AlertIQ - FPT Security Operation Platform Introduction

February 2022

PROBLEMS

So many alerts, so little times

- **55%** enterprises see more than **10,000 alerts** per day, while **27%** of enterprises see more than **1 million** alerts per day.
- **64%** of threat alerts are not addressed each day.
- In 2020, It takes more than **24 days** to detect attacker activities.

Lack of context

- **46%** of incidents are automatically classified as "**critical**" alerts, but in fact, only about **1-5%** of alerts should be categorized as **"critical"**
- Analysts waste **over half of their day** looking for problems that are either insignificant or not really problems at all.

Lack of skilled staff

- **54%** enterprise feel they are forced to **ignore security alerts** worthy further investigation because **they don't have staff and experience** to handle them.

OUR SOLUTIONS FOR BUSINESS NEEDS

MDRx

Fully managed detection and response service for business protection.

- **MDR for Cloud**: AWS, Azure and Office365 security monitoring
- **MDR for Endpoint**: Endpoint security monitoring based on VMWare Carbon Black and Microsoft Defender for Endpoint

SOC-as-a-Service

Security monitoring and detection, 24x7 SOC with tailored incident response service

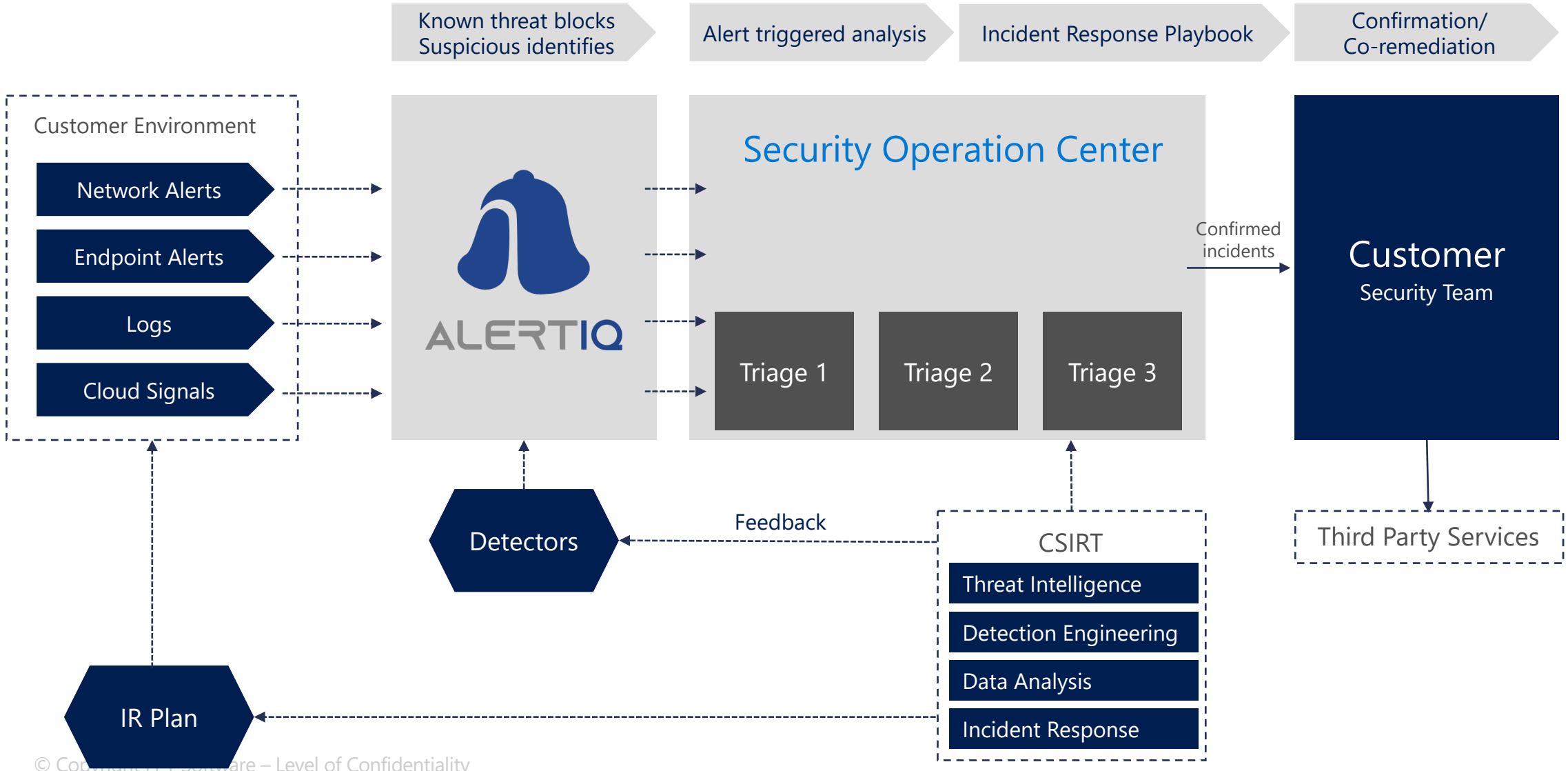
- Support IBM QRadar, Splunk and Azure Sentinel.
- Incident Response playbook design and development

Add-on Services

Bundled managed security service for enhancing your security programs

- Managed security vulnerability (internal/external)
- Managed Web Application Firewall
- Managed SIEM
- Operate security infrastructure solutions
- Detection engineering service

HOW DOES SERVICE WORKS?



ALERTIQ - FPT SECURITY OPERATION PLATFORM

MDR for Endpoint

MDR for Cloud

SOC-as-a-Service

ALERTIQ

RECORD	DETECT	INVESTIGATE	ACT
• High-volume Telemetry Collection • Normalization and Filtering	• Applied Threat Intelligence • Behavioral Analytics	• Alert Triage and Enrichment • Alert Suppression	• Automated Response • Notification and Support
	Threat Researchers	Detection Engineers	Threat Researchers

EDR: vmware Carbon Black, Microsoft

SIEM: IBM QRadar, Microsoft, splunk>

CLOUD: aws, Azure

HOW CAN WE HELP?

Capability	FPT Managed Service	Other MSSP
Onboarding time	Less than 1 week	Months
Monitoring technology	Customer's existing security tools	MSSP vendor’s proprietary tech stack
What you get	Answers that tell you what to do	Alerts you need to investigate
How you measure value	Security operations dashboard	# of alerts on PPTX graph
Customer portal	Rich, real-time and collaborative	Limited after-the-fact data
Transparency	You see exactly what our analysts see	N/A
Resilience recommendations	Actions to improve long-term security	N/A
Remediation guidance	Detailed findings reports	N/A
Proactive threat hunting	Yes	N/A

WHY ARE WE DIFFERENT?

01. Got Confirmed Threats, Not Alerts

02. Deploy in Minutes Get Results in Weeks

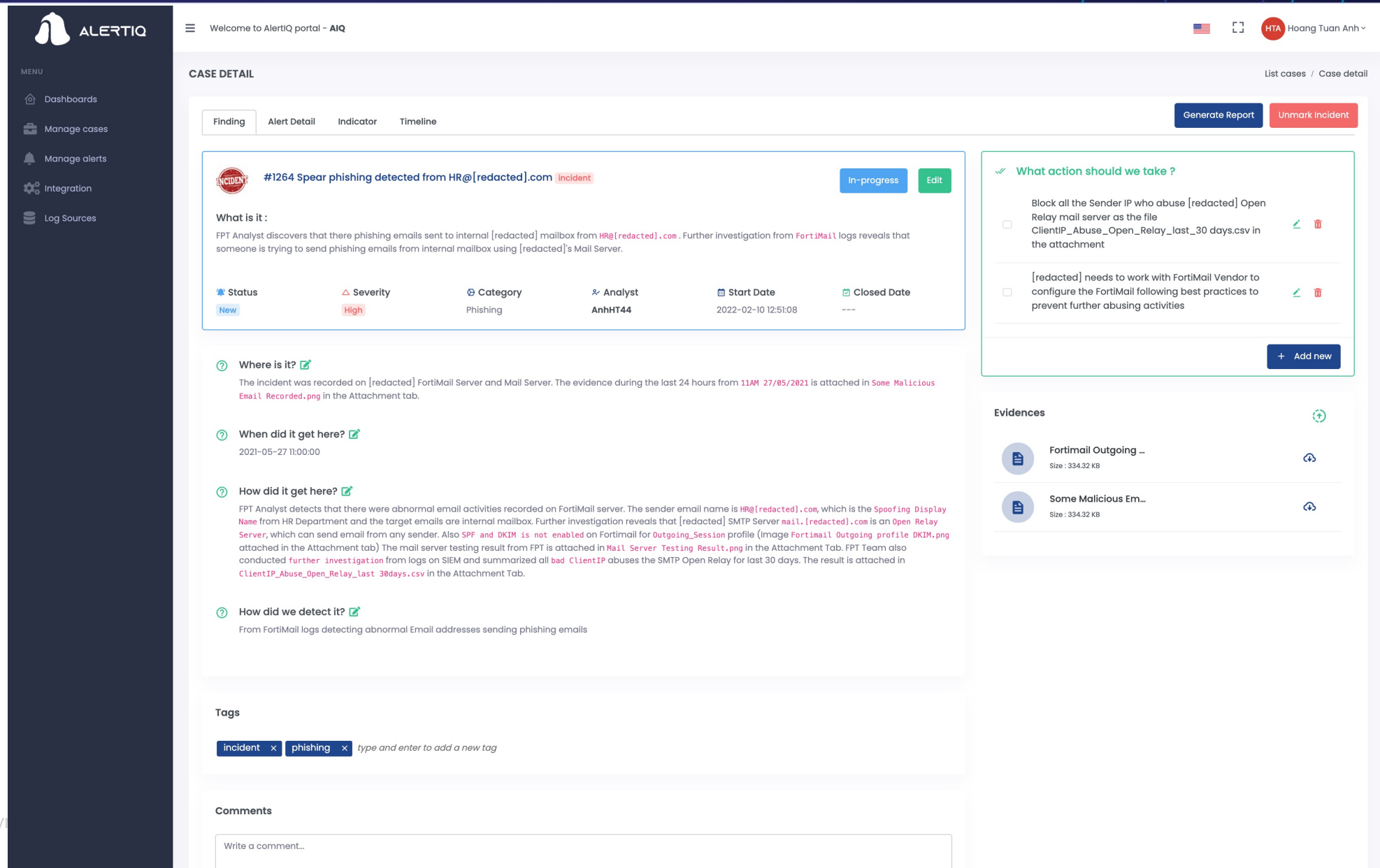
03. Fully Transparent

04. Highly Certified Expertise

05. Predictable Pricing Model

06. End-to-End Managed Support

FULLY TRANSPARENT MANAGED SECURITY



OUR SERVICE BY THE NUMBERS

Number of endpoints: 2000

With FPT Security Operation Platform - AlertIQ, we reduce significant number of alerts, eliminate noise and help customer only spend time on real threats while focusing on business-critical missions.

* This is the actual number from our customer for the last month.

12