FORTINET

Úvod

Václav Molík

Major Account Manager – Telco/ISP

Rekapitulace – Fortinet na KKDS

KKTS Plzeň 9/18	Kybernetická bezpečnost – Výzvy a příležitosti pro ISP
KKTS Olomouc 5/22	Nabídka Fortinet pro ISP
KKTS Plzeň 9/22	(1) Návrh řešení DR projektu pro RETE internet s.r.o. (2) FortiGate v síti ISP
KKDS Olomouc 4/23	Jak mohou nejen ISP splnit požadavky NIS2
KKDS Plzeň 9/23	SOC formou služby

SECURITY/NETWORK OPERATING CENTER

FortiAnalyzer – Central Log & report

FortiNAC – IoT Access Control

FortiSandbox – File Analysis

FortiNDR – Virtual Security Analyst ™

FortiSIEM – SIEM / UEBA

FortiXDR – XDR

FortiManager – Central Device Mgmt.

FortiAuthenticator – User Access Mgmt.

FortiTester – Network Tester

FortiDeceptor – Honeypot

FortiSOAR – SOAR

HOSTED SERVICES

Cloud mgmt.

FortiGate Cloud | FortiLAN Cloud | FortiExtender Cloud | FortiManager Cloud | FortiAnalyzer Cloud | FortiClient EMS Cloud | FortiToken Cloud | FortiSOAR Cloud

Cloud services

FortiPresence | FortiMail Cloud | FortiPhish | FortiGSLB | FortiConverter | Fortinet SOCaaS | FortiSASE | FortiPenTest | FortiWeb Cloud | FortiSandbox Cloud | FortiVoice Cloud | FortiMonitor

MOBILE USERS

FortiToken – 2 Factor OTP Token

FortiClient / FortiEDR – VPN, ZTNA, EPP, and SASE Client

FortiCASB

FortiCNP

SaaS

Secure SD-WAN

IPsec / SSL VPN

SASE

FortiGate – Security Gateway

ZTNA

FortiDDoS – L7 D/DOS Mitigator

FortiADC – Load Balancer

FortiMail – Mail Sec. Gateway

FortiWeb – Web App. Firewall

BRANCH OFFICE

FortiWiFi – Secure WiFi Access

FortiExtender – 3G/4G/5G WAN

LAN

FortiSwitch – Switch

FortiAP – Wireless Access Point

FortiRecorder – Surveillance Manager

FortiVoice – IP PBX

FortiIsolator – Browser Isolation

FortiProxy – Secure Web Gateway

CLICK ON PRODUCT NAME TO JUMP ONTO ITS SECTION

FortiCamera

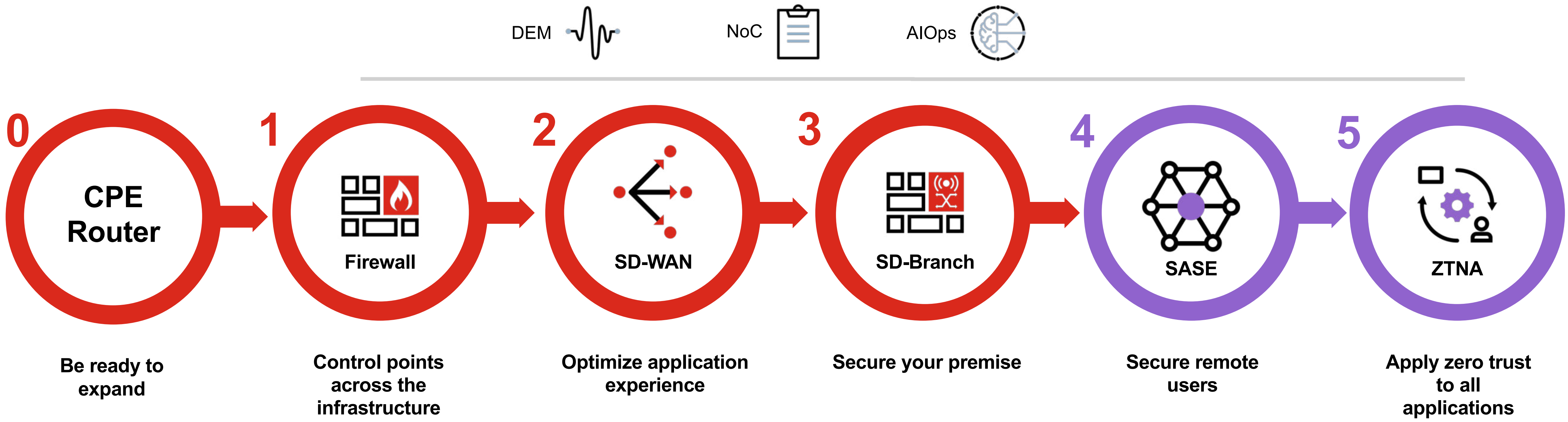
FortiFone

DATA CENTER

Secure Networking

Secure Networking Journey

The convergence of networking and security across WLAN, LAN, SD-WAN, ZTNA, SASE, and network firewall enables networking that is location, user, device, content, and application aware.



DEM

NoC

AIOps

0 CPE Router — Be ready to expand

1 Firewall — Control points across the infrastructure

2 SD-WAN — Optimize application experience

3 SD-Branch — Secure your premise

4 SASE — Secure remote users

5 ZTNA — Apply zero trust to all applications

FortiGate Entry-level NGFW Family

	40F Series	60F Series	70F Series	80F Series	90G Series
Interfaces	5x GE RJ45	10x GE RJ45	10x GE RJ45	8x GE RJ45; 2x RJ45/SFP	8x GE RJ45; 2x 10GE RJ45/SFP+
Standard	✓	✓	✓	✓	✓
WiFi	✓	✓	✓	✓	
3G/4G	✓		✓	✓	
Bypass				✓	
DSL				✓	
POE				✓	
Storage		✓	✓	✓	✓

FortiConverter Service is available for all FortiGate migrations

FortiGate to FortiGate: 4 hours *3rd-party to FortiGate: 1-2 days*

FortiGate Entry Level Series - Overview

Feature-rich Security Appliances For Small/Home Offices & Small Branch Offices

- FG-90G Series
- FG/FWF- 80F Series
- FG-70F Series
- FG/FWF- 60F Series
- FG/FWF- 40F Series

NGFW

Secure SD-WAN

5 Gbps – 28 Gbps
Firewall throughput

800 Mbps – 2.5 Gbps
NGFW Throughput

1 Gbps – 4.5 Gbps
IPS Throughput

600 Mbps – 2.2 Gbps
Threat Protection Throughput

10GE RJ45 | 10GE SFP+ | GE RJ45 | GE RJ45 PoE/+ | GE SFP
Variants: WiFi | In-built 3G4G | In-built DSL | Ruggedized

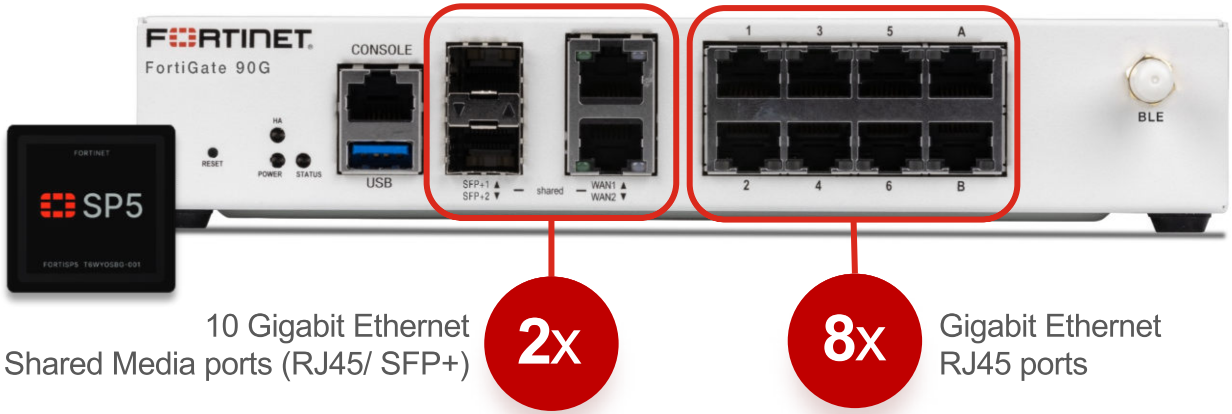
Introducing the FortiGate 90G Series

First SP5-powered FortiGate for distributed branches

Far outperforms the competition with Fortinet's latest ASIC technology

Only firewall in its class with 10GE ports for faster and more secure connections

Converged security and networking to support Hybrid Mesh Firewall deployment across branches



10 Gigabit Ethernet
Shared Media ports (RJ45/ SFP+)

2x

8x

Gigabit Ethernet
RJ45 ports

	Industry Average	FortiGate 90G	Security Compute Rating
Firewall Throughput	3.13 Gbps	**28 Gbps**	**9x**
NGFW Throughput	0.96 Gbps	**2.5 Gbps**	**2.6x**
IPsec VPN Throughput	1.53 Gbps	**25 Gbps**	**16.3x**
Threat Protection Throughput	0.98 Gbps	**2.2 Gbps**	**2.3x**
Concurrent Sessions	0.85 Million	**1.5 Million**	**1.8x**
Connections Per Second	31,000	**124,000**	**4x**

Note: Performance numbers taken from external datasheets to match as close as possible and different testing methodologies may be applied by different vendors.

FortiGate Mid-Range Series - Overview

High-Performance, Top-Rated Network Security for Mid-Sized Enterprises

- FG-900G Series
- FG-600E/F Series
- FG-400E/F Series
- FG-200E/F Series
- FG-100F Series

NGFW

Secure SD-WAN

SWG *(600 series+)*

IPS *(600 series+)*

20 Gbps – 164 Gbps
Firewall throughput

1.6 Gbps – 22 Gbps
NGFW Throughput

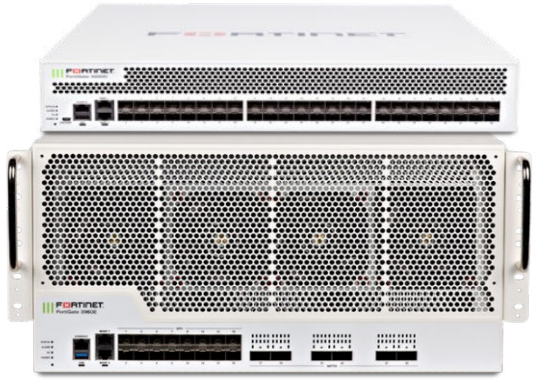
2.6 Gbps – 26 Gbps
IPS Throughput

1 Gbps – 20 Gbps
Threat Protection Throughput

GE RJ45 | GE SFP | 10GE SFP+ | 25GE SFP28

FortiGate High End Series - Overview

Data Center Firewall / Large Enterprise NGFW with High-Speed Interfaces



- FG-4000F Series
- FG-3000E/F Series
- FG-2000E/F Series
- FG-1000E/F Series

NGFW, IPS

Segmentation

SWG

Mobile Security

80 Gbps – 3.1 Tbps
Firewall throughput

9 Gbps – 82 Gbps
NGFW Throughput

11.5 Gbps – 94 Gbps
IPS Throughput

5.4 Gbps – 75 Gbps
Threat Protection Throughput

GE RJ45 | GE SFP
10GE SFP+
25GE SFP28
40GE QSFP+
100GE QSFP28
200GE QSFP56
400GE QSFP-DD

Limited Availability!

FortiExtender Vehicle for Secure Mobility

Semi-Rugged FortiExtender with integrated Wi-Fi for Mobile Fleets

Vehicle	211F
Price	$1,975
Cellular	CAT-12 LTE
Top D/L Speed	600Mbps
Deployment	Vehicle/OT
Benefit	Wi-Fi, Dual-SIM Public Safety
Connection	7-36VDC
Support	North America/Global

Překvapení na Fortinet stánku

BEEFEATER
LONDON
LONDON DRY GIN
DISTILLED IN THE HEART OF THE CITY
5cl ℮ MONTFORD PLACE LONDON SE11 5DE 40% vol.

Pozvání na Fortinet Security Day

https://events.fortinet.com/SecurityDayPraha

FORTINET

Security Day

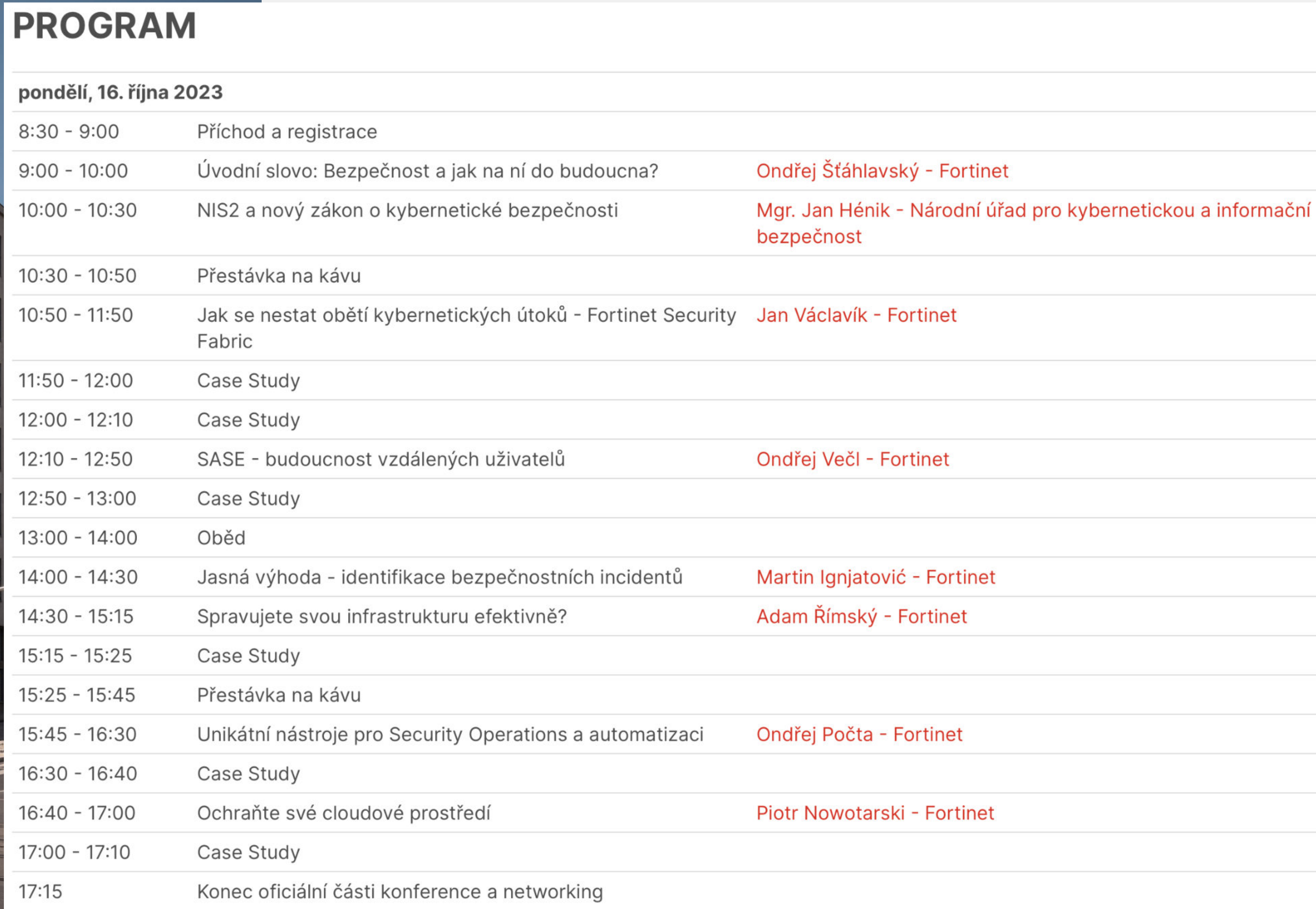
Pozvánka na naši největší zákaznickou konferenci

Fortinet Security Day
16.10. 2023 Veletržní palác, Praha 7

NASKENUJ MĚ!

Pozvání na Fortinet Security Day - 16.10. 2023

Národní galerie - Praha



PROGRAM

pondělí, 16. října 2023		
8:30 - 9:00	Příchod a registrace	
9:00 - 10:00	Úvodní slovo: Bezpečnost a jak na ní do budoucna?	Ondřej Šťáhlavský - Fortinet
10:00 - 10:30	NIS2 a nový zákon o kybernetické bezpečnosti	Mgr. Jan Hénik - Národní úřad pro kybernetickou a informační bezpečnost
10:30 - 10:50	Přestávka na kávu	
10:50 - 11:50	Jak se nestat obětí kybernetických útoků - Fortinet Security Fabric	Jan Václavík - Fortinet
11:50 - 12:00	Case Study	
12:00 - 12:10	Case Study	
12:10 - 12:50	SASE - budoucnost vzdálených uživatelů	Ondřej Večl - Fortinet
12:50 - 13:00	Case Study	
13:00 - 14:00	Oběd	
14:00 - 14:30	Jasná výhoda - identifikace bezpečnostních incidentů	Martin Ignjatović - Fortinet
14:30 - 15:15	Spravujete svou infrastrukturu efektivně?	Adam Římský - Fortinet
15:15 - 15:25	Case Study	
15:25 - 15:45	Přestávka na kávu	
15:45 - 16:30	Unikátní nástroje pro Security Operations a automatizaci	Ondřej Počta - Fortinet
16:30 - 16:40	Case Study	
16:40 - 17:00	Ochraňte své cloudové prostředí	Piotr Nowotarski - Fortinet
17:00 - 17:10	Case Study	
17:15	Konec oficiální části konference a networking	

FORTINET®

FortiCloud SOCaaS

Ondřej Večl

Senior Systems Engineer

MÁTE SOC?
A MOHLA BYCH HO VIDĚT?

Ecosystem Complexity Trends

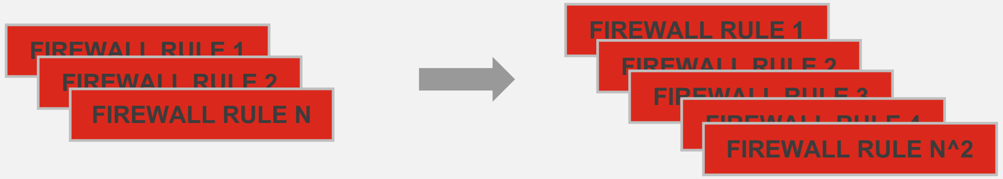
Volume of Alerts & Lengthy Manual Processes

The magnitude of alerts to investigate mask threats & are layered with countless manual workflows – **producing increased vulnerabilities, false positives & alert fatigue**

Skill Shortage & Lack of Team Collaboration

Organizations **are struggling with retaining and acquiring senior level staff –** Cybersecurity **teams experience difficulty cohesively working together**, often due to silos created by technology

Firewall Complexity



Through 2025, policy **misconfigurations**, not firewall flaws, will remain the cause of **99%** of firewall breaches and bypasses.[2]

The Demand for Automation

Organizations experiencing complexities require machine assistance to reduce TCO, improve efficiency, and security posture. By 2025, more than 90% of enterprises will have an **automation architect** [1]

[1] **Gartner**: Top 10 Trends Impacting Infrastructure and Operations for 2020 Published 14 April 2020 - ID G00464437

SOCaaS At a Glance

Cloud-based log monitoring, incident triage and escalation service with direct access to highly trained experts, cloud portal, reports, security hardening

Cloud Managed SOC

- **24x7** monitoring, incident triage and escalation
- Remediation recommendations
- Live expert support
- Reports
- Cloud **Service Portal**

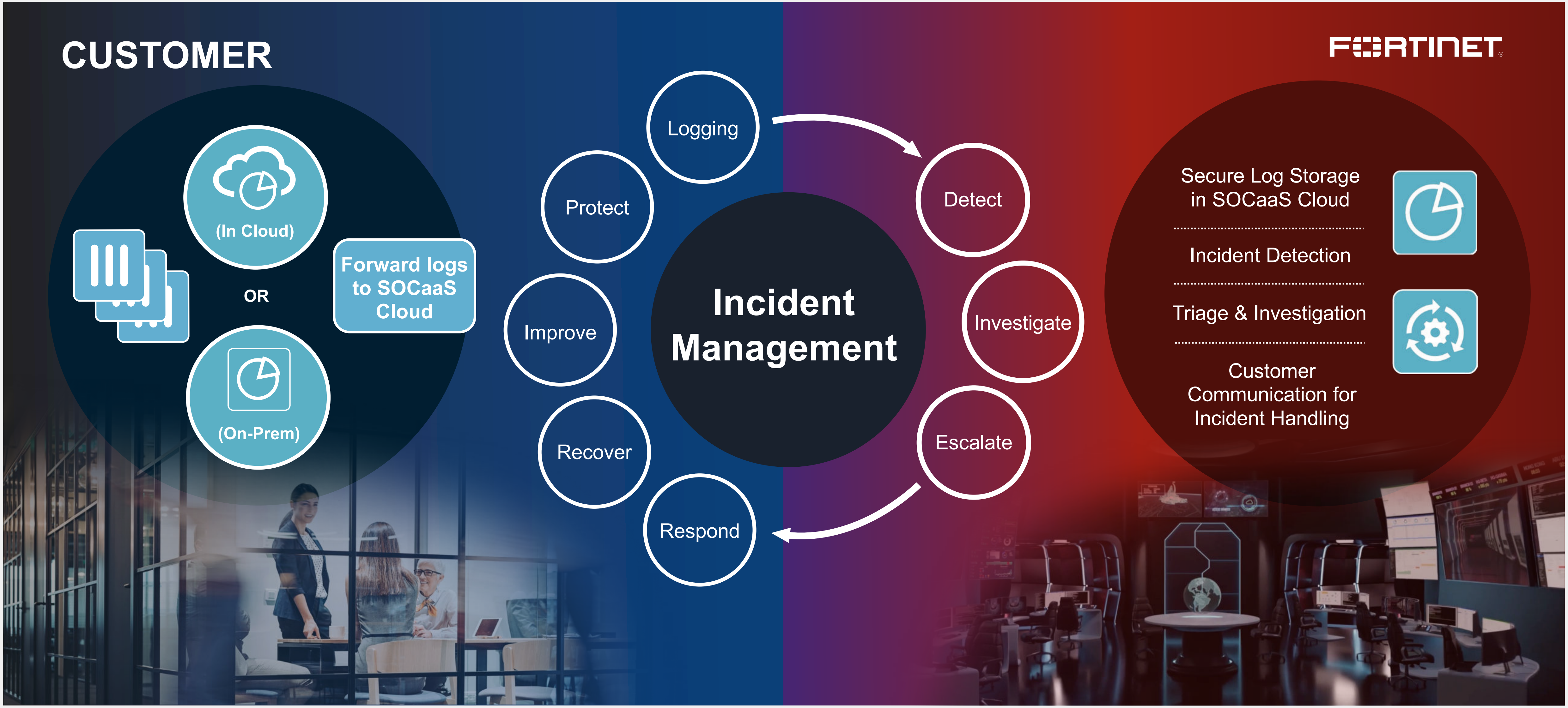
Hardening Best Practices

- Logging Best Practices
- Health Monitoring
- Tuning Recommendations
- Security Posture Review

MITRE Mapped Use Case

- Compromised Hosts
- Malware Detection
- Unauthorized Access
- Policy Violation
- Botnet / C&C
- Lateral Movement

SOCaaS Overview – Where we fit



Service Locations

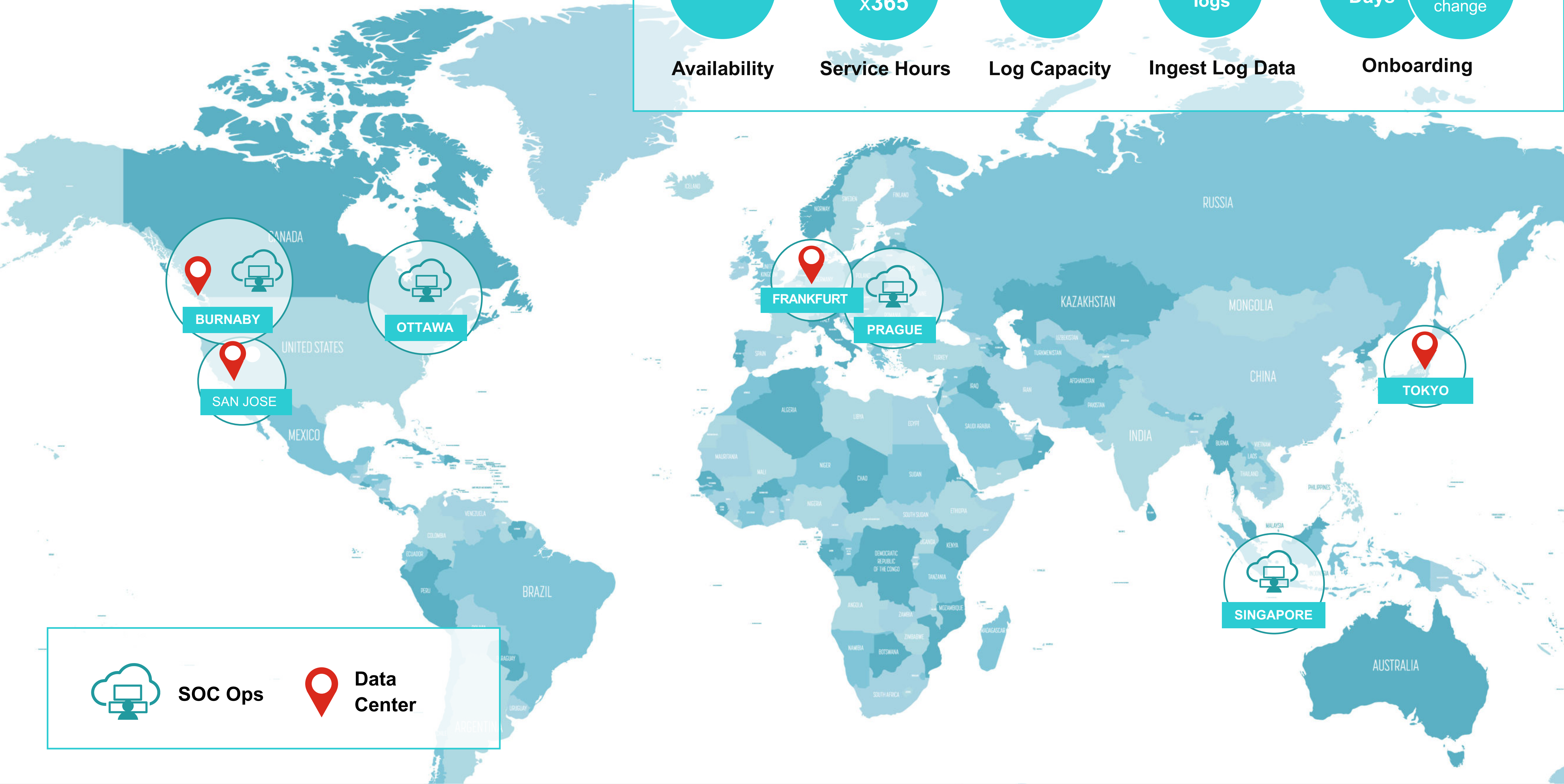
99.99%
Availability

24x7 x365
Service Hours

Unlimited
Log Capacity

FortiGate logs
Ingest Log Data

1-2 Days Simplified device change
Onboarding



SOC Ops

Data Center

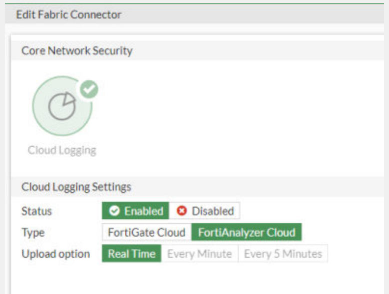
FortiCloud SOC-as-a-Service Deployment Models

Forwarding FortiGate logs to SOCaaS via FortiAnalyzer-cloud

Direct log Forwarding to SOCaaS

PRO:

- Easy to implement
  - Simple configuration:



Edit Fabric Connector

Core Network Security

Cloud Logging

Cloud Logging Settings

Status: Enabled | Disabled

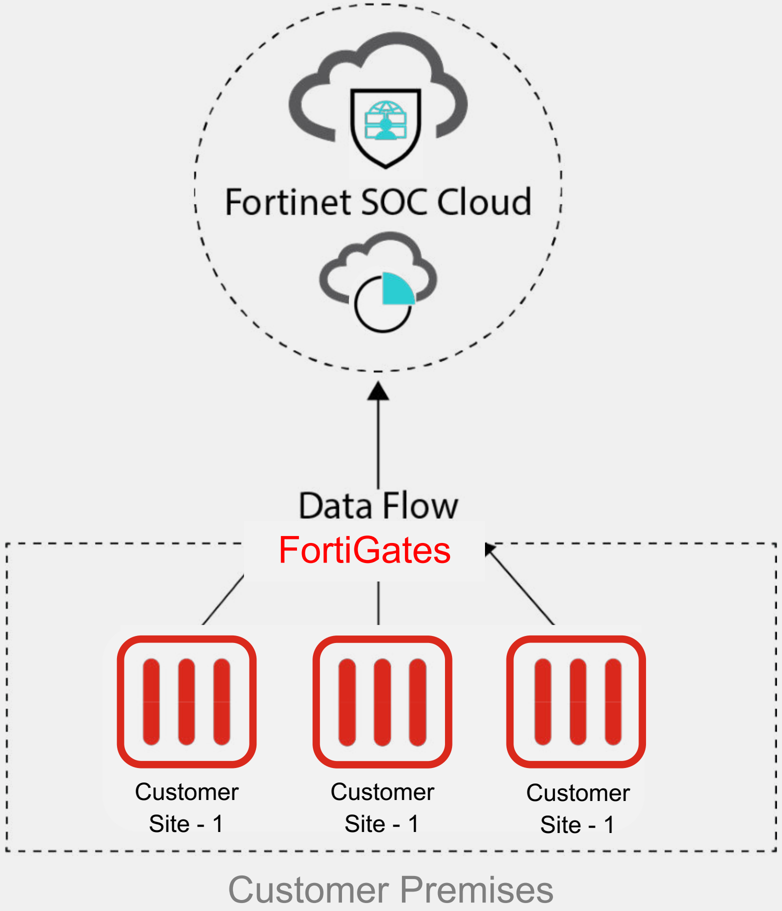
Type: FortiGate Cloud | FortiAnalyzer Cloud

Upload option: Real Time | Every Minute | Every 5 Minutes

- No additional On-Prem Installation required

CON:

- Internet access required for every FGT
- Logs only stored in Fortinet DC
- Not easy to Filter logs before sending to SoCaaS



Direct from FortiGate to FAZ Cloud

FortiCloud SOC-as-a-Service Deployment Models

Forwarding FortiGate logs to SOCaaS via On-premise FortiAnalyzer

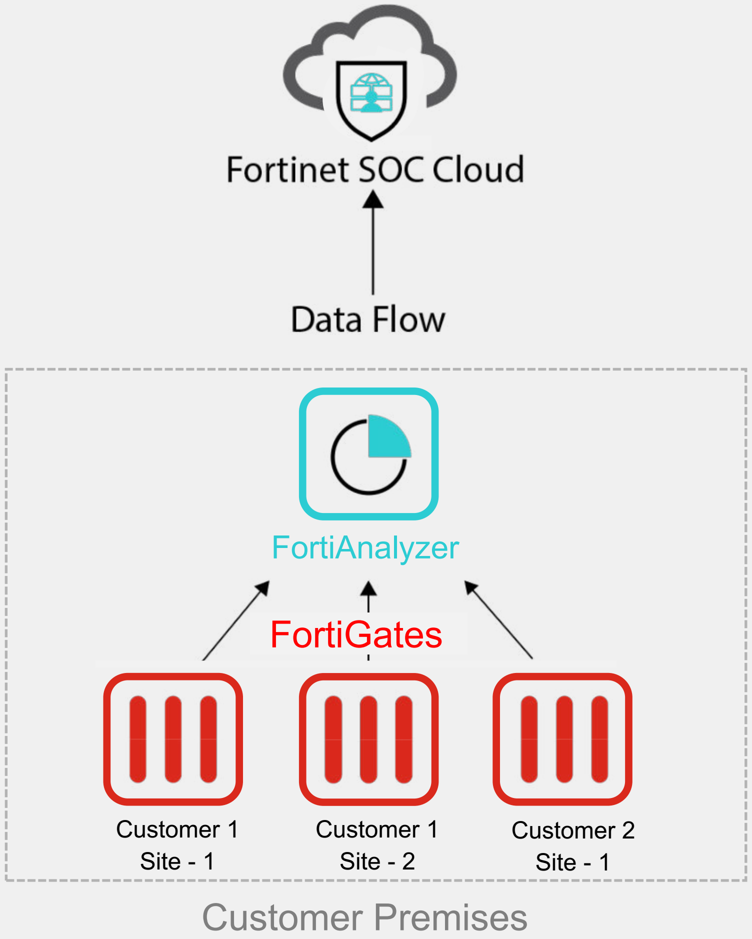
Log Forwarding via FortiAnalyzer

PRO:

- Logs also stored locally
- Easy to manage log forwarding from a single point
  - Big advantage for larger networks
- Posibility to mask or exclude log fields before sending to SoCaaS. (e.g user names or other private Info)
- Different deployment options available (Appliances, VMs)

CON:

- Additional equipment on-prem



Log forwarding from customer FortiAnalyzer (Appliance or VM)

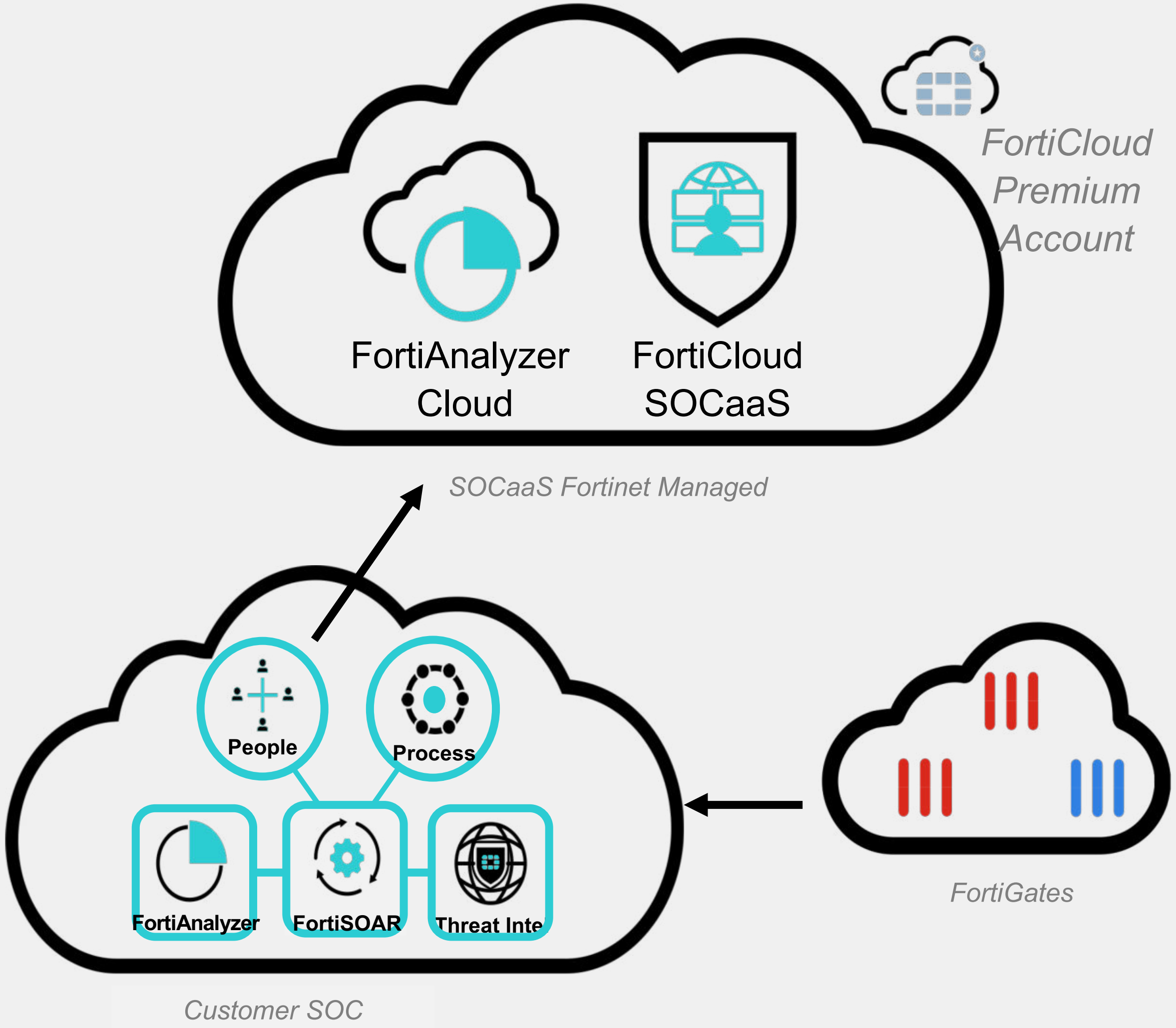
Self Managed SOC complimented by Fortinet Managed

Powered by Fortinet AI-Driven Security Operations Technology Stack

- **Own SoC complimented with SoCaaS**

PRO:

- Own SoC Team
- SoCaaS helps to provide 365/24/7
- Expand SOC coverage by offloading common use cases to Fortinet's SOCaaS
- Utilize skilled resources to refocus efforts on more advanced initiatives and priority business scenarios
- **CON:**
- Need for highly trained dedicated experts
  - Security Analyst is a full-time job
- Additional tools required to build own SoC (SOAR solution)



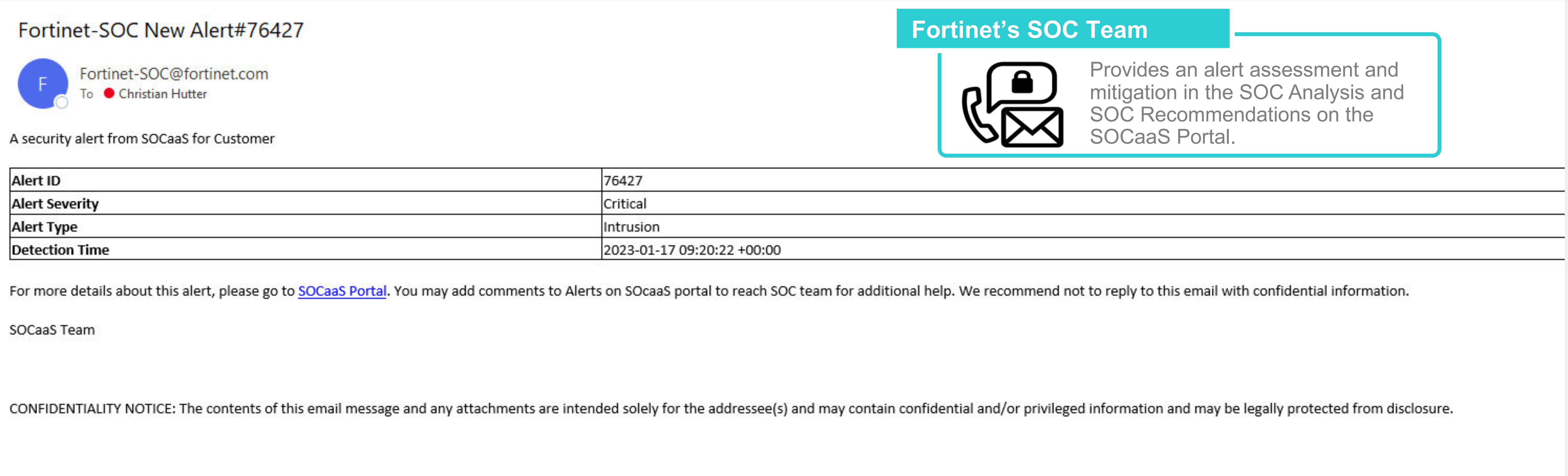
SLA Matrix

Response time by severity

CRITICAL (P1, Priority 1)	**Escalation Time**	Phone: 15 min. Email: 15 min.
HIGH (P2, Priority 2)	**Escalation Time**	Phone: 45 min. Email: 90 min.
MEDIUM (P3, Priority 3)	**Escalation Time**	Phone: NA Email: 90 min.
LOW (P4, Priority 4)	**Escalation Time**	Phone: N/A. Email: 6 hours

Fortinet Escalated Alerting

SOCaaS Incident notification email example



Fortinet-SOC New Alert#76427

Fortinet-SOC@fortinet.com
To Christian Hutter

A security alert from SOCaaS for Customer

Alert ID	76427
Alert Severity	Critical
Alert Type	Intrusion
Detection Time	2023-01-17 09:20:22 +00:00

For more details about this alert, please go to SOCaaS Portal. You may add comments to Alerts on SOcaaS portal to reach SOC team for additional help. We recommend not to reply to this email with confidential information.

SOCaaS Team

CONFIDENTIALITY NOTICE: The contents of this email message and any attachments are intended solely for the addressee(s) and may contain confidential and/or privileged information and may be legally protected from disclosure.

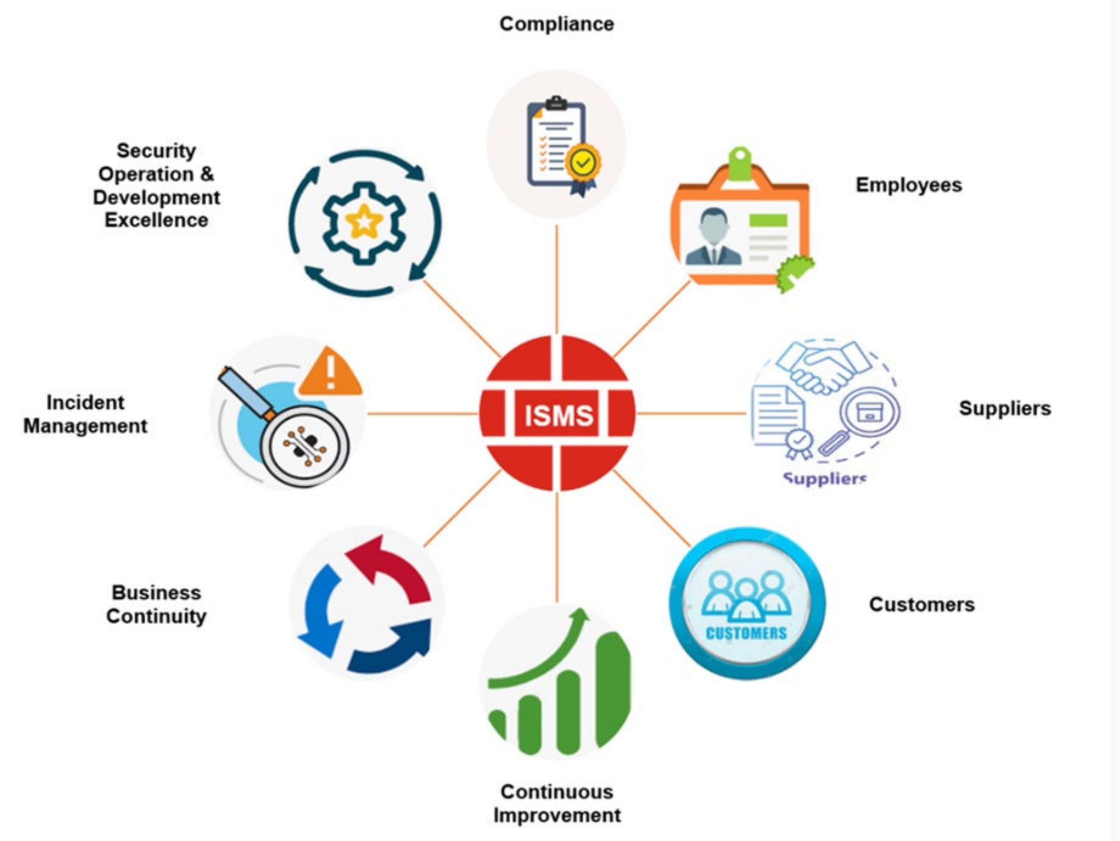
Fortinet's SOC Team

Provides an alert assessment and mitigation in the SOC Analysis and SOC Recommendations on the SOCaaS Portal.

ISO/IEC 27001 & SOC 2 Certification

A certified ISMS demonstrates a commitment to information security by an organization, and provides assurance that information security is addressed properly by means of:

- ✓ **Compliance** – compliance with laws, regulations, and contractual obligations.
- ✓ **Customers** – ensure customer data privacy, integrity, and confidentiality requirements.
- ✓ **Employees** – highly skilled, well-trained, and security-aware workforce.
- ✓ **Suppliers** – suppliers that align both business and security objectives with Fortinet.
- ✓ **Secure Operation/Development Excellence** – security injected into daily operation and development activities.
- ✓ **Business Continuity** – ensure business continuity with a well-defined BCP and readiness for execution.
- ✓ **Incident Management** – an incident occurrence is not a matter of 'if' but 'when' and a robust, responsive Incident Management Program reduces the impact of an incident to a minimum.
- ✓ **Continuous Improvement** – a certified ISMS will facilitate and drive continual improvement.



FortiCloud SOC-as-a-Service Summary

Our Differentiators

Mature Operation

- 24x7 Operations
- Live experts support
- Three SOC centers
- SOC2 & ISO27001 Certified

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

SOC 2 TYPE II COMPLIANT

Skilled Experts

- Experienced SOC People
- Direct access to FortiGuard Labs
- Fortinet Best Practices

Automated Process

- SOAR for SOC automation
- AI assisted incident triage
- Scalable

Integrated Services

- FAZ-Cloud integration for easy onboarding
- Managed FortiGate Service integration for fast Containment
- Forensic Service Integration for endpoint remediation

Best-In-Class Technology

- Fortinet owns the SOC technology end-to-end
- Innovation Leader
- Priority access to product support
- FortiGuard Bigdata and AI

FortiClient Forensic Service

FortiClient Forensic Service

- FortiClient Forensic Service provides analysis to help endpoint customers respond to and recover from cyber incidents.

Collection:

- Collecting disk artifacts and memory snapshots that may be relevant to the investigation. Collections are conducted securely via a remote agent with minimal customer interaction.

Analysis:

Analyzing targeted digital evidence to determine the initial attack vector, establish timeline of malicious activity, and identify the extent of compromise.

Examination:

Examining file system contents, processing log files, and extracting statistical results to prioritize high value items for analysis.

Reporting:

Synthesizing the findings in a high-level executive summary with details on remediation recommendations.

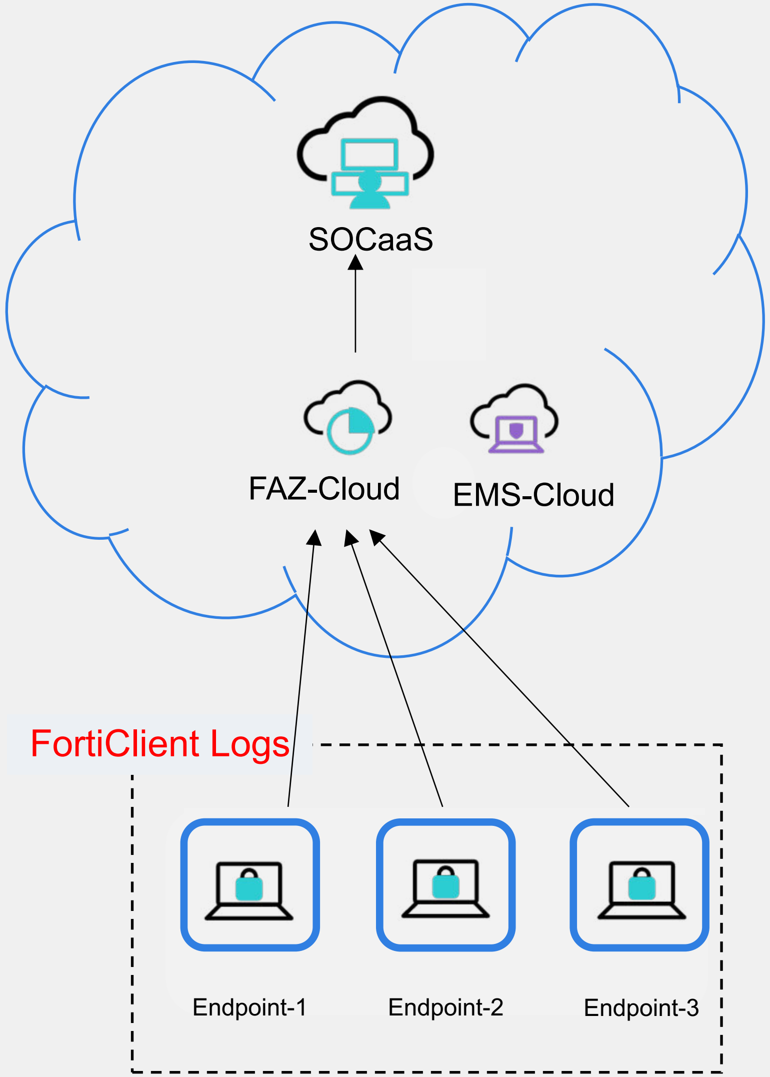
- FortiClient Forensic Service is only available for EMS-Cloud today

Forensic Service Deployment Models

Forwarding FortiClient logs to SOCaaS via FortiAnalyzer-cloud

Log Forwarding via FAZ-Cloud to SOCaaS:

- Requires EMS-Cloud with Forensic Service Subscription
- Requires FortiAnalyzer-Cloud Storage Add-On Subscription



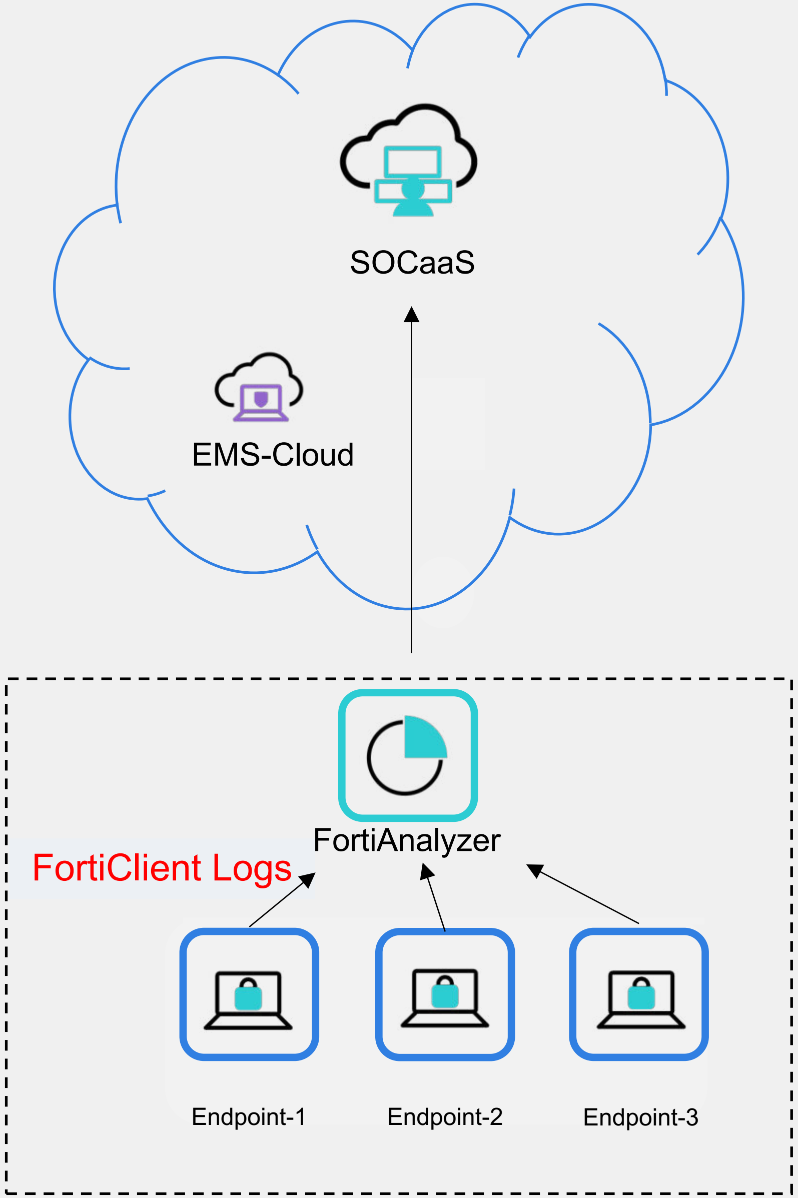
Direct from FortiClient to FAZ Cloud

Forensic Service Deployment Models

Forwarding FortiClient logs to SOCaaS via On-Prem FAZ

Log Forwarding via On-Prem FAZ to SOCaaS:

- Requires only EMS-Cloud with Forensic Service Subscription



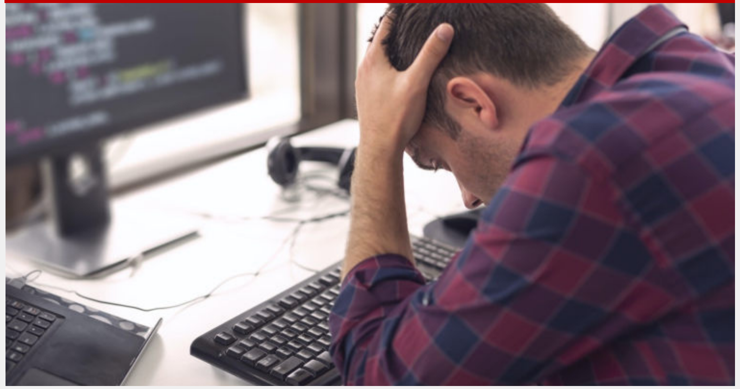
Via On-Prem FAZ to SOCaaS

Managed FortiGate Service

NOC Challenges

Human Errors

occurred during the manual and lengthy migration process



82% of data breaches involved a human element.

Source: Verizon 2022 Data Breaches Investigations Report

Complexity

due to the increasing number of apps, devices, users connected to the network

41.6 billion of connected IoT devices by 2025, with a 28.7% CAGR.

Source: IDC

Lack of Expertise

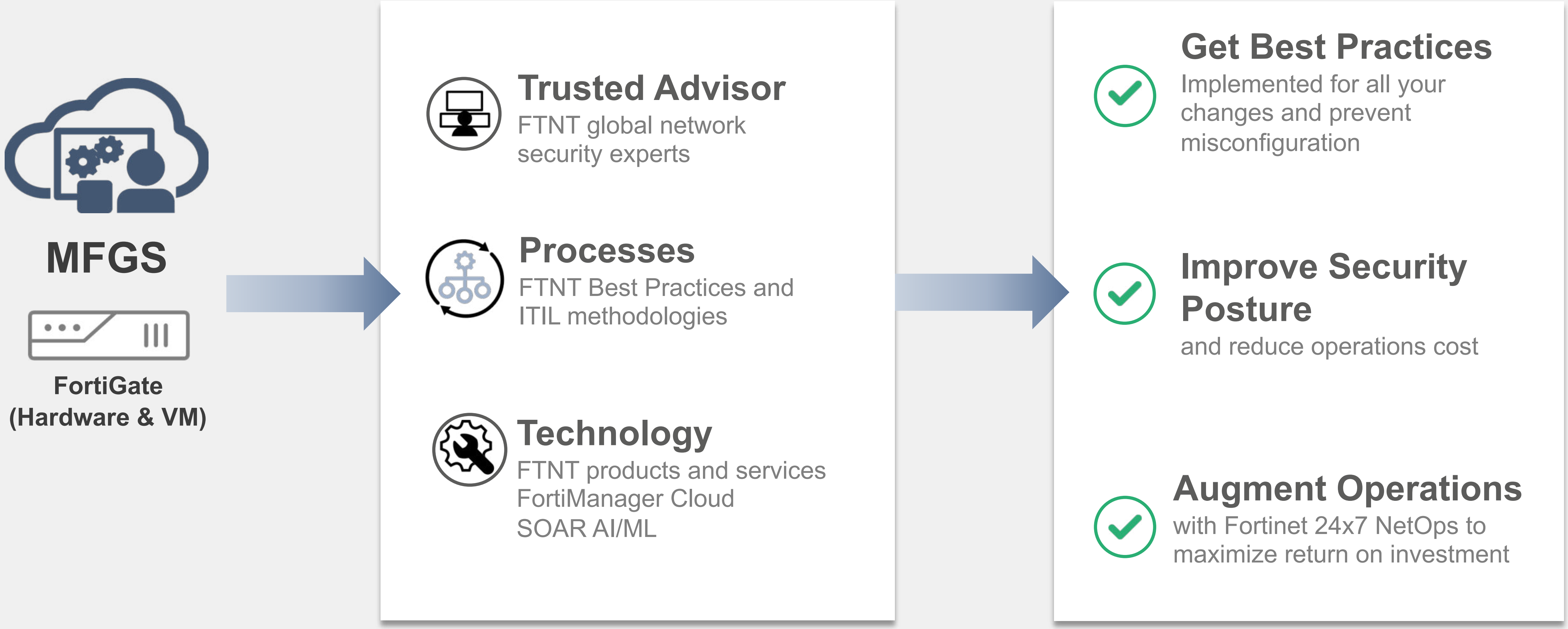
in firewall configurations and security best practices

60% of organizations struggle to recruit cybersecurity talent and 52% struggle to retain it.

Source: Fortinet 2022 Cybersecurity Skills Gap Global Research Report

How Can Managed FortiGate Service Help?

24x7 Cloud-based, fully managed global network operations service



MFGS

FortiGate (Hardware & VM)

Trusted Advisor
FTNT global network security experts

Processes
FTNT Best Practices and ITIL methodologies

Technology
FTNT products and services
FortiManager Cloud
SOAR AI/ML

✓ **Get Best Practices**
Implemented for all your changes and prevent misconfiguration

✓ **Improve Security Posture**
and reduce operations cost

✓ **Augment Operations**
with Fortinet 24x7 NetOps to maximize return on investment

What will Manage FortiGate Experts Perform?

Change Management

- Evaluation / Implementation / Verification of change requests
- FSBP and ITIL methodology

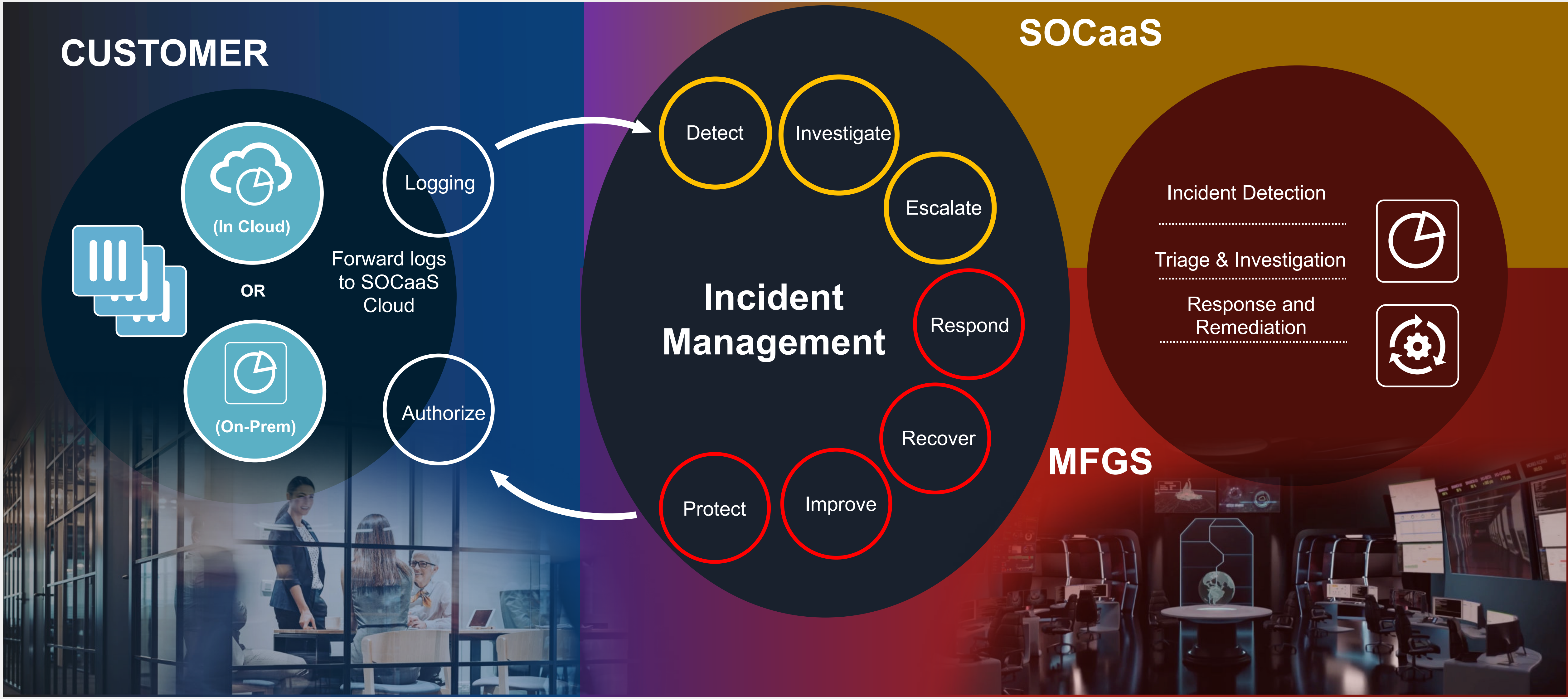
System Hardening

- **SOCaaS Incident Remediation**
- PSIRT Advisories Response
- Fortiguard Outbreak Response
- System Audit
- Security Posture Review

Device Provisioning

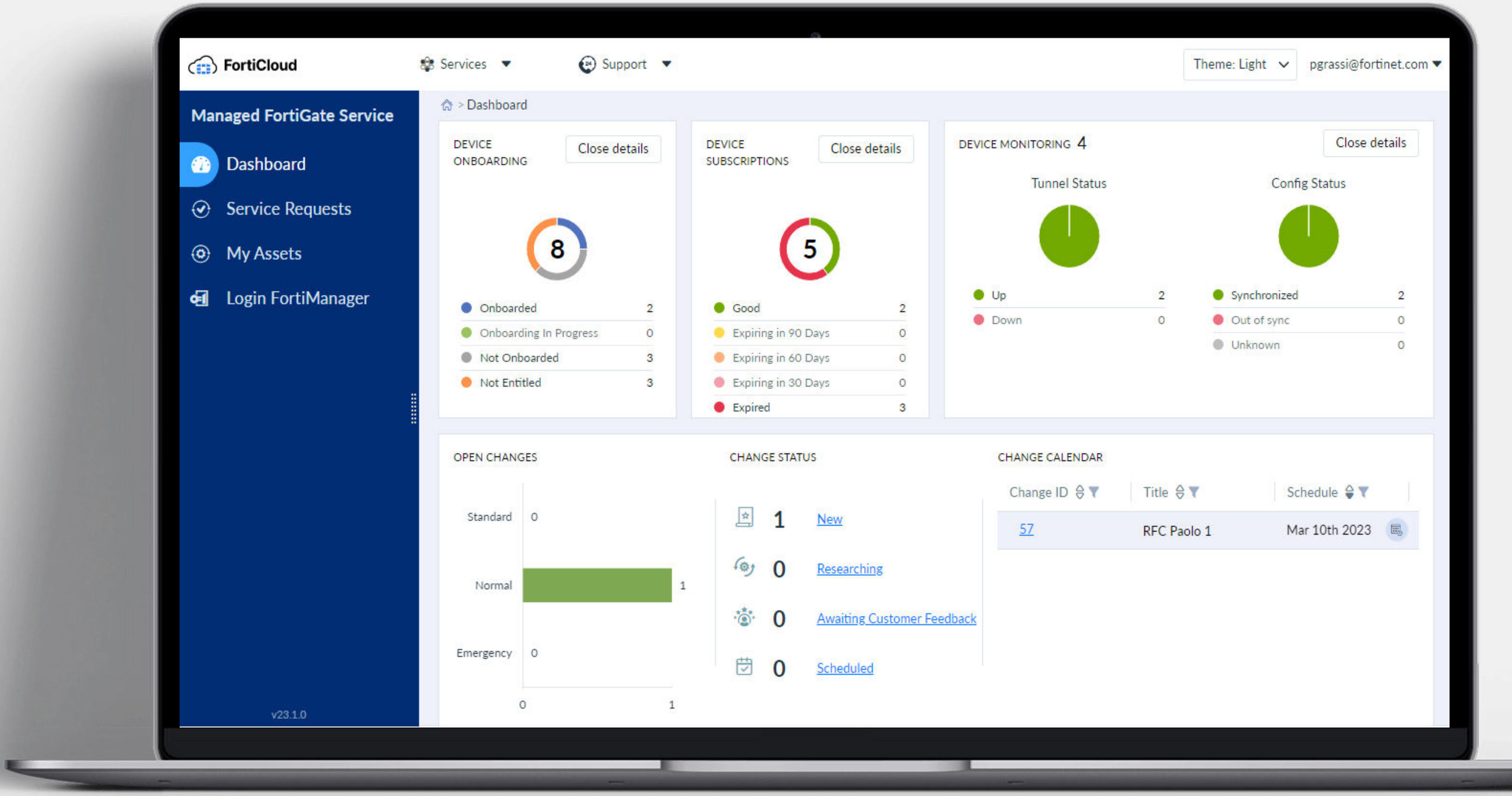
- NGFW Deployment
- Security Fabric Setup
- Secure SD-WAN
- ZTNA
- Remote Access

Incident Response – SOCaaS + MFGS



How does the customer engage with our Experts?

- Request Onboard
- Request Change
- Approve Change
- Update Ticket
- Schedule Deployment
- Request Consultation
- View Reports



FortiCloud   Services ▾   Support ▾   Theme: Light ▾   pgrassi@fortinet.com ▾

Managed FortiGate Service

- Dashboard
- Service Requests
- My Assets
- Login FortiManager

v23.1.0

⌂ > Dashboard

DEVICE ONBOARDING   Close details

8

● Onboarded	2
● Onboarding In Progress	0
● Not Onboarded	3
● Not Entitled	3

DEVICE SUBSCRIPTIONS   Close details

5

● Good	2
● Expiring in 90 Days	0
● Expiring in 60 Days	0
● Expiring in 30 Days	0
● Expired	3

DEVICE MONITORING 4   Close details

Tunnel Status

● Up	2
● Down	0

Config Status

● Synchronized	2
● Out of sync	0
● Unknown	0

OPEN CHANGES

Standard	0
Normal	1
Emergency	0

CHANGE STATUS

1	New
0	Researching
0	Awaiting Customer Feedback
0	Scheduled

CHANGE CALENDAR

Change ID	Title	Schedule
57	RFC Paolo 1	Mar 10th 2023

What are the SLAs of Managed FortiGate Service?

Emergency

Evaluation Time 1 Hour

Implementation Time 4 Hours

Normal

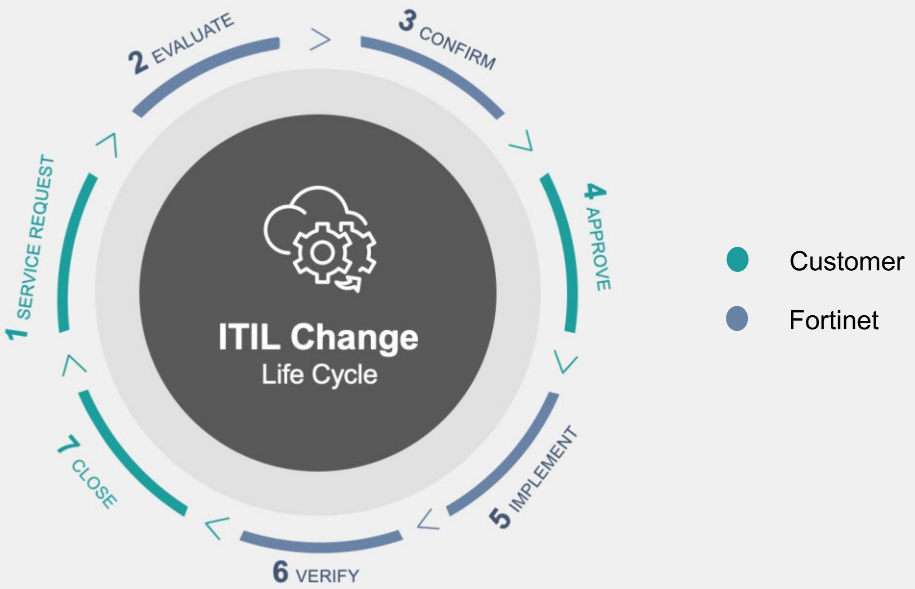
Evaluation Time 4 Hours

Implementation Time 1 B Day

Standard

Evaluation Time 1 B Day

Implementation Time 2 B days



Customer Benefits

Fortinet Best Practices Audit, Use Case Coverage, System Hardening, Policy Tuning Recommendations, Security Posture Review, PSIRT Response, and Outbreak Response.

✓ Eliminate Errors

Fortinet NOC experts to manage the full lifecycle of your Fortinet FortiGates

✓ Simplify Operations

Change management driven by Fortinet best practices using ITIL™ Continual Service Improvement

✓ Predictable Costs

Customers have a predictable cost for their network security operations

✓ Full Visibility

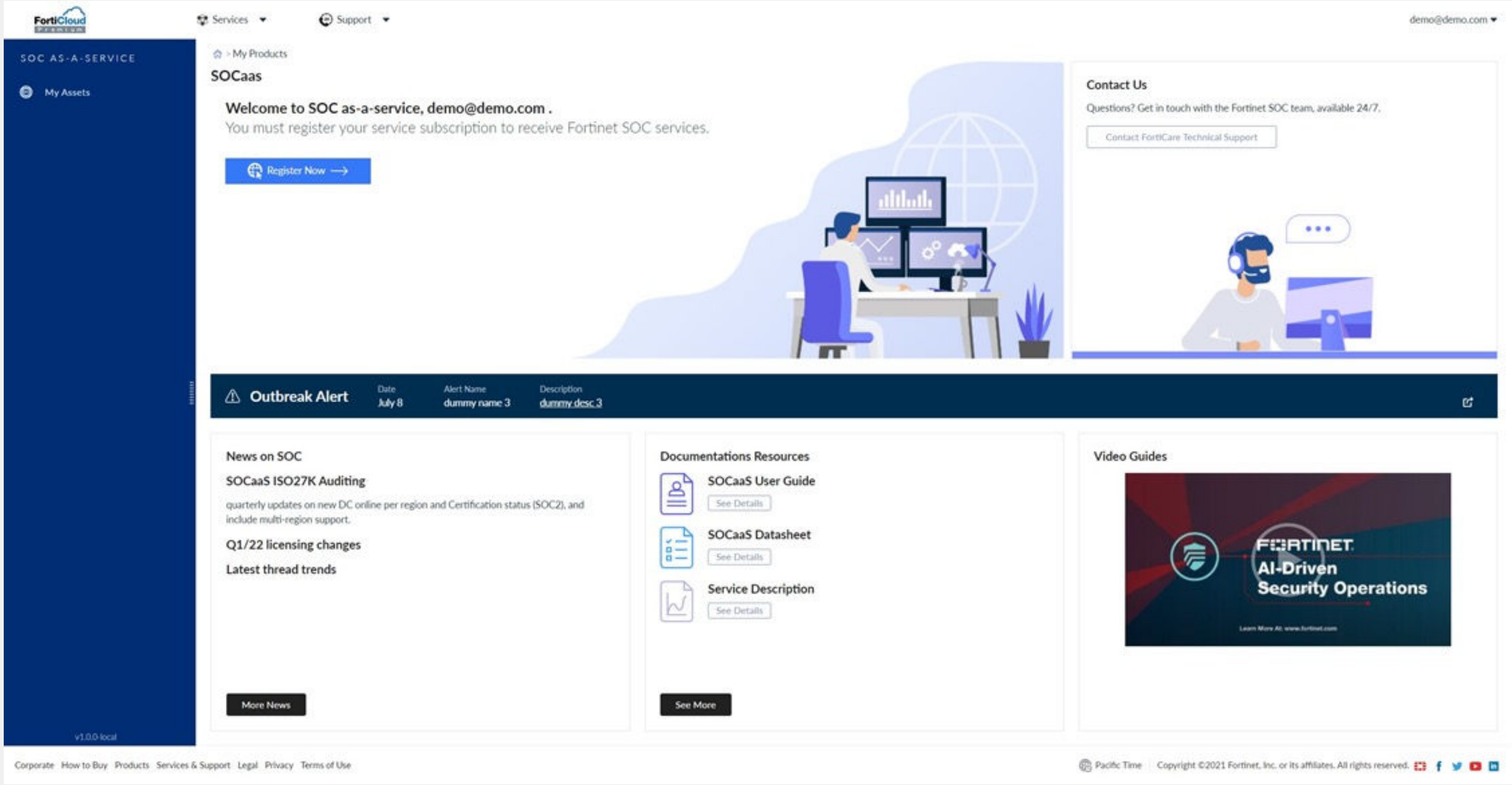
Gain full visibility of the service, raise change requests, review implementation schedules, and post-implementation reports.

FORTINET®

SOC as a Service

SOCaaS Portál - ukázka

Home Page (For customers without SOC subscription)



SOCaas

Welcome to SOC as-a-service, demo@demo.com .

You must register your service subscription to receive Fortinet SOC services.

Contact Us

Questions? Get in touch with the Fortinet SOC team, available 24/7.

Outbreak Alert

Date	Alert Name	Description
July 8	dummy name 3	dummy desc 3

News on SOC

SOCaaS ISO27K Auditing

quarterly updates on new DC online per region and Certification status (SOC2), and include multi-region support.

Q1/22 licensing changes

Latest thread trends

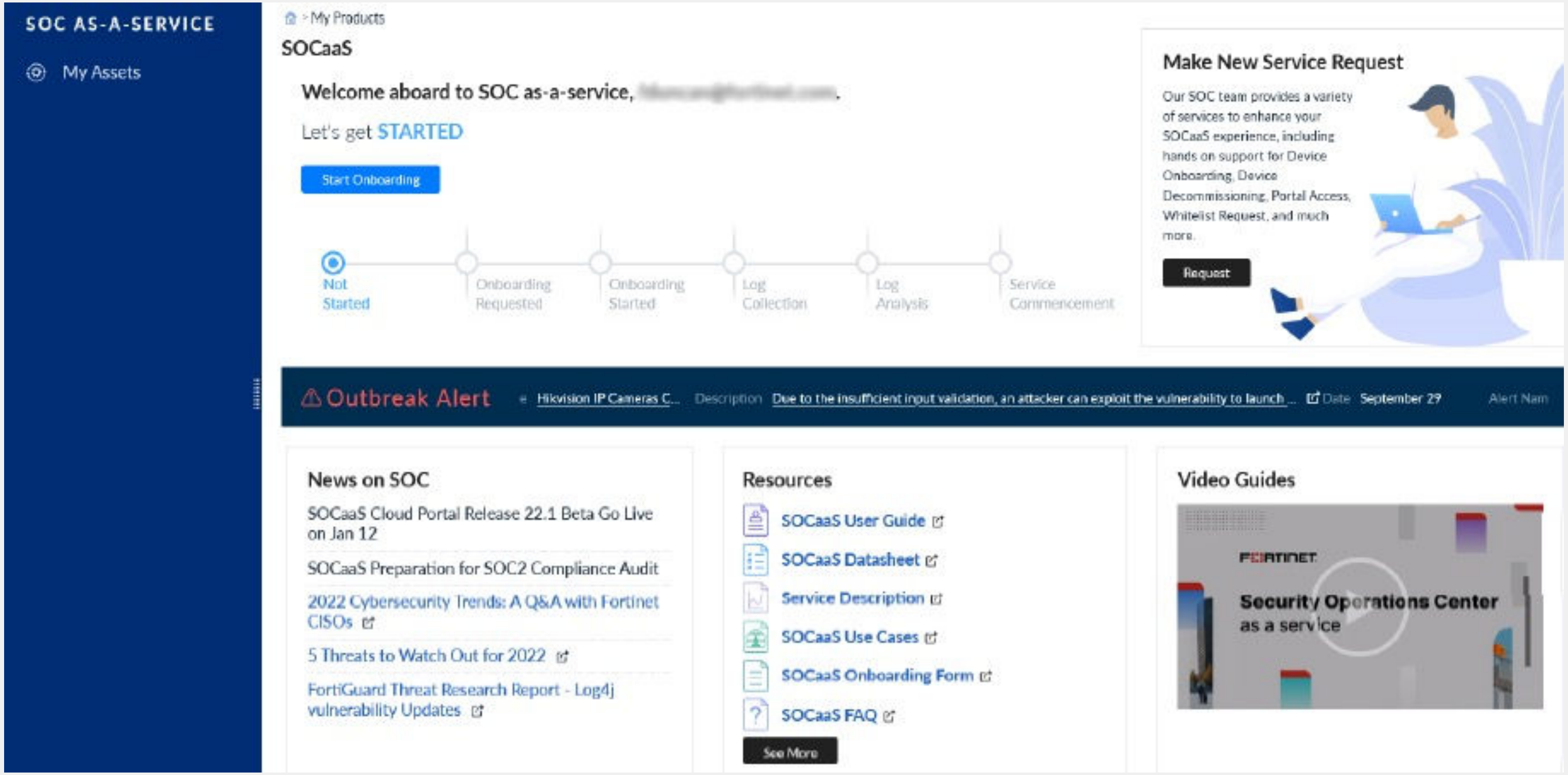
Documentations Resources

- SOCaaS User Guide
- SOCaaS Datasheet
- Service Description

Video Guides

Copyright ©2021 Fortinet, Inc. or its affiliates. All rights reserved.

Home Page (For customers with SOC subscription)



SOC AS-A-SERVICE

My Assets

My Products

SOCaaS

Welcome aboard to SOC as-a-service, [redacted].

Let's get STARTED

Make New Service Request

Our SOC team provides a variety of services to enhance your SOCaaS experience, including hands on support for Device Onboarding, Device Decommissioning, Portal Access, Whitelist Request, and much more.

Outbreak Alert

Hikvision IP Cameras C... Description Due to the insufficient input validation, an attacker can exploit the vulnerability to launch ... Date September 29 Alert Nam

News on SOC

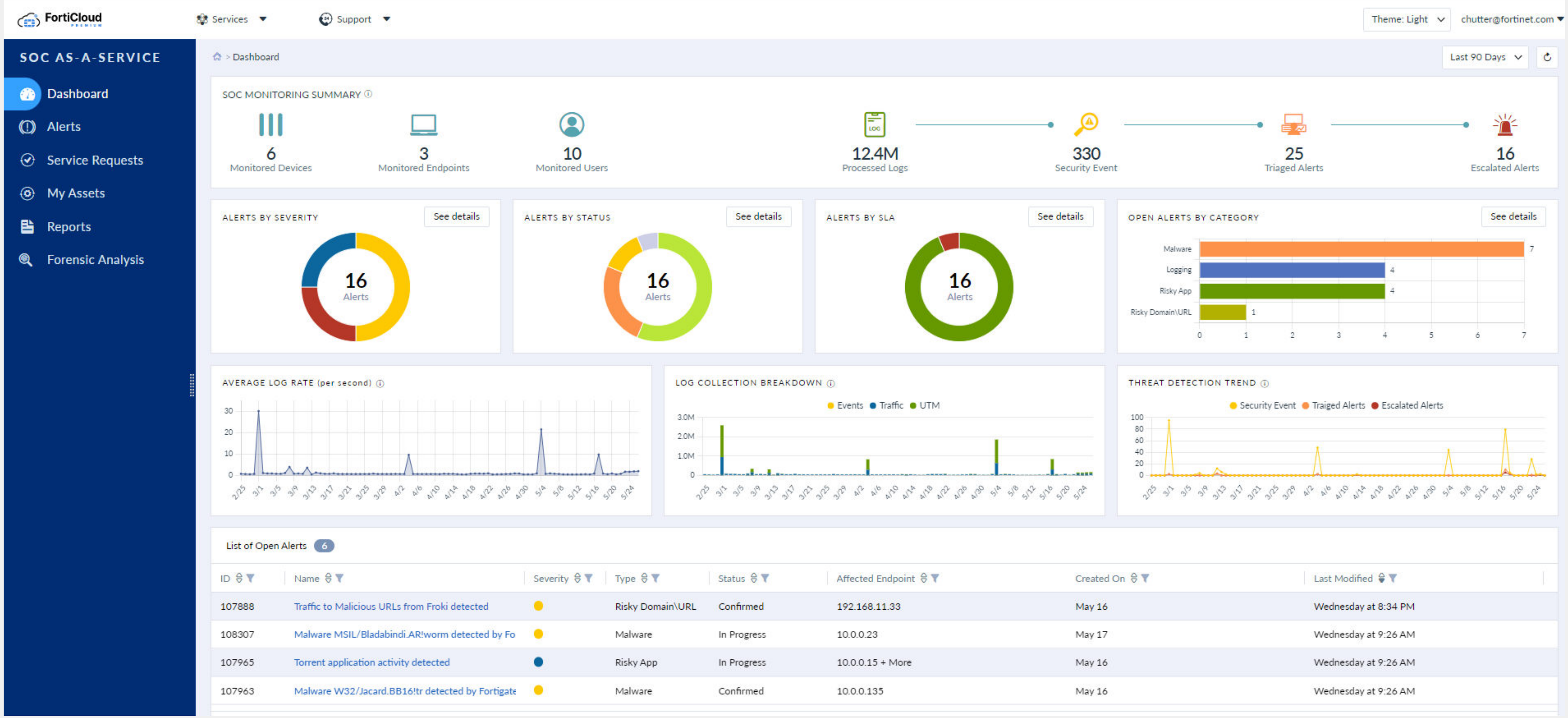
- SOCaaS Cloud Portal Release 22.1 Beta Go Live on Jan 12
- SOCaaS Preparation for SOC2 Compliance Audit
- 2022 Cybersecurity Trends: A Q&A with Fortinet CISOs
- 5 Threats to Watch Out for 2022
- FortiGuard Threat Research Report - Log4j vulnerability Updates

Resources

- SOCaaS User Guide
- SOCaaS Datasheet
- Service Description
- SOCaaS Use Cases
- SOCaaS Onboarding Form
- SOCaaS FAQ

Video Guides

Dashboard



SOC MONITORING SUMMARY

6 Monitored Devices	3 Monitored Endpoints	10 Monitored Users	12.4M Processed Logs	330 Security Event	25 Triaged Alerts	16 Escalated Alerts

ALERTS BY SEVERITY: 16 Alerts

ALERTS BY STATUS: 16 Alerts

ALERTS BY SLA: 16 Alerts

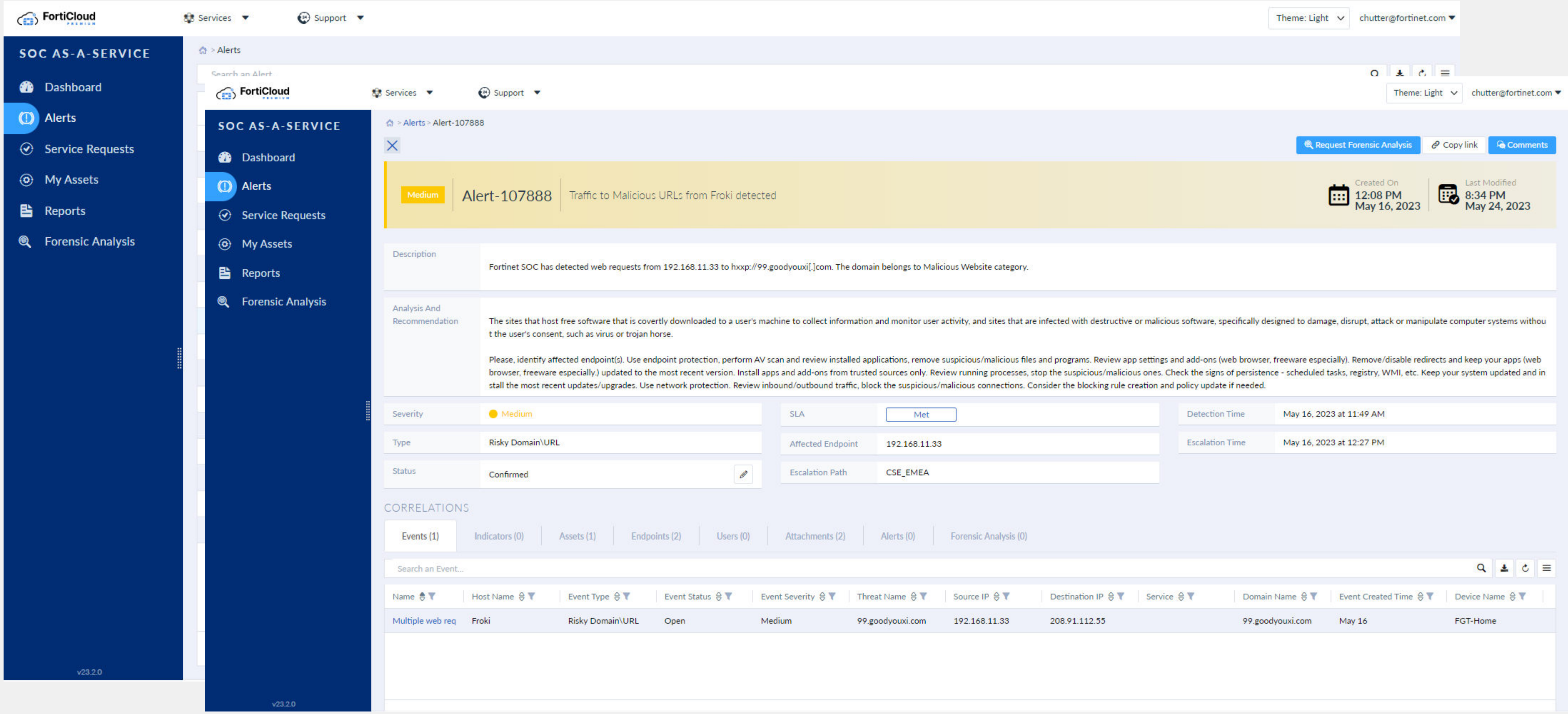
OPEN ALERTS BY CATEGORY

Category	Count
Malware	7
Logging	4
Risky App	4
Risky Domain\URL	1

List of Open Alerts 6

ID	Name	Severity	Type	Status	Affected Endpoint	Created On	Last Modified
107888	Traffic to Malicious URLs from Froki detected	●	Risky Domain\URL	Confirmed	192.168.11.33	May 16	Wednesday at 8:34 PM
108307	Malware MSIL/Bladabindi.AR!worm detected by Fo	●	Malware	In Progress	10.0.0.23	May 17	Wednesday at 9:26 AM
107965	Torrent application activity detected	●	Risky App	In Progress	10.0.0.15 + More	May 16	Wednesday at 9:26 AM
107963	Malware W32/Jacard.BB16!tr detected by Fortigate	●	Malware	Confirmed	10.0.0.135	May 16	Wednesday at 9:26 AM

Alerts



Medium | Alert-107888 | Traffic to Malicious URLs from Froki detected

Created On 12:08 PM May 16, 2023

Last Modified 8:34 PM May 24, 2023

Description

Fortinet SOC has detected web requests from 192.168.11.33 to hxxp://99.goodyouxi[.]com. The domain belongs to Malicious Website category.

Analysis And Recommendation

The sites that host free software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse.

Please, identify affected endpoint(s). Use endpoint protection, perform AV scan and review installed applications, remove suspicious/malicious files and programs. Review app settings and add-ons (web browser, freeware especially). Remove/disable redirects and keep your apps (web browser, freeware especially.) updated to the most recent version. Install apps and add-ons from trusted sources only. Review running processes, stop the suspicious/malicious ones. Check the signs of persistence - scheduled tasks, registry, WMI, etc. Keep your system updated and install the most recent updates/upgrades. Use network protection. Review inbound/outbound traffic, block the suspicious/malicious connections. Consider the blocking rule creation and policy update if needed.

Severity	● Medium	SLA	Met	Detection Time	May 16, 2023 at 11:49 AM
Type	Risky Domain\URL	Affected Endpoint	192.168.11.33	Escalation Time	May 16, 2023 at 12:27 PM
Status	Confirmed	Escalation Path	CSE_EMEA		

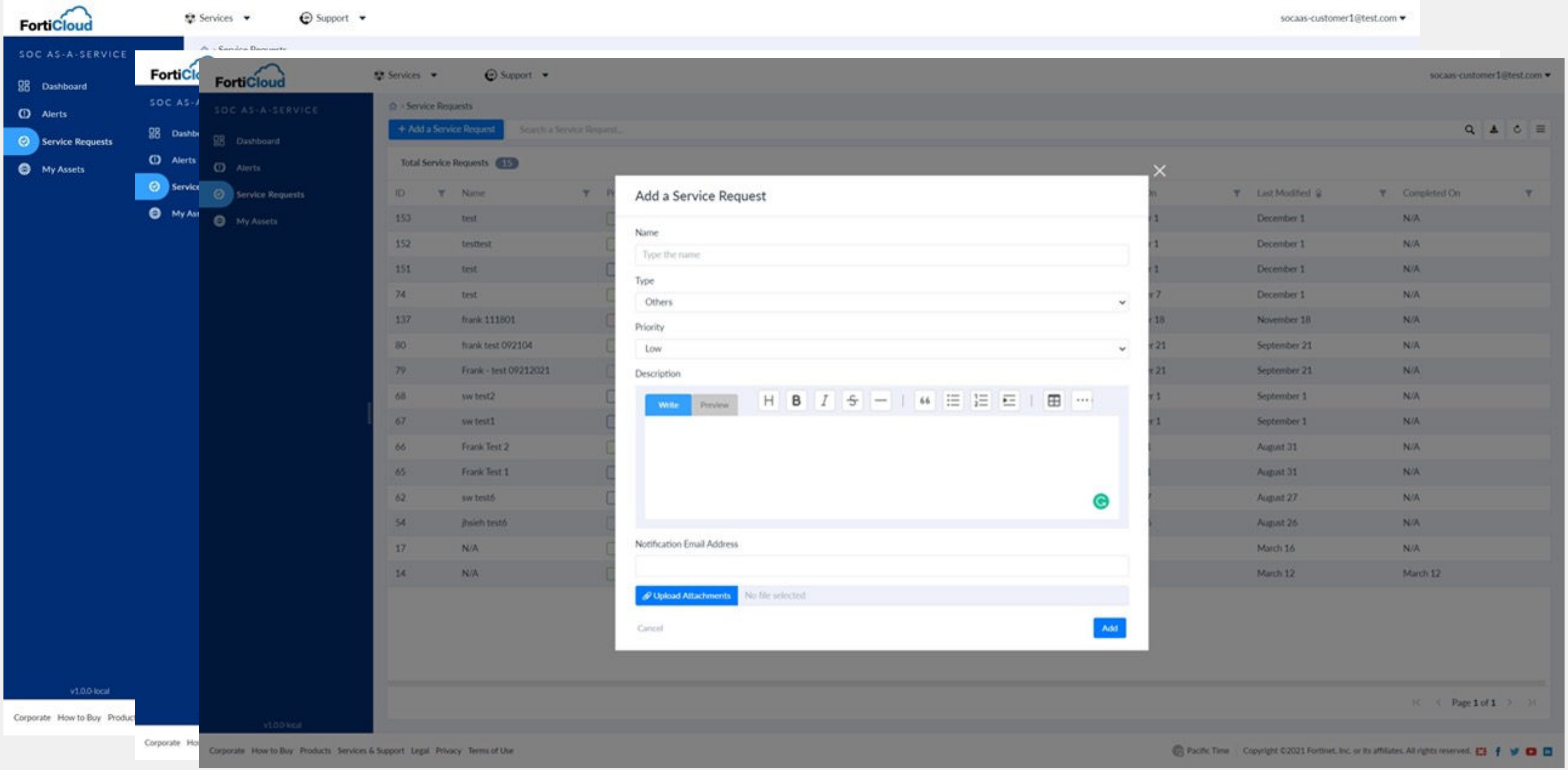
CORRELATIONS

Events (1) | Indicators (0) | Assets (1) | Endpoints (2) | Users (0) | Attachments (2) | Alerts (0) | Forensic Analysis (0)

Search an Event...

Name	Host Name	Event Type	Event Status	Event Severity	Threat Name	Source IP	Destination IP	Service	Domain Name	Event Created Time	Device Name
Multiple web req	Froki	Risky Domain\URL	Open	Medium	99.goodyouxi.com	192.168.11.33	208.91.112.55		99.goodyouxi.com	May 16	FGT-Home

Service Requests



Service Requests

Total Service Requests 15

ID	Name	Last Modified	Completed On
153	test	December 1	N/A
152	testtest	December 1	N/A
151	test	December 1	N/A
74	test	December 1	N/A
137	frank 111801	November 18	N/A
80	frank test 092104	September 21	N/A
79	Frank - test 09212021	September 21	N/A
68	sw test2	September 1	N/A
67	sw test1	September 1	N/A
66	Frank Test 2	August 31	N/A
65	Frank Test 1	August 31	N/A
62	sw test6	August 27	N/A
54	jhsieh test6	August 26	N/A
17	N/A	March 16	N/A
14	N/A	March 12	March 12

Page 1 of 1

Add a Service Request

Name: Type the name

Type: Others

Priority: Low

Description

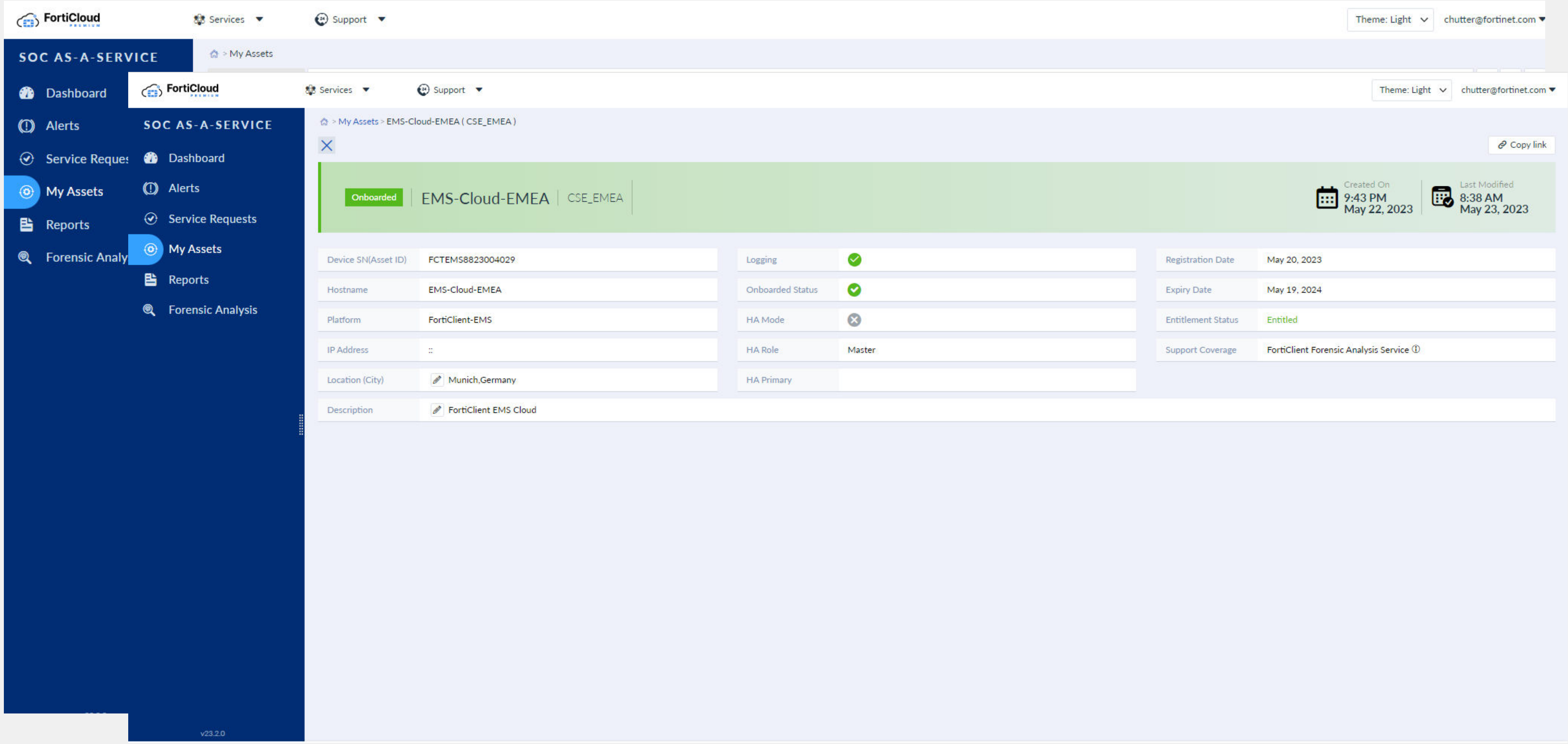
Notification Email Address

Upload Attachments No file selected

Corporate How to Buy Products Services & Support Legal Privacy Terms of Use

Pacific Time Copyright ©2021 Fortinet, Inc. or its affiliates. All rights reserved.

My Assets



> My Assets > EMS-Cloud-EMEA (CSE_EMEA)

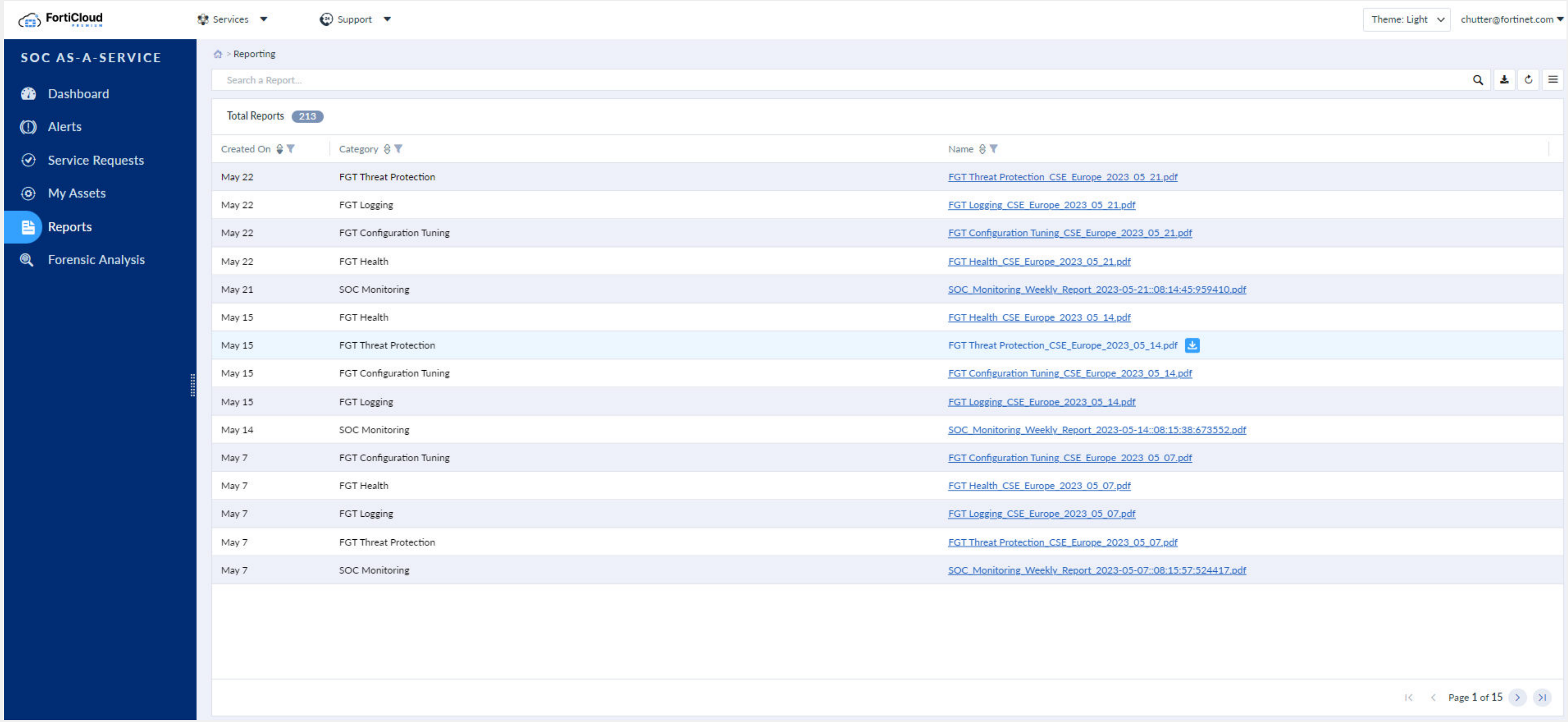
Onboarded | EMS-Cloud-EMEA | CSE_EMEA

Created On 9:43 PM May 22, 2023

Last Modified 8:38 AM May 23, 2023

Device SN(Asset ID)	FCTEMS8823004029	Logging	✓	Registration Date	May 20, 2023
Hostname	EMS-Cloud-EMEA	Onboarded Status	✓	Expiry Date	May 19, 2024
Platform	FortiClient-EMS	HA Mode	☒	Entitlement Status	Entitled
IP Address	::	HA Role	Master	Support Coverage	FortiClient Forensic Analysis Service ⓘ
Location (City)	Munich,Germany	HA Primary			
Description	FortiClient EMS Cloud				

Reports



Theme: Light

chutter@fortinet.com

Total Reports 213

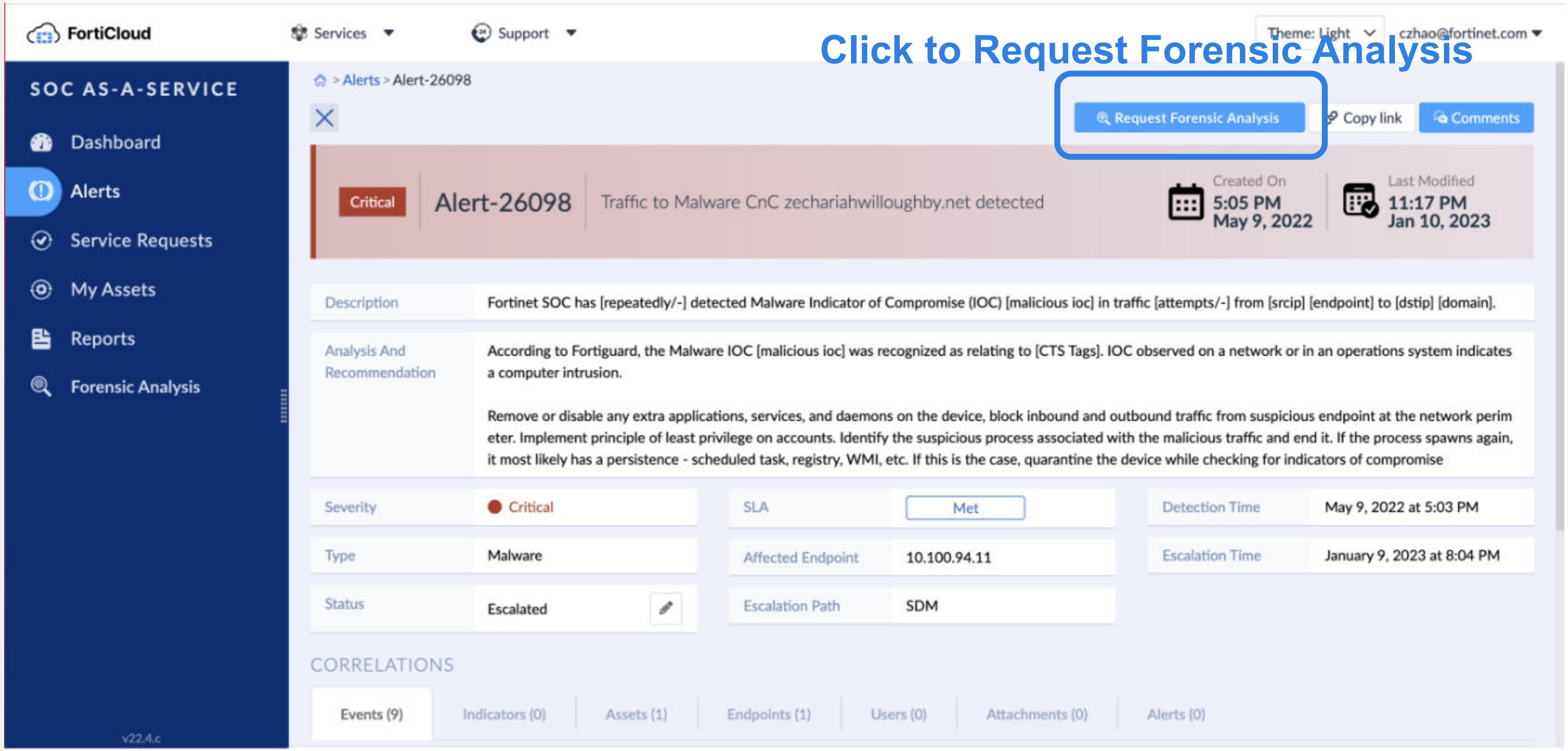
Created On	Category	Name
May 22	FGT Threat Protection	FGT Threat Protection_CSE_Europe_2023_05_21.pdf
May 22	FGT Logging	FGT Logging_CSE_Europe_2023_05_21.pdf
May 22	FGT Configuration Tuning	FGT Configuration Tuning_CSE_Europe_2023_05_21.pdf
May 22	FGT Health	FGT Health_CSE_Europe_2023_05_21.pdf
May 21	SOC Monitoring	SOC_Monitoring_Weekly_Report_2023-05-21::08:14:45:959410.pdf
May 15	FGT Health	FGT Health_CSE_Europe_2023_05_14.pdf
May 15	FGT Threat Protection	FGT Threat Protection_CSE_Europe_2023_05_14.pdf
May 15	FGT Configuration Tuning	FGT Configuration Tuning_CSE_Europe_2023_05_14.pdf
May 15	FGT Logging	FGT Logging_CSE_Europe_2023_05_14.pdf
May 14	SOC Monitoring	SOC_Monitoring_Weekly_Report_2023-05-14::08:15:38:673552.pdf
May 7	FGT Configuration Tuning	FGT Configuration Tuning_CSE_Europe_2023_05_07.pdf
May 7	FGT Health	FGT Health_CSE_Europe_2023_05_07.pdf
May 7	FGT Logging	FGT Logging_CSE_Europe_2023_05_07.pdf
May 7	FGT Threat Protection	FGT Threat Protection_CSE_Europe_2023_05_07.pdf
May 7	SOC Monitoring	SOC_Monitoring_Weekly_Report_2023-05-07::08:15:57:524417.pdf

Page 1 of 15

Endpoint Forensics

ukázka

Incident Response Endpoint Forensics



Click to Request Forensic Analysis

Critical | Alert-26098 | Traffic to Malware CnC zechariahwilloughby.net detected

Created On: 5:05 PM May 9, 2022

Last Modified: 11:17 PM Jan 10, 2023

Description: Fortinet SOC has [repeatedly/-] detected Malware Indicator of Compromise (IOC) [malicious ioc] in traffic [attempts/-] from [srcip] [endpoint] to [dstip] [domain].

Analysis And Recommendation: According to Fortiguard, the Malware IOC [malicious ioc] was recognized as relating to [CTS Tags]. IOC observed on a network or in an operations system indicates a computer intrusion.

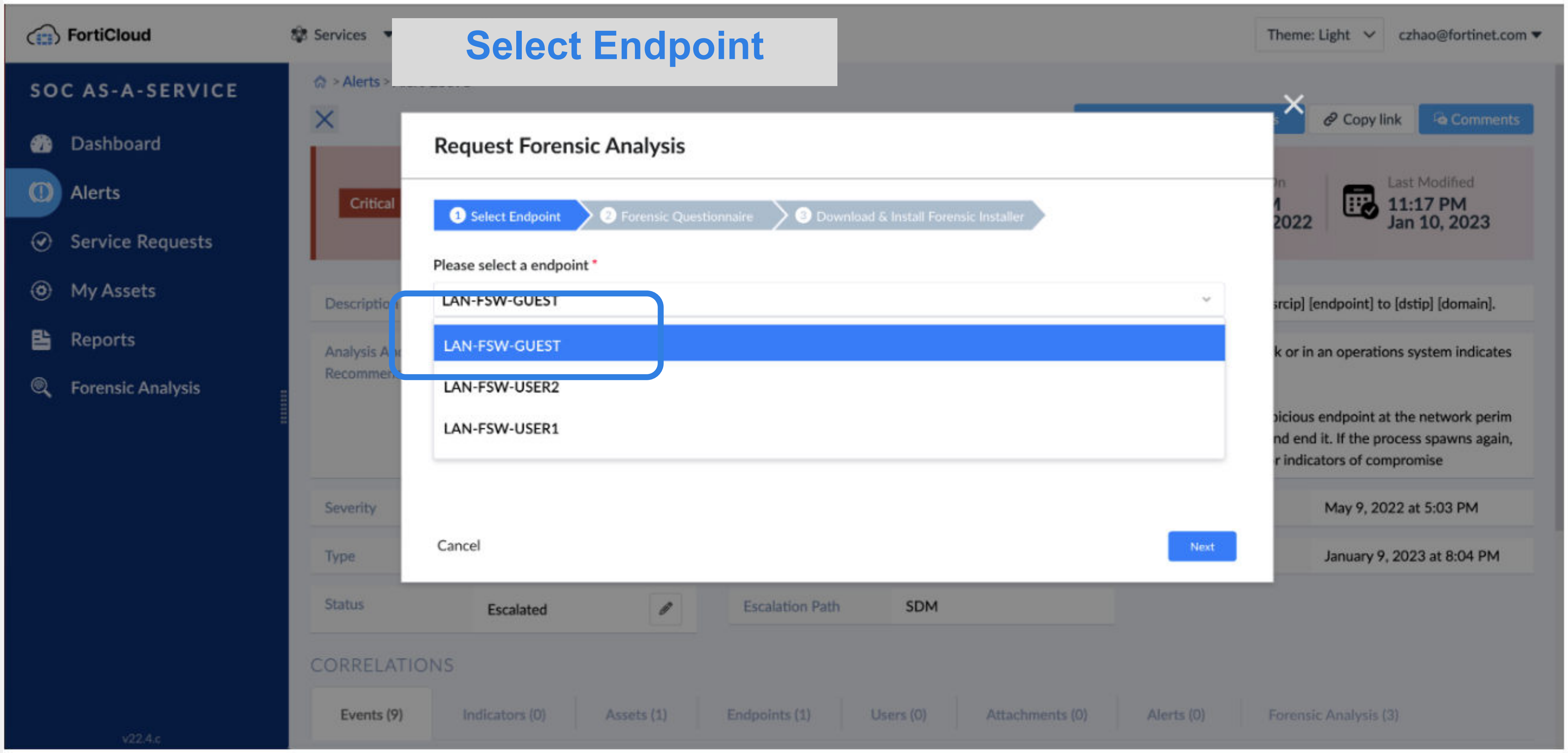
Remove or disable any extra applications, services, and daemons on the device, block inbound and outbound traffic from suspicious endpoint at the network perimeter. Implement principle of least privilege on accounts. Identify the suspicious process associated with the malicious traffic and end it. If the process spawns again, it most likely has a persistence - scheduled task, registry, WMI, etc. If this is the case, quarantine the device while checking for indicators of compromise

Severity	● Critical	SLA	Met	Detection Time	May 9, 2022 at 5:03 PM
Type	Malware	Affected Endpoint	10.100.94.11	Escalation Time	January 9, 2023 at 8:04 PM
Status	Escalated	Escalation Path	SDM		

CORRELATIONS

Events (9) | Indicators (0) | Assets (1) | Endpoints (1) | Users (0) | Attachments (0) | Alerts (0)

Select Endpoint



Request Forensic Analysis

1 Select Endpoint > 2 Forensic Questionnaire > 3 Download & Install Forensic Installer

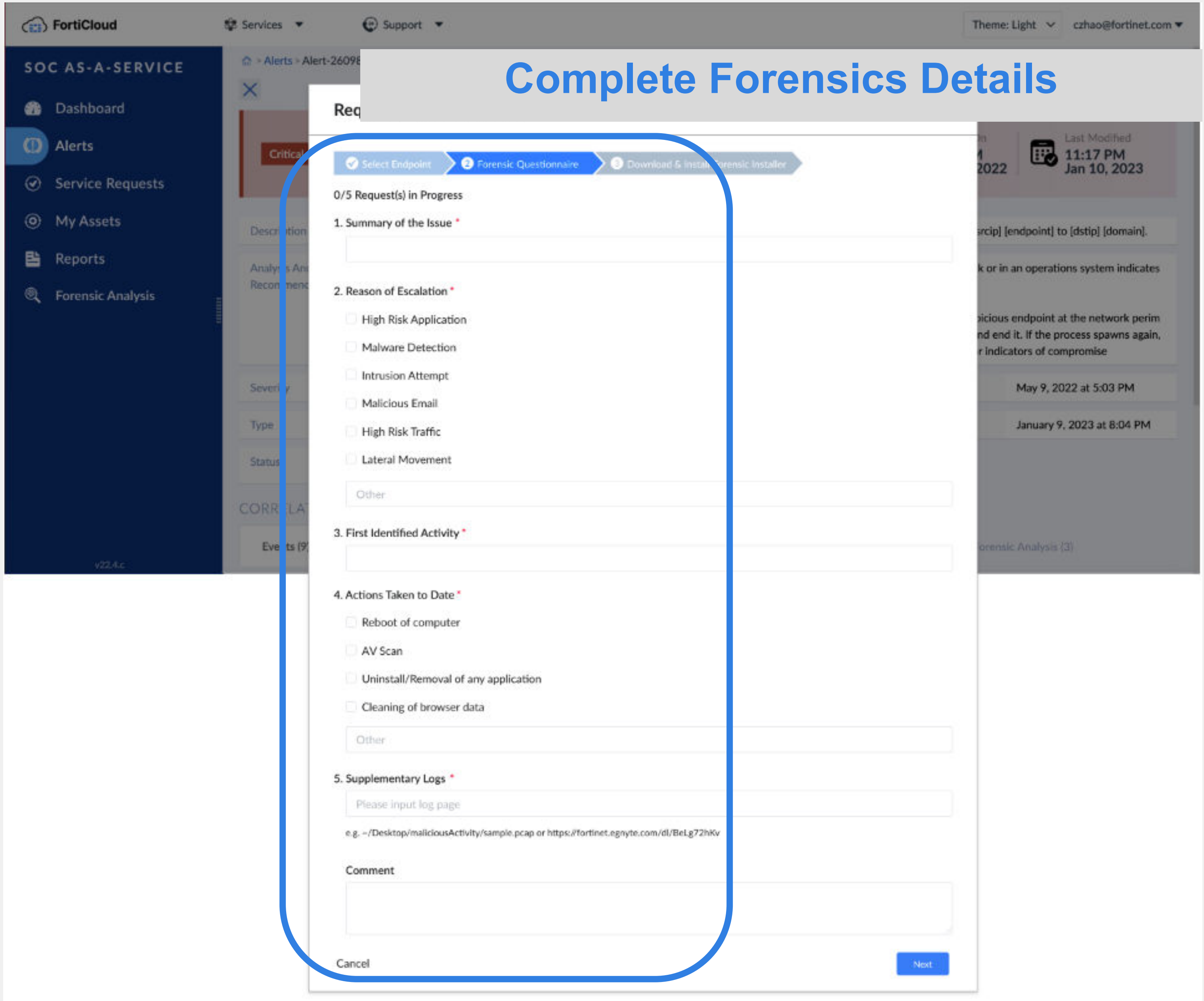
Please select a endpoint *

LAN-FSW-GUEST

- LAN-FSW-GUEST
- LAN-FSW-USER2
- LAN-FSW-USER1

Cancel | Next

Complete Forensics Details



0/5 Request(s) in Progress

1. Summary of the Issue *

2. Reason of Escalation *

- □ High Risk Application
- □ Malware Detection
- □ Intrusion Attempt
- □ Malicious Email
- □ High Risk Traffic
- □ Lateral Movement
- Other

3. First Identified Activity *

4. Actions Taken to Date *

- □ Reboot of computer
- □ AV Scan
- □ Uninstall/Removal of any application
- □ Cleaning of browser data
- Other

5. Supplementary Logs *

Please input log page

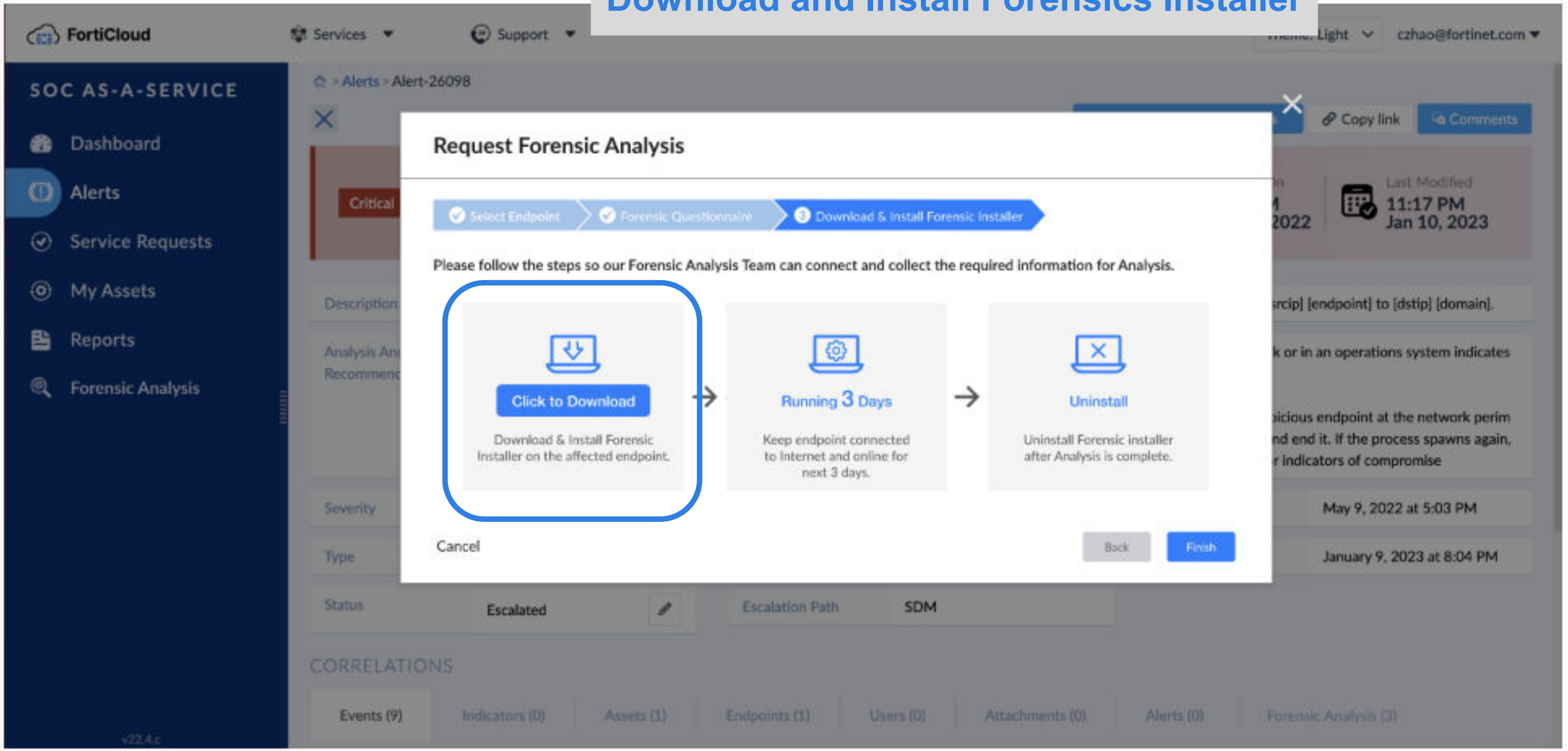
e.g. ~/Desktop/maliciousActivity/sample.pcap or https://fortinet.egnyte.com/dl/BeLg72hKv

Comment

Cancel

Next

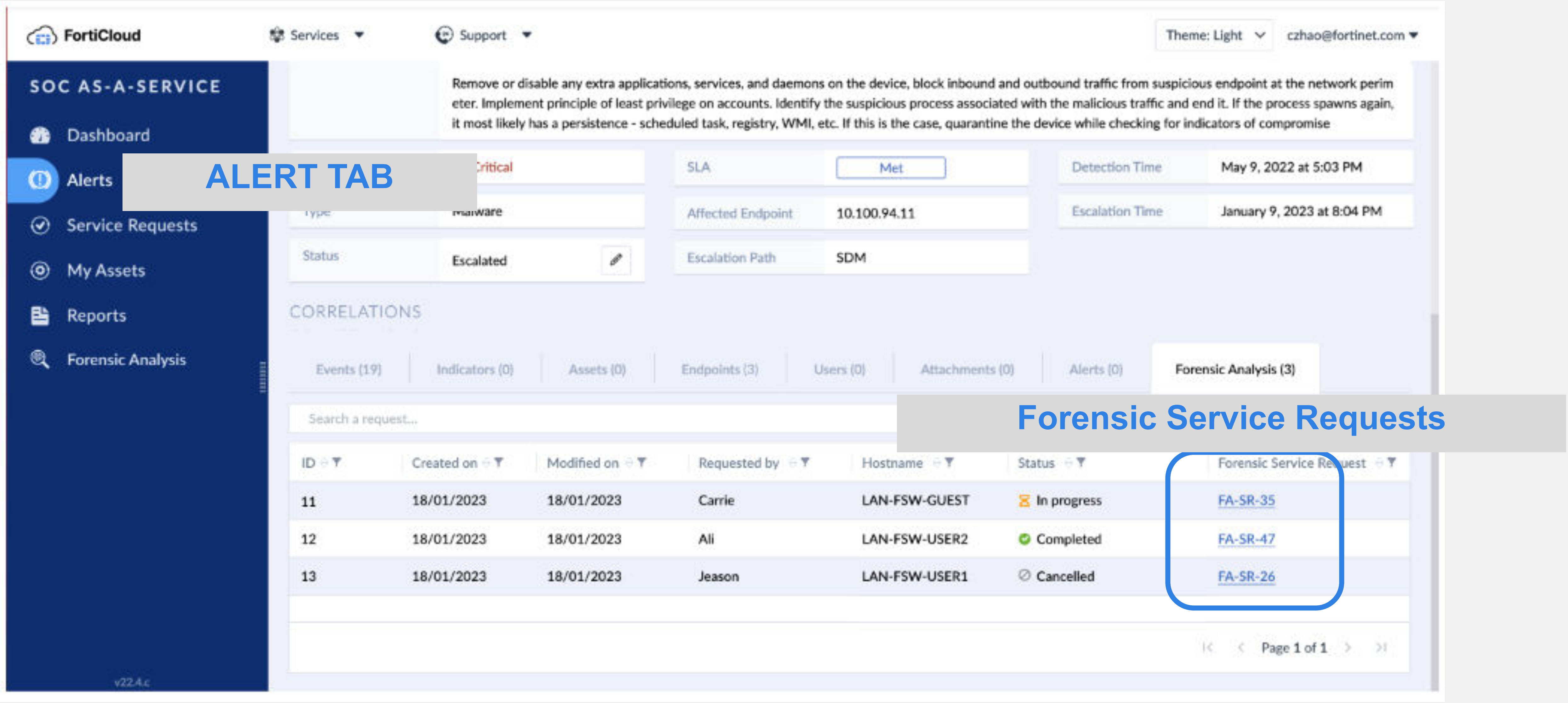
Download and Install Forensics Installer



Please follow the steps so our Forensic Analysis Team can connect and collect the required information for Analysis.

1. Click to Download: Download & Install Forensic Installer on the affected endpoint.
2. Running 3 Days: Keep endpoint connected to Internet and online for next 3 days.
3. Uninstall: Uninstall Forensic installer after Analysis is complete.

- Forensic Agent will automatically collect the necessary data and send it to the Forensic Team



ALERT TAB

Remove or disable any extra applications, services, and daemons on the device, block inbound and outbound traffic from suspicious endpoint at the network perimeter. Implement principle of least privilege on accounts. Identify the suspicious process associated with the malicious traffic and end it. If the process spawns again, it most likely has a persistence - scheduled task, registry, WMI, etc. If this is the case, quarantine the device while checking for indicators of compromise

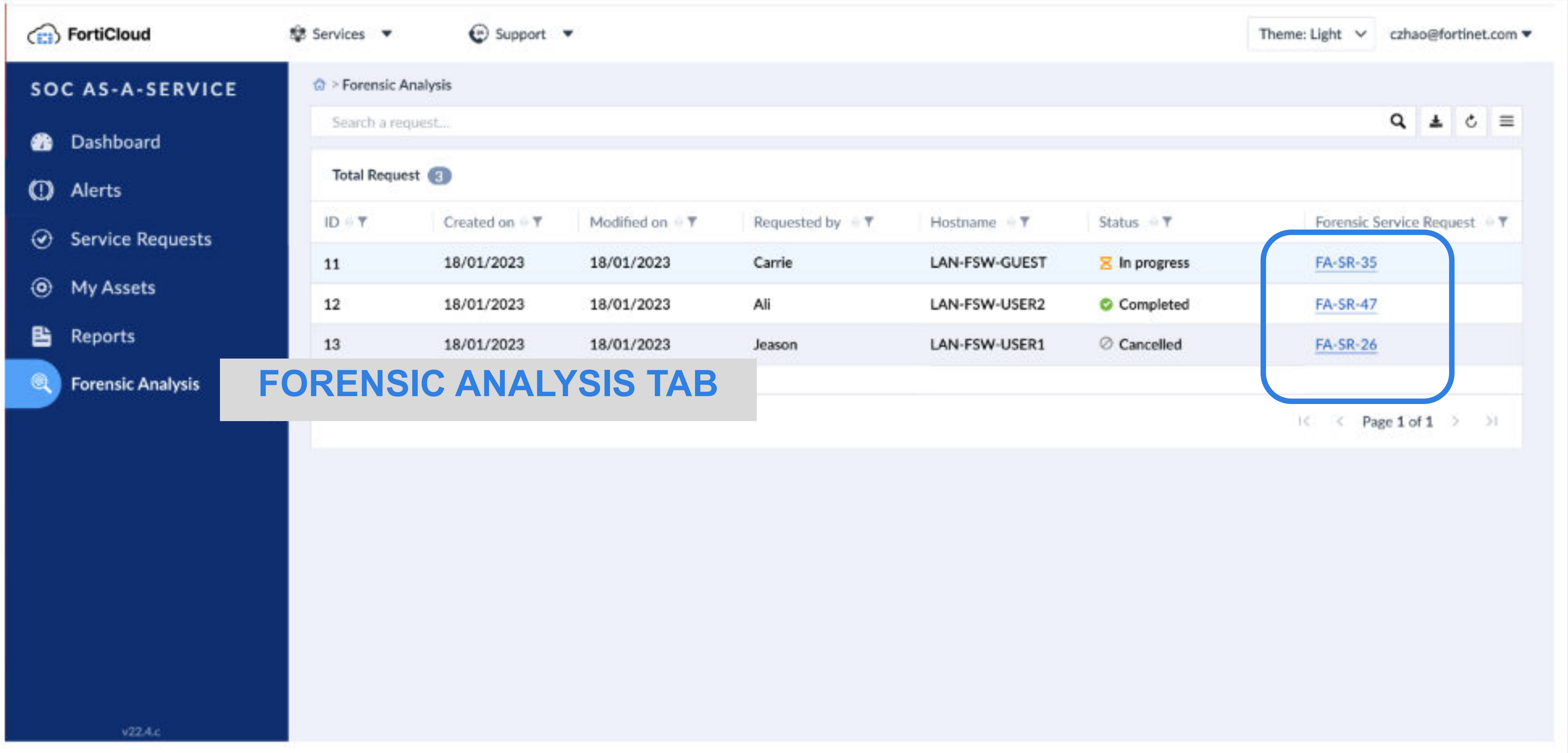
	Critical	SLA	Met	Detection Time	May 9, 2022 at 5:03 PM
Type	Malware	Affected Endpoint	10.100.94.11	Escalation Time	January 9, 2023 at 8:04 PM
Status	Escalated	Escalation Path	SDM		

CORRELATIONS

Forensic Service Requests

ID	Created on	Modified on	Requested by	Hostname	Status	Forensic Service Request
11	18/01/2023	18/01/2023	Carrie	LAN-FSW-GUEST	In progress	FA-SR-35
12	18/01/2023	18/01/2023	Ali	LAN-FSW-USER2	Completed	FA-SR-47
13	18/01/2023	18/01/2023	Jeason	LAN-FSW-USER1	Cancelled	FA-SR-26

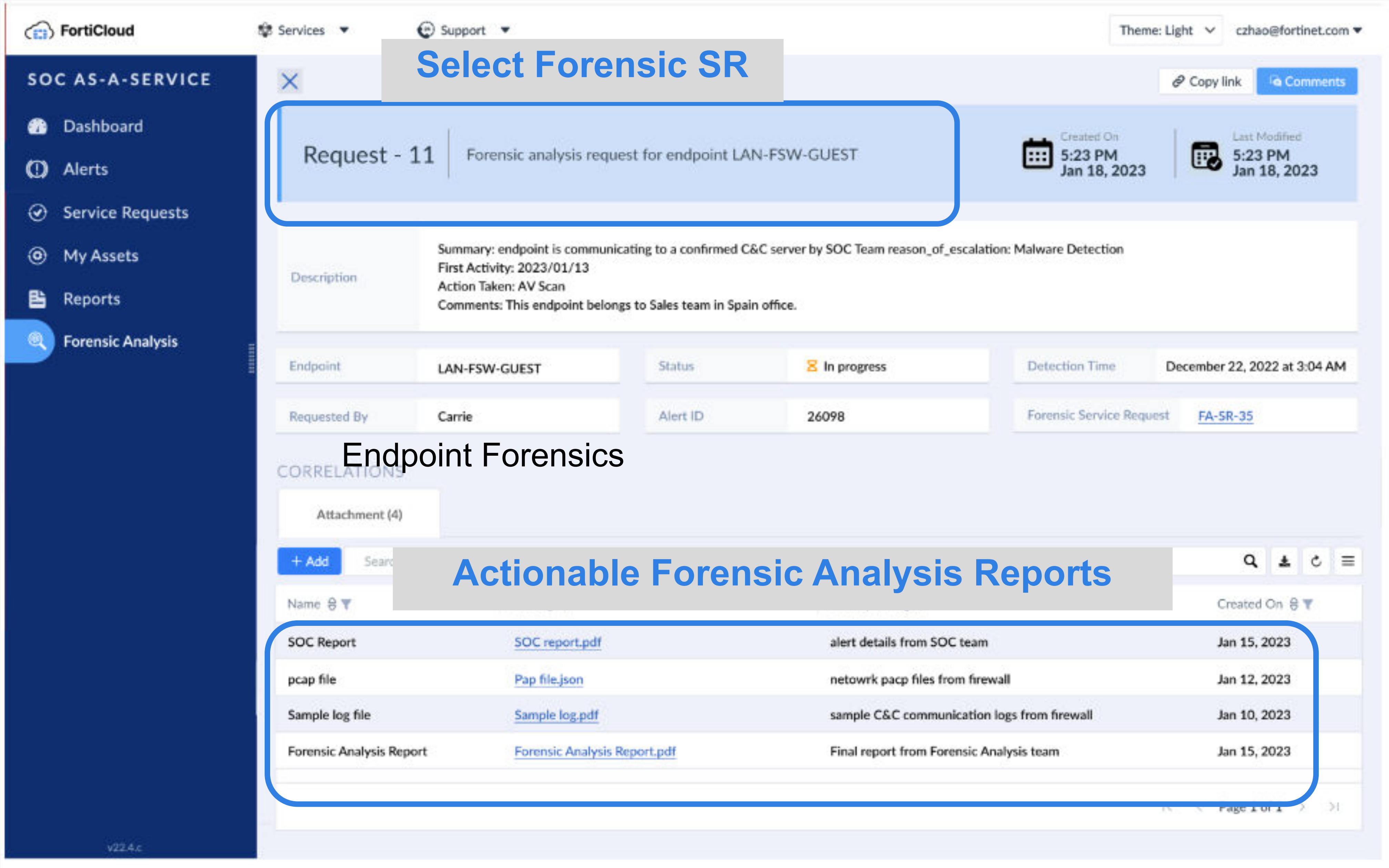
Page 1 of 1



Total Request 3

ID	Created on	Modified on	Requested by	Hostname	Status	Forensic Service Request
11	18/01/2023	18/01/2023	Carrie	LAN-FSW-GUEST	⌛ In progress	FA-SR-35
12	18/01/2023	18/01/2023	Ali	LAN-FSW-USER2	✓ Completed	FA-SR-47
13	18/01/2023	18/01/2023	Jeason	LAN-FSW-USER1	⊘ Cancelled	FA-SR-26

FORENSIC ANALYSIS TAB



Select Forensic SR

Endpoint Forensics

Actionable Forensic Analysis Reports

Request - 11 | Forensic analysis request for endpoint LAN-FSW-GUEST

Created On 5:23 PM Jan 18, 2023

Last Modified 5:23 PM Jan 18, 2023

Description: Summary: endpoint is communicating to a confirmed C&C server by SOC Team reason_of_escalation: Malware Detection
First Activity: 2023/01/13
Action Taken: AV Scan
Comments: This endpoint belongs to Sales team in Spain office.

Endpoint	LAN-FSW-GUEST	Status	In progress	Detection Time	December 22, 2022 at 3:04 AM
Requested By	Carrie	Alert ID	26098	Forensic Service Request	FA-SR-35

CORRELATIONS

Attachment (4)

Name			Created On
SOC Report	SOC report.pdf	alert details from SOC team	Jan 15, 2023
pcap file	Pap file.json	netowrk pacp files from firewall	Jan 12, 2023
Sample log file	Sample log.pdf	sample C&C communication logs from firewall	Jan 10, 2023
Forensic Analysis Report	Forensic Analysis Report.pdf	Final report from Forensic Analysis team	Jan 15, 2023

FORTINET®