



AlertIQ - FPT Security Operation Platform Introduction

February 2022



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.



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

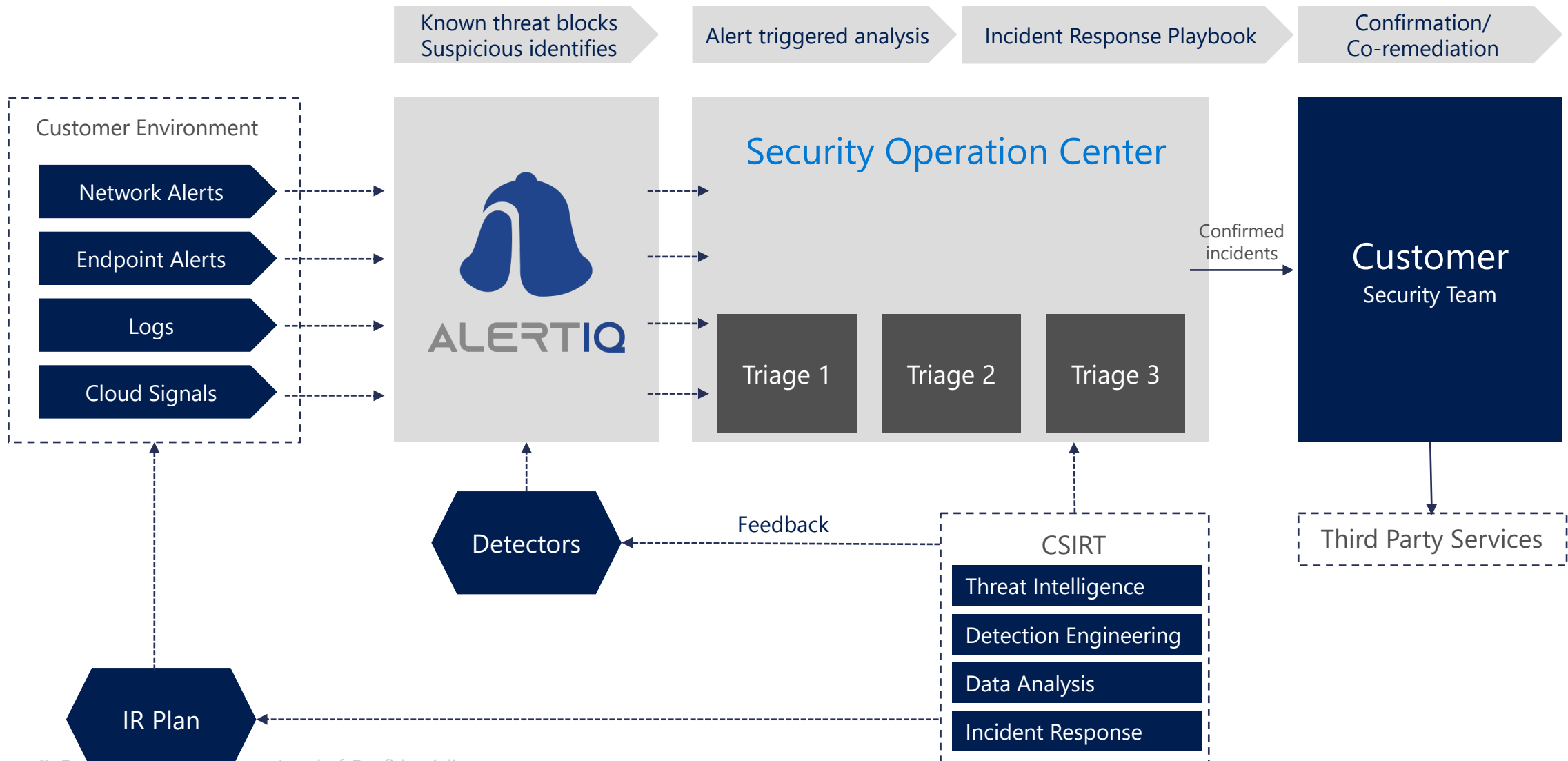


Add-on Services

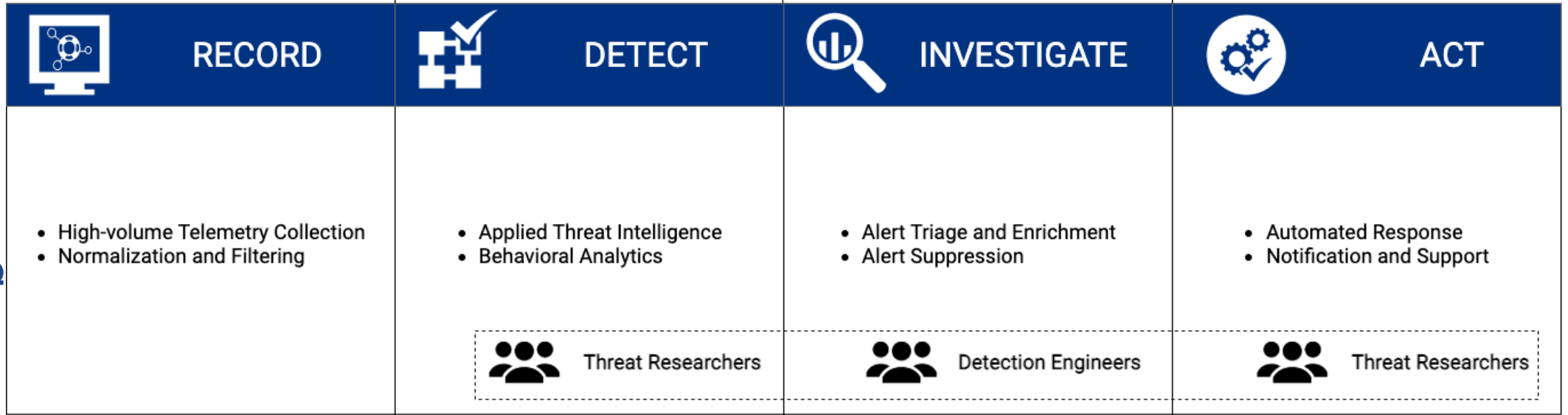
Bundled managed security service for enhancing your security programs

- 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



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



Welcome to AlertIQ portal - AIQ

HTA Hoang Tuan Anh

- Dashboards
- Manage cases
- Manage alerts
- Integration
- Log Sources

CASE DETAIL

List cases / Case detail

- Finding
- Alert Detail
- Indicator
- Timeline

Generate Report Unmark Incident

#1264 Spear phishing detected from HR@[redacted].com Incident In-progress Edit

What is it:
FPT Analyst discovers that there phishing emails sent to internal [redacted] mailbox from HR@[redacted].com. Further investigation from FortiMail logs reveals that someone is trying to send phishing emails from internal mailbox using [redacted]'s Mail Server.

Status	Severity	Category	Analyst	Start Date	Closed Date
New	High	Phishing	AnhHT44	2022-02-10 12:51:08	---

What action should we take ?

- Block all the Sender IP who abuse [redacted] Open Relay mail server as the file ClientIP_Abuse_Open_Relay_last_30 days.csv in the attachment
- [redacted] needs to work with FortiMail Vendor to configure the FortiMail following best practices to prevent further abusing activities

+ Add new

- Where is it?**
The incident was recorded on [redacted] FortiMail Server and Mail Server. The evidence during the last 24 hours from 11AM 27/05/2021 is attached in **Some Malicious Email Recorded.png** in the Attachment tab.
- When did it get here?**
2021-05-27 11:00:00
- How did it get here?**
FPT Analyst detects that there were abnormal email activities recorded on FortiMail server. The sender email name is HR@[redacted].com, which is the **Spoofing Display Name** from HR Department and the target emails are internal mailbox. Further investigation reveals that [redacted] SMTP Server mail.[redacted].com is an **Open Relay Server**, which can send email from any sender. Also **SPF and DKIM is not enabled** on Fortimail for **Outgoing_Session** profile (image **Fortimail Outgoing profile DKIM.png** attached in the Attachment tab) The mail server testing result from FPT is attached in **Mail Server Testing Result.png** in the Attachment Tab. FPT Team also conducted **further investigation** from logs on SIEM and summarized all **bad ClientIP** abuses the SMTP Open Relay for last 30 days. The result is attached in **ClientIP_Abuse_Open_Relay_Last_30days.csv** in the Attachment Tab.
- How did we detect it?**
From FortiMail logs detecting abnormal Email addresses sending phishing emails

- ### Evidences
- Fortimail Outgoing ...**
Size : 334.32 KB
 - Some Malicious Em...**
Size : 334.32 KB

Tags: incident x phishing x type and enter to add a new tag

Comments

Write a comment...

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.

Questions?

