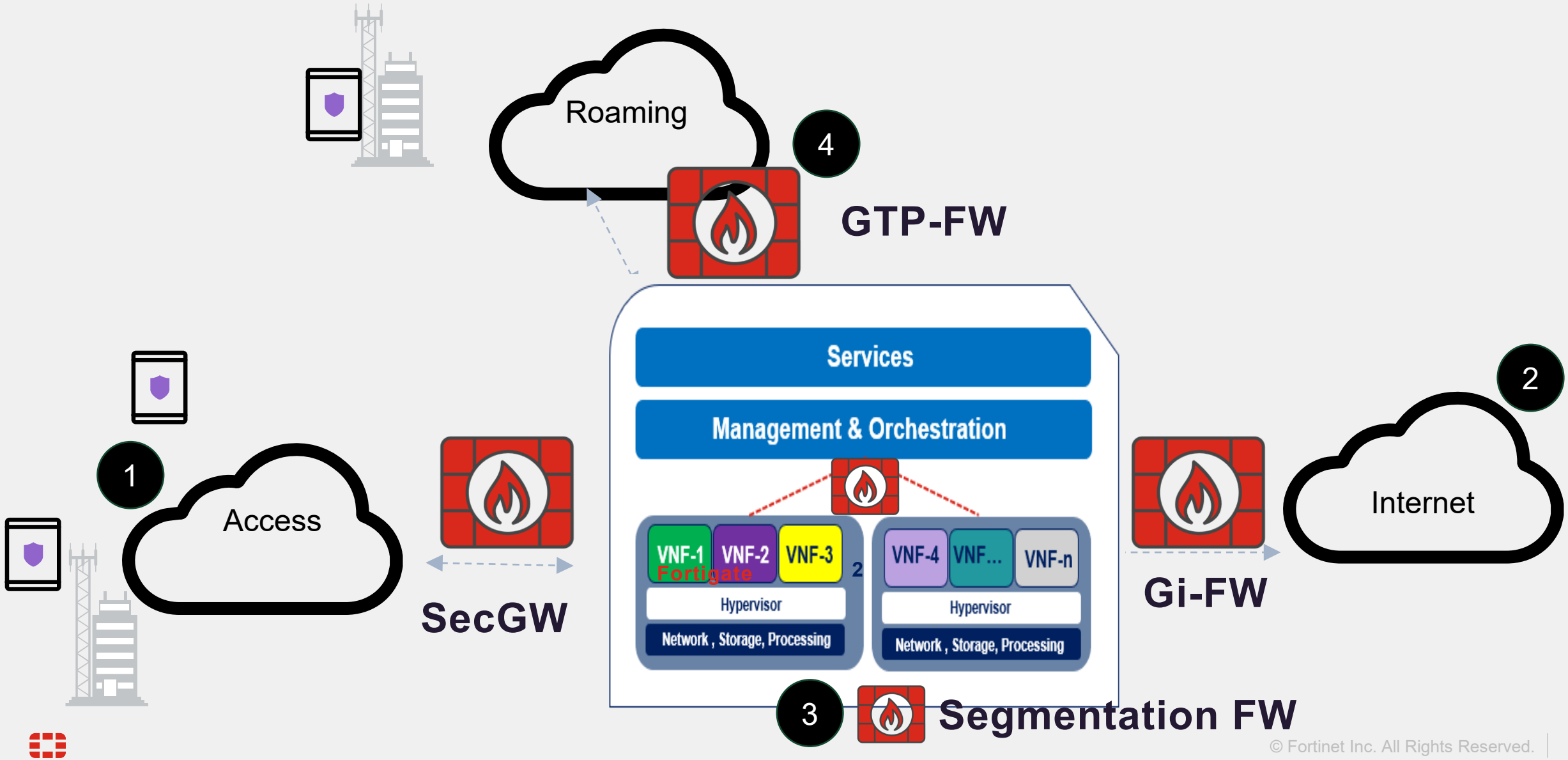
Based on UK TSA Code of Practice


Network
Users
Business
Resilient Platform
AI

https://www.fortiguard.com/threat-map
https://www.fortiguard.com/threat-research/industry



Step-1: Protect Perimeter



Step-2: Expand to Convergent Data Center

With AI SoC

Incident Response

SoC

AI

Convergent Data Center

E2W

NGFW

WAF

IT Cloud

NDR
Network Detection and Response

Deceptor
Honeypot

EDR
Endpoint Detection and Response

Management & Orchestration

E2W

Core Network

Services

Management & Orchestration

PCRF FW SMSc PGW SGW HSS

Hypervisor

Network, Storage, Processing

NGFW

WAF

Network & IT Services

DNS PKI DHCP

Hypervisor

X86 Compute

Telco Cloud

WAF

Firewall

CNAPP

salesforce Microsoft 365

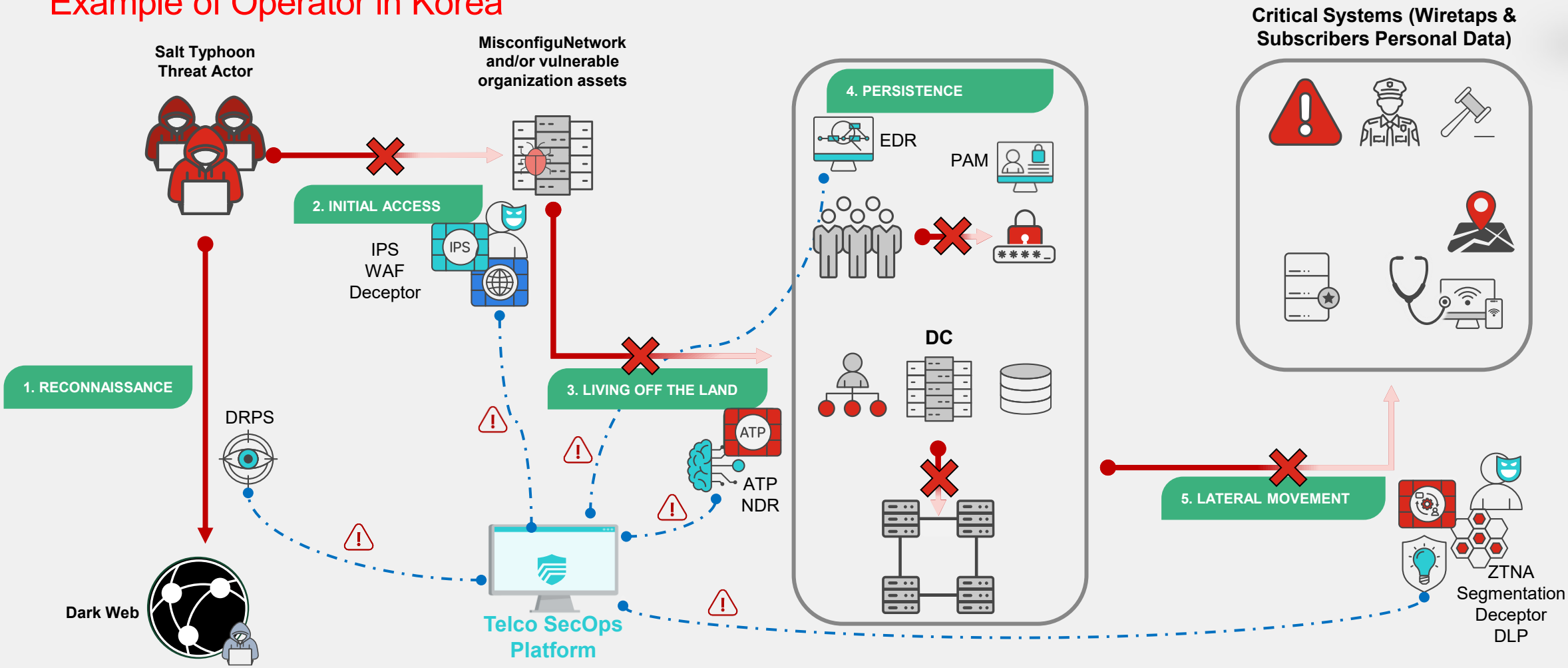
SaaS

aws

Public Cloud

Step-3: Resillient Network Protection

Example of Operator in Korea

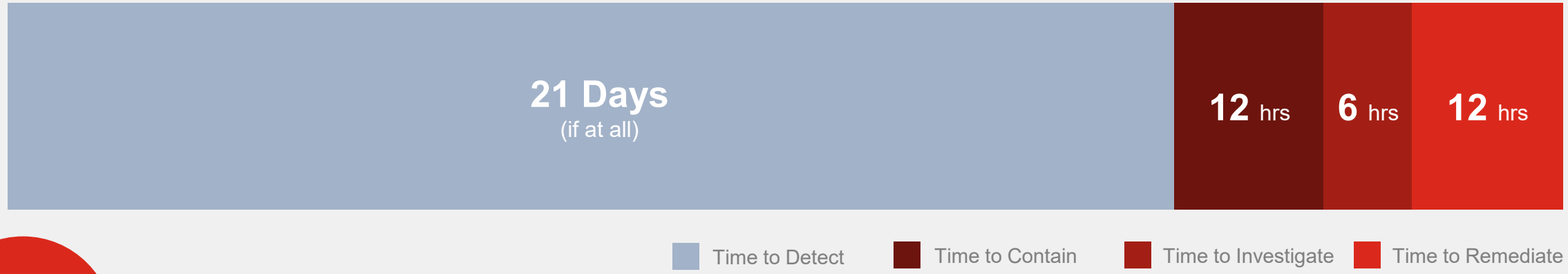


Reconnaissance | Initial Access & Execution | Persistence & Privilege Escalation | Lateral Movement & Exfiltration


Business
Users
Network
Resilient Platform

When Attackers Get in, They Stay Longer and Cost You More

Average time from detection to remediation



52%

of organizations report SecOps is harder than two years ago, citing threats, attack surface, volume/complexity[1]

SEC Rule

4 Days

to disclose material of a cybersecurity incident

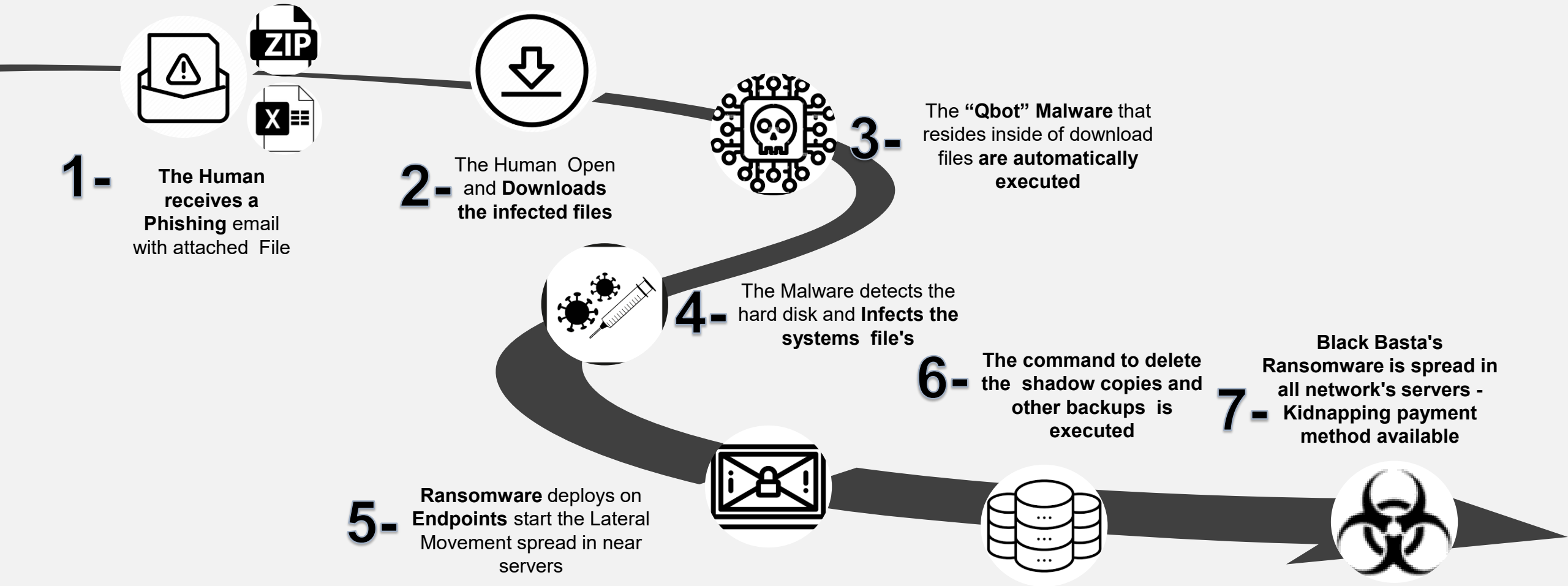
$9.4M

Avg breach cost

Source: Enterprise Strategy Group, 1. ESG Research, SOC Modernization Survey, January 2025.

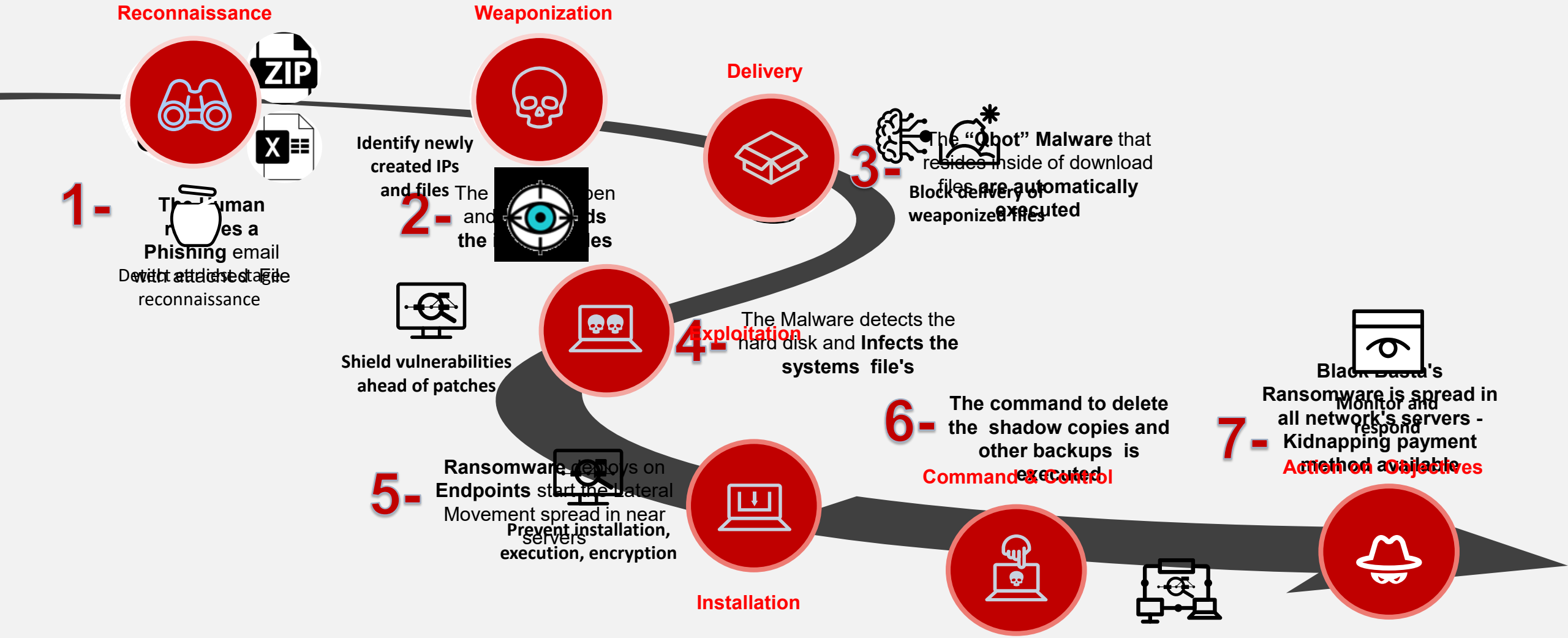
Ransomware, how it works

Black Basta´s Real Case

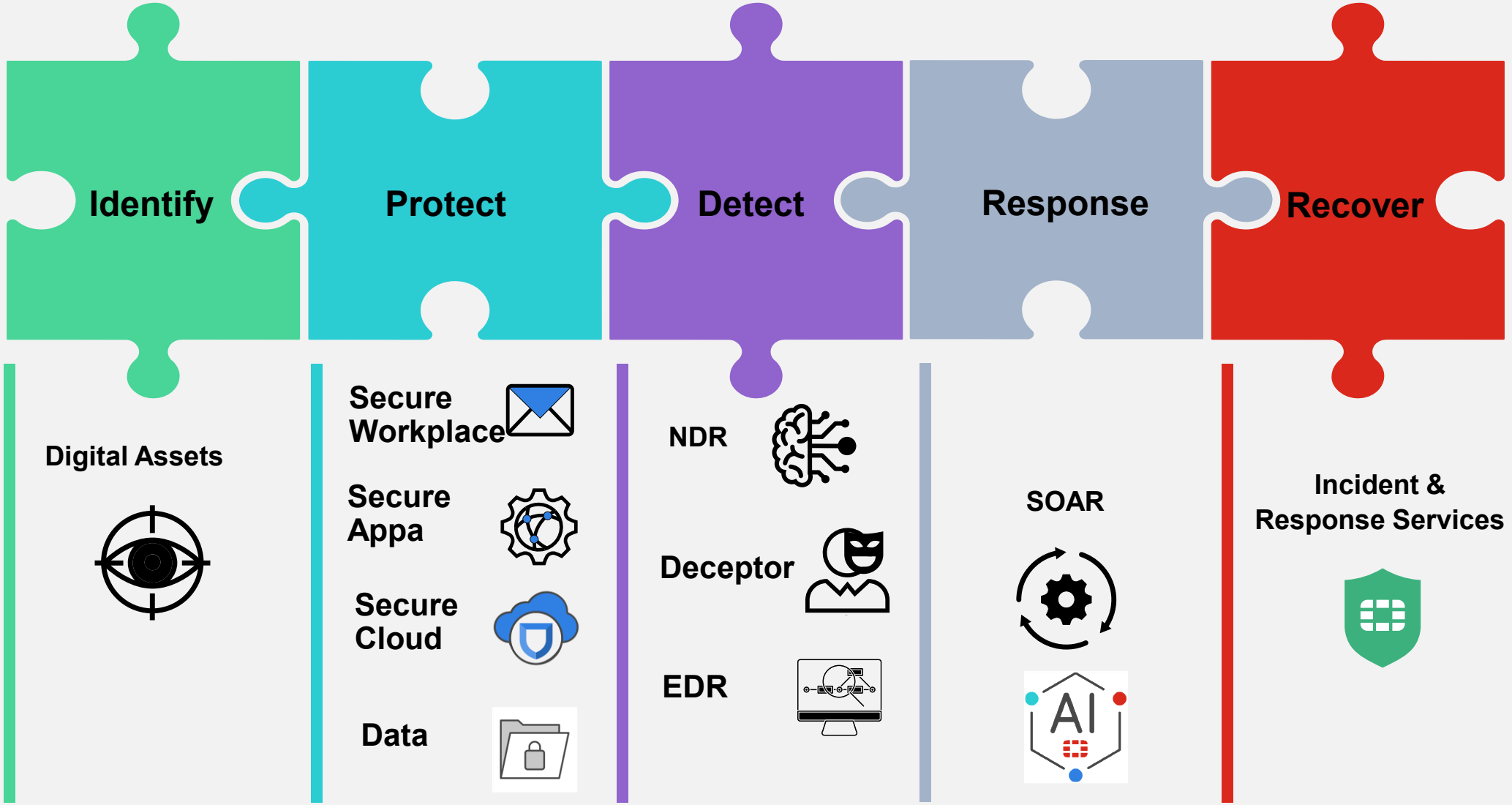


What could have been done??

Applying an adequate Anti-Ransomware security strategy



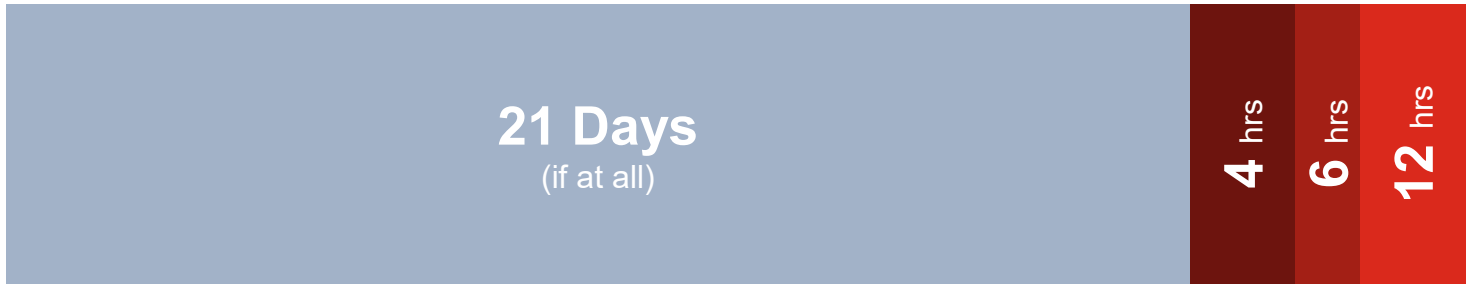
Applying NIST Model



Achieve Threat Response In Minutes, Not Weeks

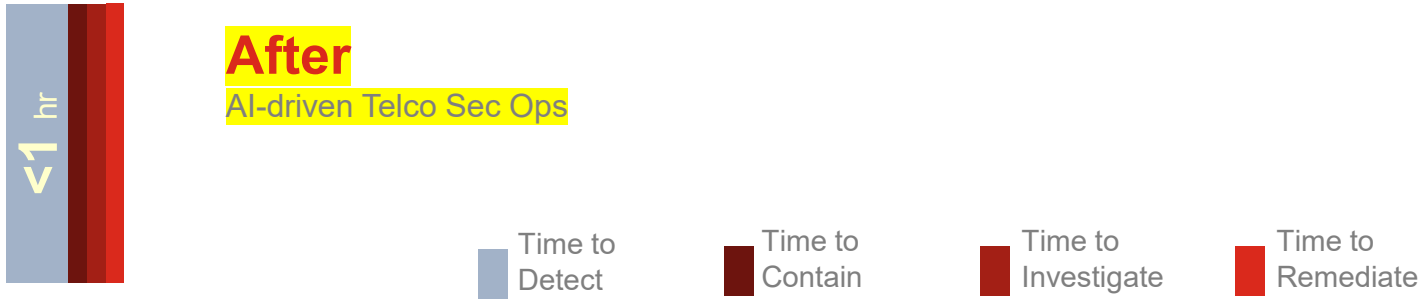
Before

Manual incident response and reporting



After

AI-driven Telco Sec Ops



Source: Enterprise Strategy Group, a division of Tech Target, Inc.

Source: Enterprise Strategy Group, 1. ESG Research, SOC Modernization Survey, January 2025

Resilient Platform

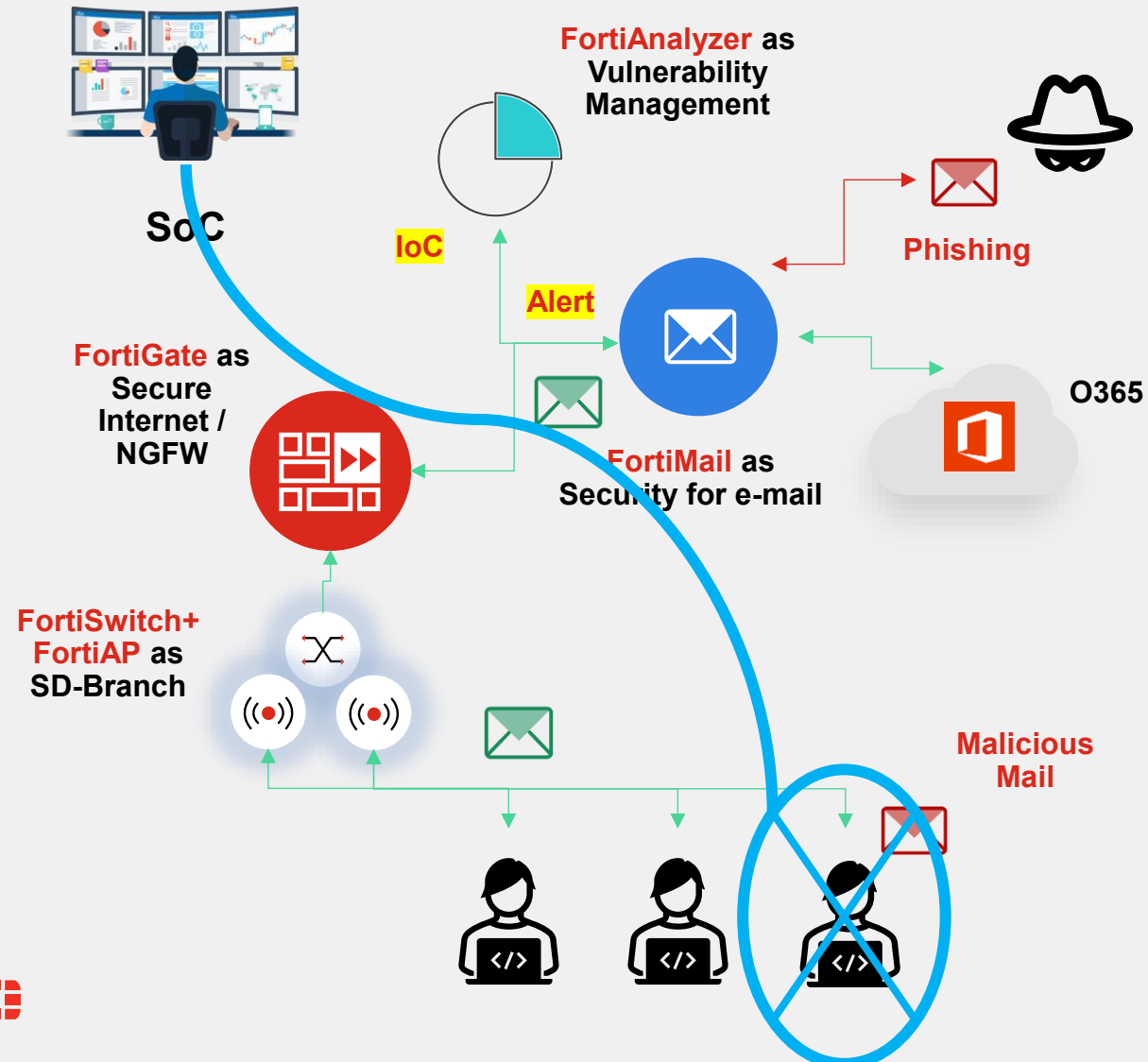
1. Platform Architecture
2. AI Powered SoC

Users

Network

Business

Step-1: Platform Architecture in Motion…



1. FortiMail Protects malicious mails incoming and Outgoing
2. User sends Credentials via Mail
3. FortiMail detects, Blocks (Data Loss Prevention), and generates alert to FortiAnalyzer (SoC)
4. FortiAnalyzer generates Indicator of compromise (IoC)
5. Telco SOC can automate an action to block this user workstation

Step-2: Integration of AI into CyberSecurity Process

Assist

AI Assisted Operations

Proactive, Automated SOC and NOC

Protect

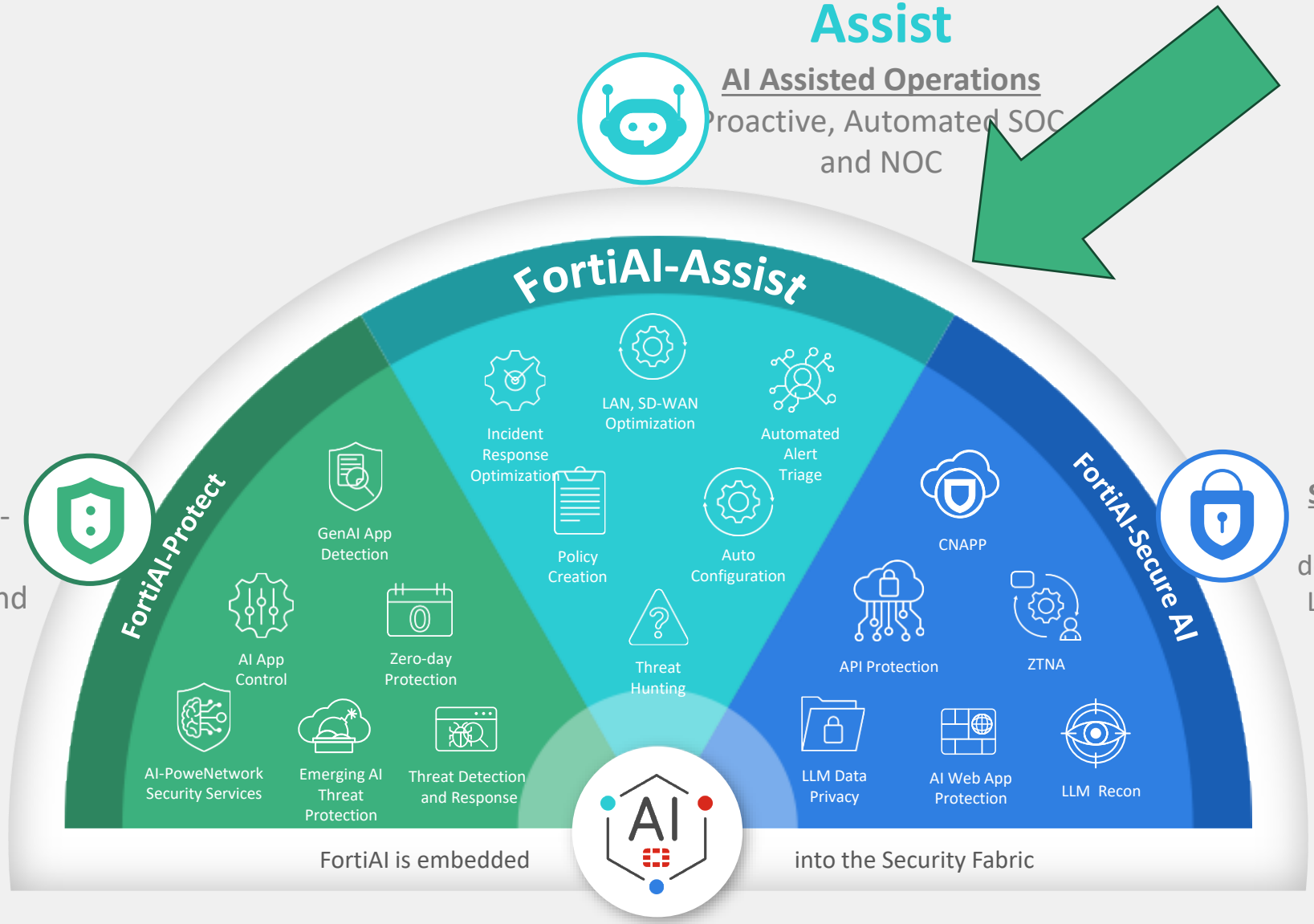
Secure AI Usage

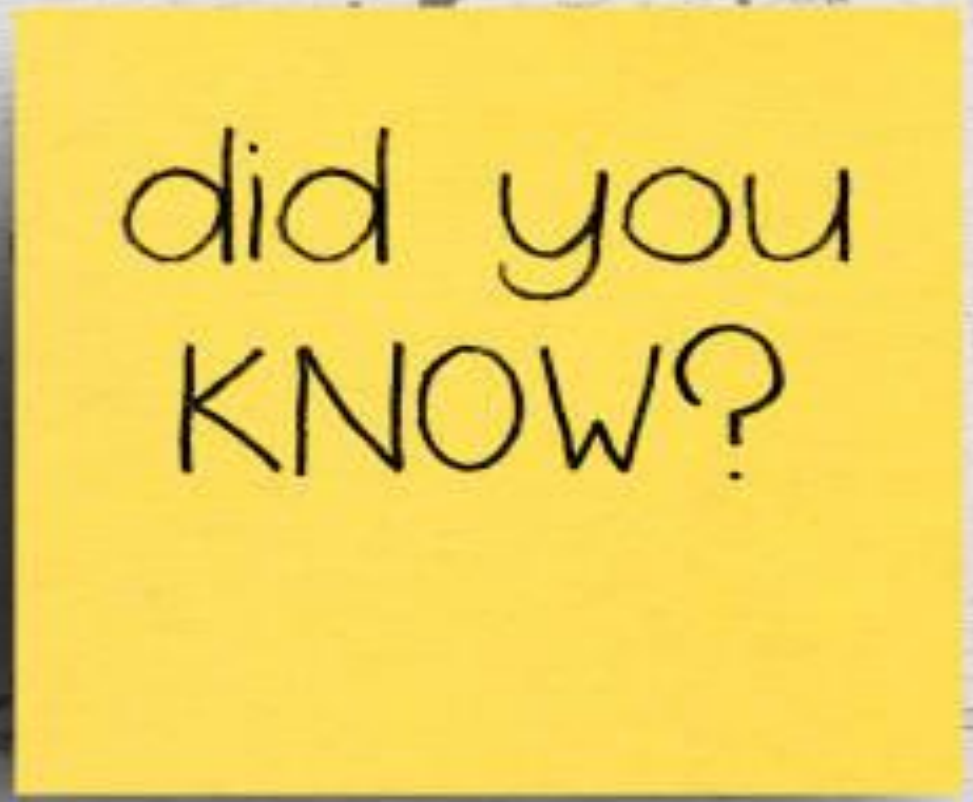
Defends against zero-day,
emerging AI threats and GenAI usage

Secure AI

Secure LLM, AI systems

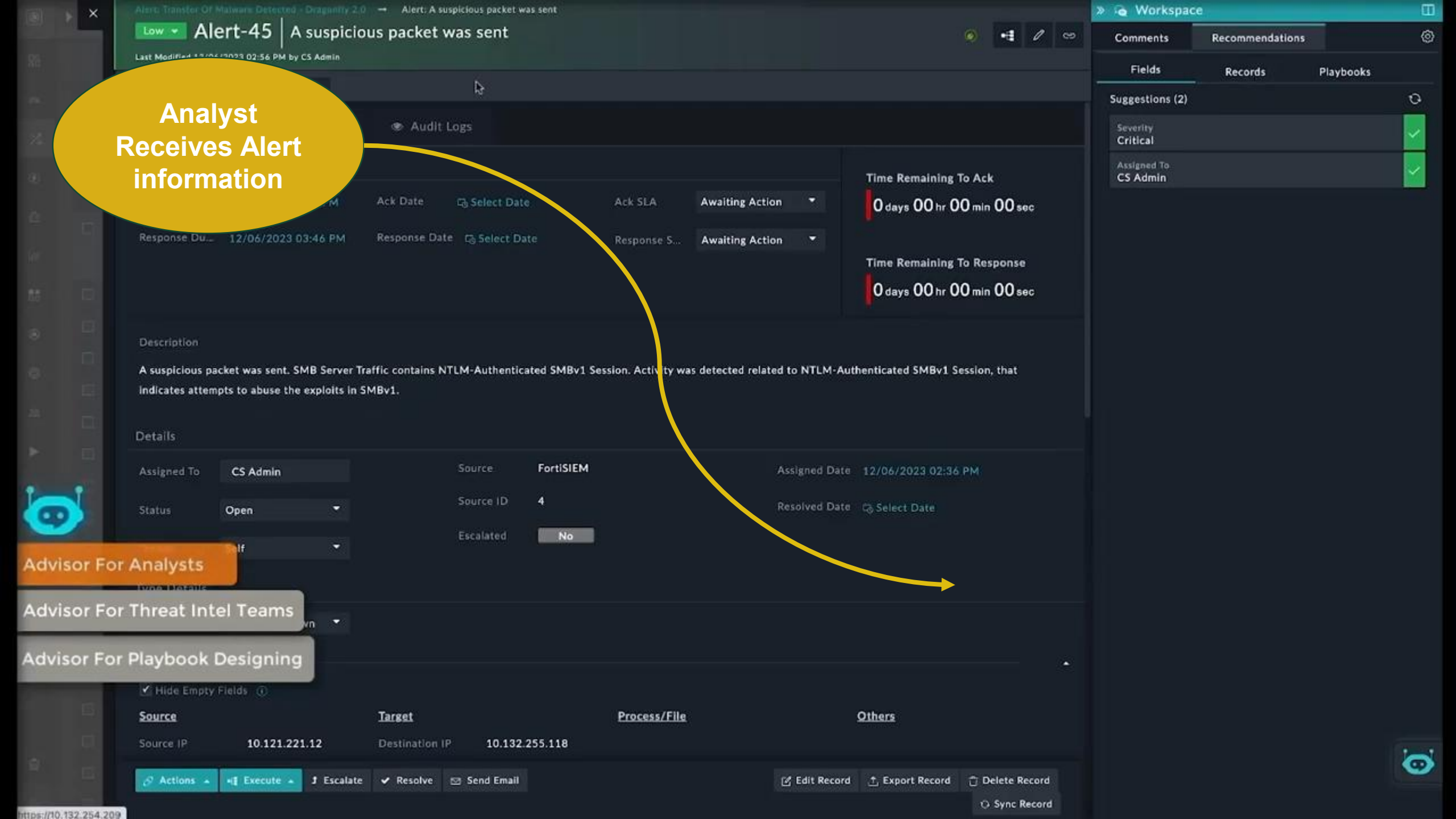
Secure by design deployment and usage of LLM Models, AI systems

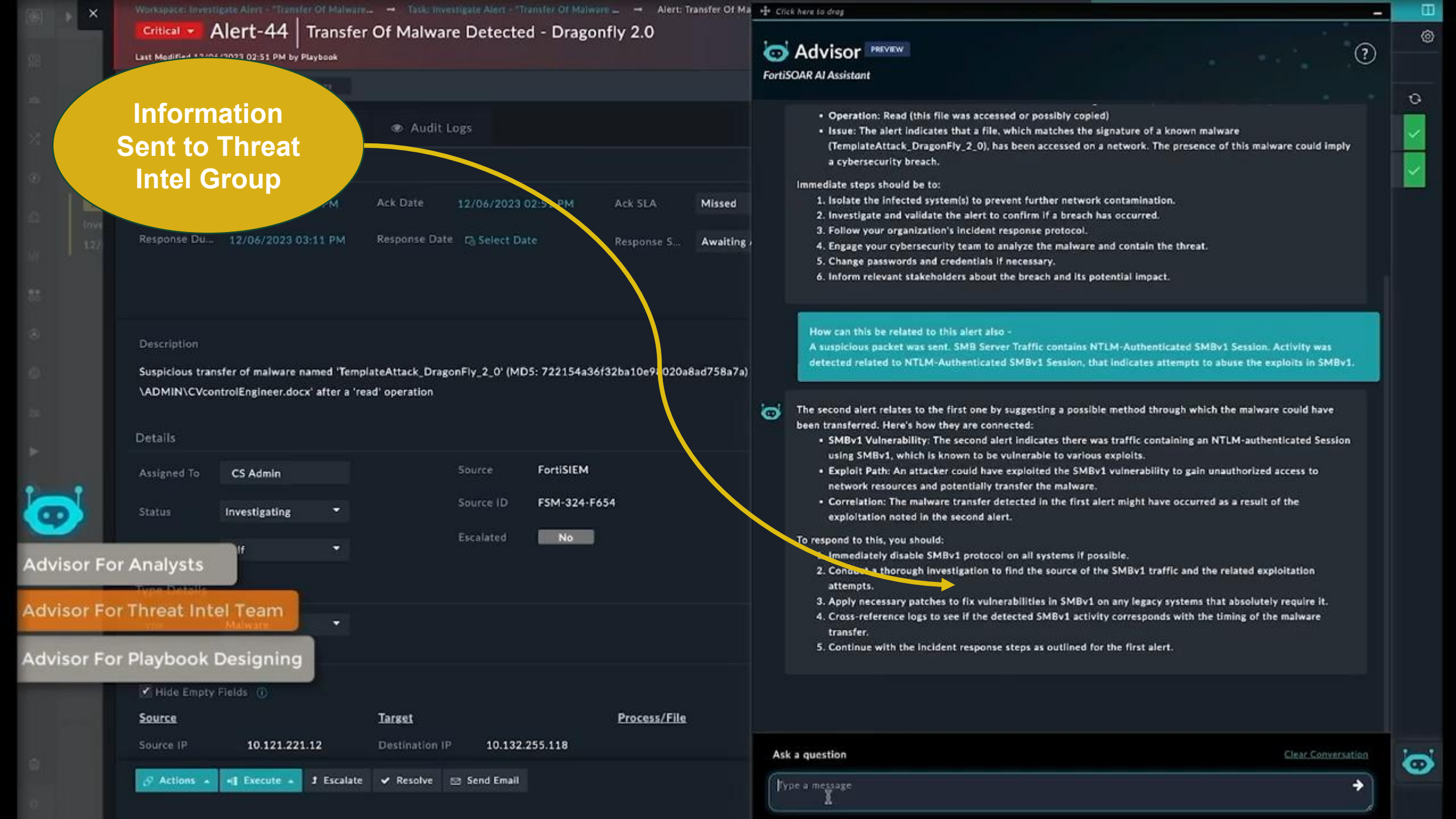


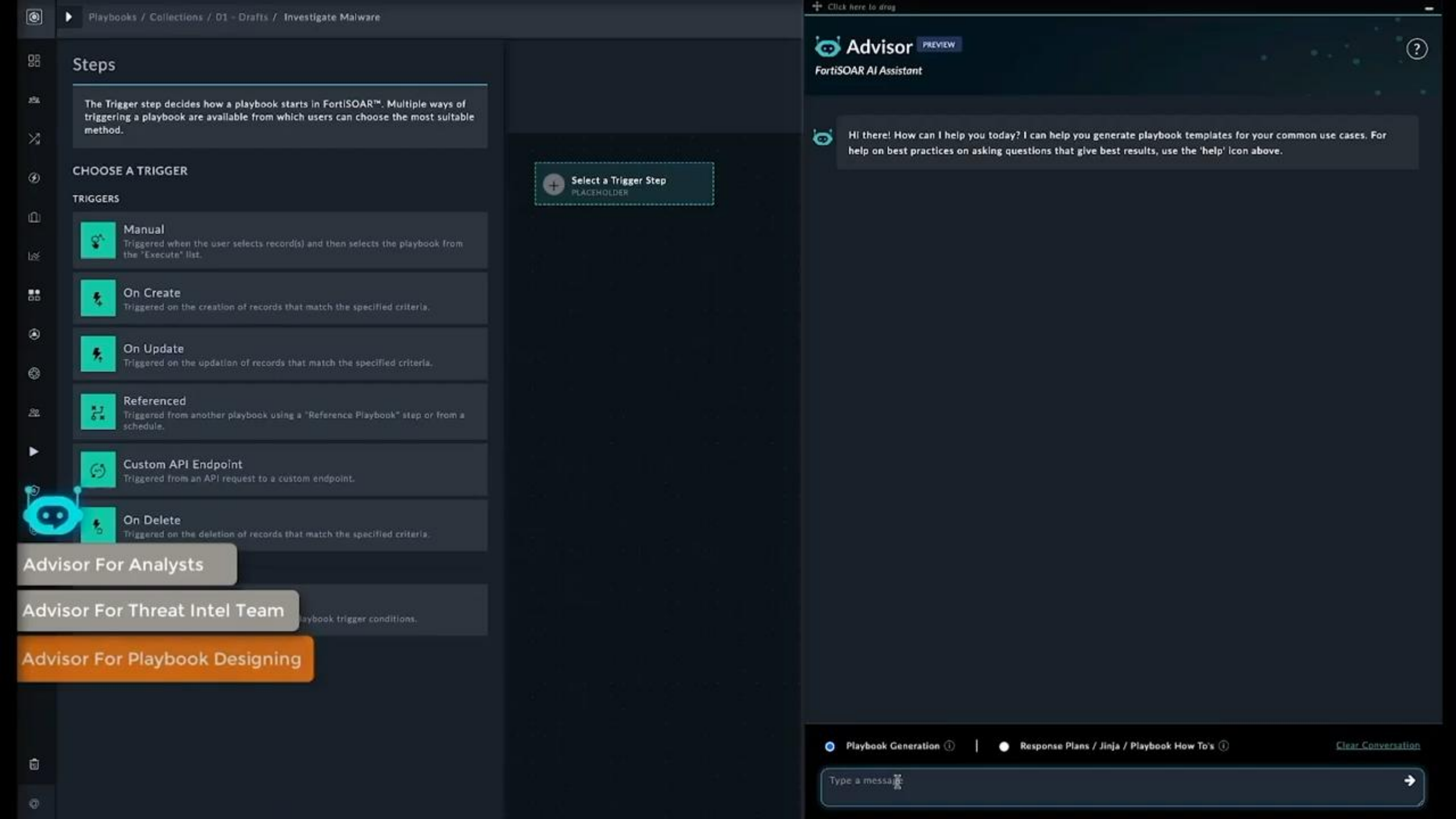


4.7 Mill CyberSecurity Professionals Gap

Source: Fortinet SyberSecurity Skills Gap report

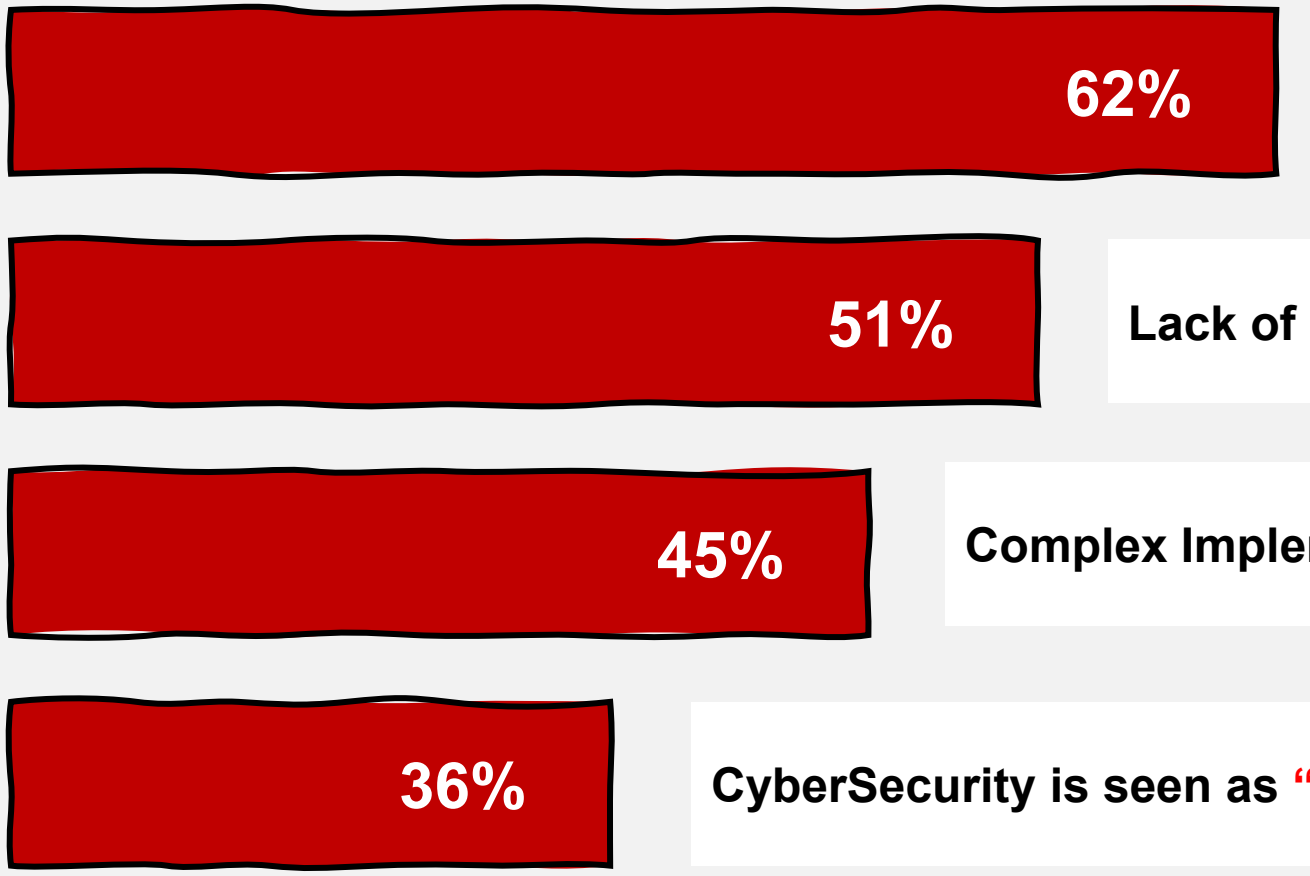

Analyst Receives Alert information
Low
Alert-45
A suspicious packet was sent
Audit Logs
Ack Date
Select Date
Ack SLA
Awaiting Action
Response Du...
12/06/2023 03:46 PM
Response Date
Select Date
Response S...
Awaiting Action
Time Remaining To Ack
0 days 00 hr 00 min 00 sec
Time Remaining To Response
0 days 00 hr 00 min 00 sec
Description
A suspicious packet was sent. SMB Server Traffic contains NTLM-Authenticated SMBv1 Session. Activity was detected related to NTLM-Authenticated SMBv1 Session, that indicates attempts to abuse the exploits in SMBv1.
Details
Assigned To
CS Admin
Source
FortiSIEM
Assigned Date
12/06/2023 02:36 PM
Status
Open
Source ID
4
Resolved Date
Select Date
Escalated
No
Advisor For Analysts
Advisor For Threat Intel Teams
Advisor For Playbook Designing
Hide Empty Fields
Source
Target
Process/File
Others
Source IP
10.121.221.12
Destination IP
10.132.255.118
Actions
Execute
Escalate
Resolve
Send Email
Edit Record
Export Record
Delete Record
Sync Record
Workspace
Comments
Recommendations
Fields
Records
Playbooks
Suggestions (2)
Severity
Critical
Assigned To
CS Admin


Information Sent to Threat Intel Group
Critical
Alert-44
Transfer Of Malware Detected - Dragonfly 2.0
Audit Logs
Ack Date
Ack SLA
Missed
Response Date
Select Date
Awaiting
Description
Suspicious transfer of malware named 'TemplateAttack_DragonFly_2_0' (MD5: 722154a36f32ba10e9
020a8ad758a7a)
\ADMIN\CVcontrolEngineer.docx' after a 'read' operation
Details
Assigned To
CS Admin
Status
Investigating
Source
FortiSIEM
Source ID
FSM-324-F654
Escalated
No
Advisor For Analysts
Advisor For Threat Intel Team
Advisor For Playbook Designing
Hide Empty Fields
Source
Target
Process/File
Source IP
10.121.221.12
Destination IP
10.132.255.118
Actions
Execute
Escalate
Resolve
Send Email
Advisor
PREVIEW
FortiSOAR AI Assistant
Operation: Read (this file was accessed or possibly copied)
Issue: The alert indicates that a file, which matches the signature of a known malware (TemplateAttack_DragonFly_2_0), has been accessed on a network. The presence of this malware could imply a cybersecurity breach.
Immediate steps should be to:
1. Isolate the infected system(s) to prevent further network contamination.
2. Investigate and validate the alert to confirm if a breach has occurred.
3. Follow your organization's incident response protocol.
4. Engage your cybersecurity team to analyze the malware and contain the threat.
5. Change passwords and credentials if necessary.
6. Inform relevant stakeholders about the breach and its potential impact.
How can this be related to this alert also -
A suspicious packet was sent. SMB Server Traffic contains NTLM-Authenticated SMBv1 Session. Activity was detected related to NTLM-Authenticated SMBv1 Session, that indicates attempts to abuse the exploits in SMBv1.
The second alert relates to the first one by suggesting a possible method through which the malware could have been transferred. Here's how they are connected:
SMBv1 Vulnerability: The second alert indicates there was traffic containing an NTLM-authenticated Session using SMBv1, which is known to be vulnerable to various exploits.
Exploit Path: An attacker could have exploited the SMBv1 vulnerability to gain unauthorized access to network resources and potentially transfer the malware.
Correlation: The malware transfer detected in the first alert might have occurred as a result of the exploitation noted in the second alert.
To respond to this, you should:
1. Immediately disable SMBv1 protocol on all systems if possible.
2. Conduct a thorough investigation to find the source of the SMBv1 traffic and the related exploitation attempts.
3. Apply necessary patches to fix vulnerabilities in SMBv1 on any legacy systems that absolutely require it.
4. Cross-reference logs to see if the detected SMBv1 activity corresponds with the timing of the malware transfer.
5. Continue with the incident response steps as outlined for the first alert.
Ask a question
Clear Conversation
Type a message


Playbooks / Collections / 01 - Drafts / Investigate Malware
Steps
The Trigger step decides how a playbook starts in FortiSOAR™. Multiple ways of triggering a playbook are available from which users can choose the most suitable method.
CHOOSE A TRIGGER
TRIGGERS
Manual
Triggered when the user selects record(s) and then selects the playbook from the "Execute" list.
On Create
Triggered on the creation of records that match the specified criteria.
On Update
Triggered on the updation of records that match the specified criteria.
Referenced
Triggered from another playbook using a "Reference Playbook" step or from a schedule.
Custom API Endpoint
Triggered from an API request to a custom endpoint.
On Delete
Triggered on the deletion of records that match the specified criteria.
Select a Trigger Step
PLACEHOLDER
Advisor PREVIEW
FortiSOAR AI Assistant
Hi there! How can I help you today? I can help you generate playbook templates for your common use cases. For help on best practices on asking questions that give best results, use the 'help' icon above.
Playbook Generation
Response Plans / Jinja / Playbook How To's
Clear Conversation
Type a message
Advisor For Analysts
Advisor For Threat Intel Team
Advisor For Playbook Designing

Barriers in Cyber-Security Adoption

What Companies say…



Limited Budget

Lack of Qualified Staff

Complex Implementations

CyberSecurity is seen as “Expense” and not as “Investment”

Source: ISC2 – Estado de Ciberseguridad LATAM 2023

Breaking Barriers with Cyber-Resillient Platform

62%	Limited Budget	Cost Optimization witn Plataform Architecture
51%	Lack of Qualified Staff	SoC powered with AI
45%	Complex Implementations	Native integrations within same Platform
36%	CyberSecurity is seen as “Expense” and not as “Investment”	Business Protection with anti-Ransomware

Source: ISC2 – Estado de Ciberseguridad LATAM 2023

Fortinet Contributes to the Sustainability of Society

SUSTAINABLE DEVELOPMENT GOALS

https://www.un.org/sustainabledevelopment/news/communications-material/

Our Environmental Commitment

Net Zero Goal

Aspiring to reach net zero emissions by 2050 across our entire value chain.

Science-Based Targets

Progressing toward SBTi-validated near-term climate targets

Product Environmental Impacts

Reducing footprint through product energy efficiency, sustainable packaging, and circular practices.

Fortinet's Path to Net Zero

Sustainable Operations

Reducing natural gas usage and transitioning to low-emissions cooling systems in our buildings.

Renewable Energy

Achieving 100% renewable electricity use in all owned sites by 2030.

Sustainable Supply Chain

Ensuring suppliers have climate programs that align with ours.

Sustainable Products

Reducing product energy consumption and embedding circular practices in our products and packaging.

[Ambitious corporate climate action - Science Based Targets Initiative]

SBTi-Validated Near-Term Climate Targets

58.8%

Emissions Reduction Target

Absolute reduction of Scope 1 and 2 emissions by 2030 from a 2021 base year.

60.5%

Supplier Engagement

Of suppliers (by spend) will have science-based GHG emissions reduction targets by 2029.

69.2%

Customer Engagement

Of customers (by revenue) will have science-based GHG emissions reduction targets by 2029.

Fortinet Contributes to the Sustainability of Society

Addressing Cybersecurity Risk to Society

Global Partnerships and Collaboration

Joint Cyber Defense Collaborative · NATO OTAN · MITRE ENGENUITY · Cyber Threat Alliance · FIRST · World Economic Forum · INTERPOL · Center for Cybersecurity Policy and Law

Respecting the Environment

Pledge

NET ZERO

by 2030
Fortinet owned facilities

by 2050
across value chain

88%
less power consumption over industry-standard CPUs

REACH Compliance · RoHS · U.S. Securities and Exchange Commission · WEEE

Closing the Cybersecurity Skills Gap

Pledge

1 Million

people trained in cybersecurity by

2026

Women in Cybersecurity · WiCyS · Women 4 Cyber · TechVets · WOMCY Latam Women in Cybersecurity

600+
schools across 98 countries

Promoting Responsible Business

100%

of our key contract manufacturers trained on our compliance and ethics standards

FORTINET
Trusted Resource Center

CSA STAR · GDPR · HIPAA · ISMAP · ISO 27001 · ISO 27001 SoA · ISO 9001 · SOC 2 · TISAX · VPAT

FORTINET

¡Thank you!