

The Fortinet logo, featuring the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is replaced by a red square icon with a white grid pattern.

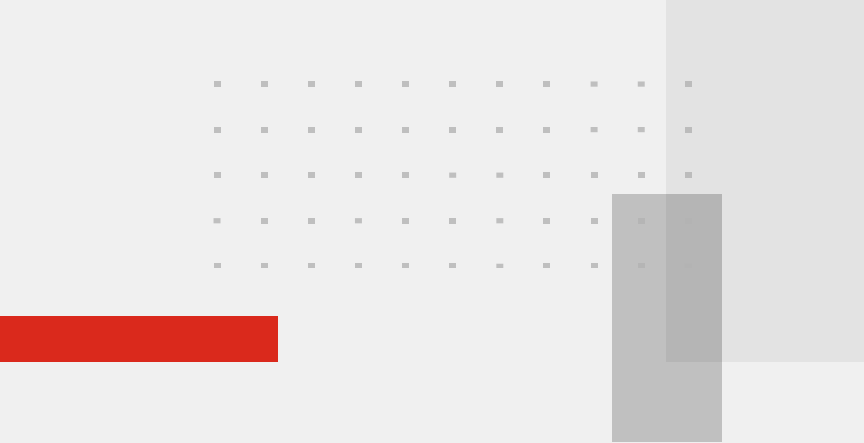
FORTINET

Může ISP efektivně rozšířit NOC a začít budovat SOC?

Jan Kolmačka

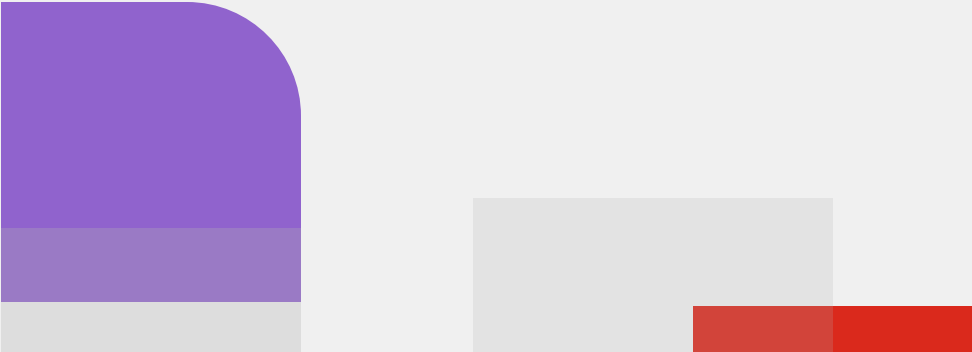
Systems Engineer

A solid red horizontal bar.



Agenda

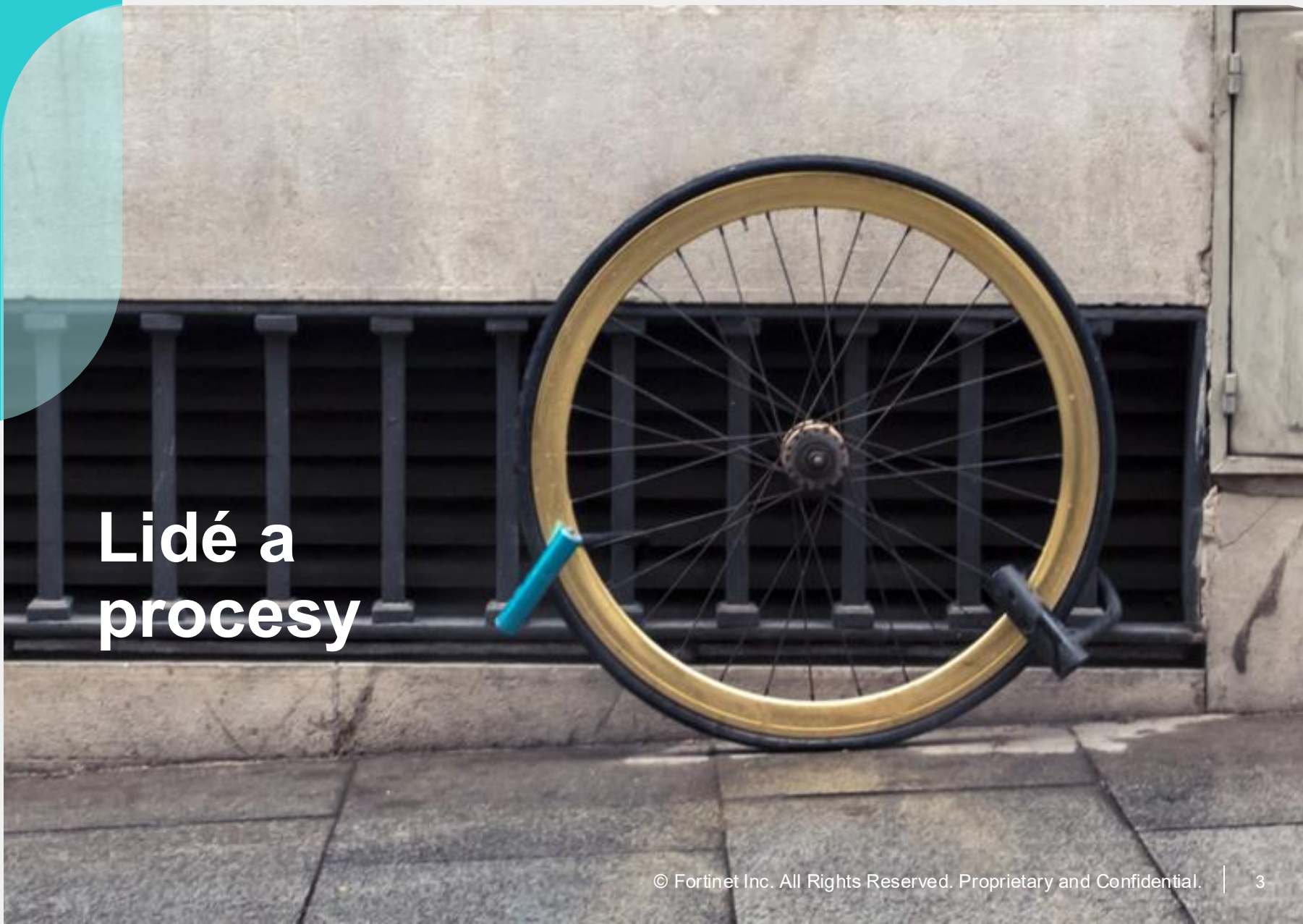
NOC & SOC platformy Fortinetu:

- FortiAnalyzer
 - FortiGuard SOC-as-a-Service
 - Managed FortiGate Service
 - FortiSIEM
- 



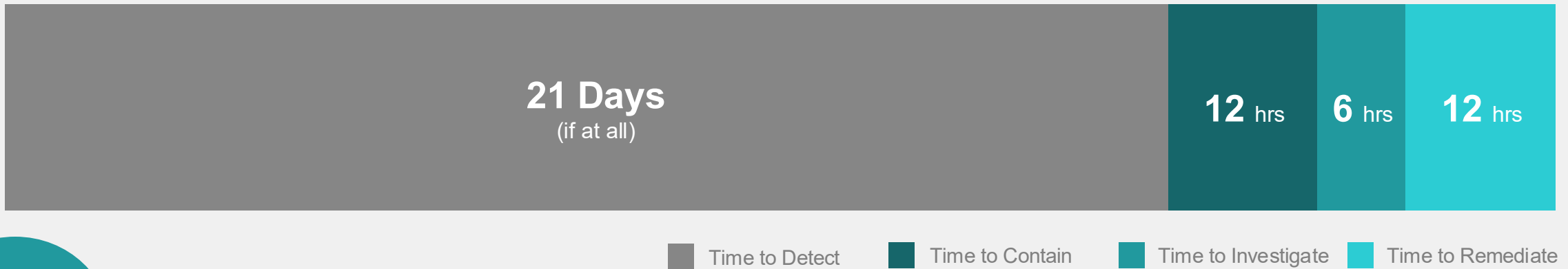
**Falešný
pocit
bezpečí**

**Lidé a
procesy**



Náklady za falešný pocit bezpečí

Průměrný čas od odhalení k vyřešení hrozby



52%

of organizations report
SecOps is harder than 2 years
ago, citing threats, attack
surface, volume/complexity¹

NIS2 Rule

1 Day

to initially report
incident

\$9.4M

Avg Breach Cost



FortiAnalyzer: Funkce na klíč pro začínající SOC



Appliance



Virtual Machine



Cloud



Big Data



Unified Data Lake

Jednotný pohled na logy, dění v síti, výstrahy, hrozby a incidenty

Native Threat Intelligence

Intelligence FortiGuard Labs v reálném čase, včetně Outbreak detekce a Indicator of Compromise (IOC)

Built-in SOC Automation

Zahrnuje odhlehčené funkce SIEMu a SOARu s předkonfigurovaným obsahem

Embedded GenAI-Assistant

Integrovaná FortiAI, pomocí GenAI pro zvýšení efektivity a odezvy

Flexible Deployments

Jednoduché možnosti nasazení jako HW, virtuální appliance nebo v cloudu

FortiAnalyzer: FortiGuard IOC and Outbreak Detection Service

IOC (Indicator of Compromise)

- forenzní data z 500 000 IOC denně
- Seznam IP adres, domén a URL
- FortiAnalyzer identifikuje podezřelé nebo škodlivé infekce a případný průnik
- Historická analýza logů
- Volitelná automatizace pomocí předdefinovaných playbooků

Outbreak Detection

- Aktualizované balíčky hrozeb, event handlerů, korelačních pravidel a reportů
- Souhrné reporty o aktuálních rychle se šířících hrozbách



FortiAnalyzer: Obohacení indikátorů

The screenshot displays the FortiAnalyzer web interface. On the left, the 'Incident Analysis' panel shows a summary for an incident with ID 'IN00000', name 'Malicious-Detections-At-Endpoint', and severity 'High'. The main panel, 'Enrich History', shows the enrichment process for the indicator 'unwaveringmedia.com'. It includes a table with the following data:

Confidence	IOC Category	IOC Tags	Web Filter Category	AV Category
High	Malware CnC	Malware CnC, Backdoor	Malicious Websites	--

Below the table, a 'VirusTotal Summary' section shows a circular progress indicator for 6/93 items. A bar chart displays the results: 6 Malicious (red), 61 Harmless (green), and 26 Undetected (grey). The bottom section, 'Security Vendors' Analysis', shows results from various vendors:

Vendor	Result
Dr.Web	Malicious
AlphaSOC	Malicious
CyRadar	Malicious
Fortinet	Malicious



Intuitivní monitorování a detekce s real-time kontextem síťové aktivity, rizik, zranitelností a pokusů o útok

- Kategorizace hrozeb, stanovení priorit a opětovné skenování
- Vizualizace nalezených hrozeb
- Automatická odezva na detekci hrozeb

FortiAnalyzer: IOC v akci

FAZVM64-KVM

Dashboards

Device Manager

FortiView

Threats

Traffic

Shadow IT

Applications & Websites

VPN

System

Threats & Events

Traffic Analysis

SD-WAN

Fabric Devices

Local System Performan...

Custom Views

Log View

Fabric View

Incidents & Events

FortiAI

Reports

System Settings

Top Threats

Threat Map

Indicator of Compromise

FortiSandbox Detection

Indicator of Compromise > Blocklist

epid=1041

Summary

Source (User/IP): Jan

Last Detected: 2025-03-03 15:00

Host Name: PC01

OS: WIN64

Log Types: webfilter traffic

Security Actions: timeout deny (1+)

Verdict: Infected

of Threats: 2

Acknowledge: ACK

Device Name: Local-FGT

Device ID:

Detect Pattern	Threat Type	Threat Name	Category	Detect Method	# of Events	Log Type	Security Act
192.243.59.20	PUP	SpywareCnC		infected-ip	47	traffic	Details
192.243.61.227	PUP	SpywareCnC		infected-ip	45	traffic	Details
quickerapparently.com	Malware	Attack	Spyware and Malware	infected-domain	3	webfilter	Details
192.243.59.20	PUP	SpywareCnC		infected-ip	2	webfilter	Details
capaciousdrewreligion.com	PUP	SpywareCnC		infected-domain	1	webfilter	Details

Local-FGT

Dashboard

Status

Security

Network

Assets & Identities

WiFi

FortiView Sources

FortiView Destinations

FortiView Applications

FortiView Web Sites

FortiView Policies

FortiView Sessions

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Security Fabric

Log & Report

Quarantine

Category

Banned IP 2

Source

Administrat... 2

Device

10.0.1.150 1

10.200.1.1 1

Create new

Delete

Remove All

Search

Details	Device	Source	Expires	Description
Banned IP 2				
10.0.1.150	10.0.1.150	Administrative	Never	
10.200.1.1	10.200.1.1	Administrative	Never	

5

5

FortiAnalyzer: Security Automation Service

- Poskytuje balíčky obsahující nové reporty, event handlers, korelační pravidla, log parsery, konektory a playbooky pro SIEM/SOAR funkce FortiAnalyzera
- Umožní analyzovat a reagovat na bezpečnostní incidenty pomocí předdefinovaných scénářů
- Aktualizace - nové parsery a pravidla vydávány na pravidelné bázi, cca 1x za měsíc
- Duben 2025: 31 log parserů

Cisco IOS, Aruba, CheckPoint, Palo Alto, Sophos, Juniper, Zscaler, SonicWall, ForcePoint, Okta, SentinelOne, CrowdStrike, Office365, VMware, Windows, Ubuntu, Apache, Nginx, atd....

Aktuální přehled zde:

<https://www.fortiguard.com/services/security-automation-service>

<https://docs.fortinet.com/document/fortianalyzer/7.6.0/soc-automation-content-pack>



FortiAnalyzer: Incidenty

FAZVM64-KVM

Dashboards

Device Manager

FortiView

Log View

Fabric View

Incidents & Events

Incidents

Event Monitor

Event Handlers

Indicators

Outbreak Alerts

Automation

Log Parsers

Safeguarding

FortiAI

Reports

System Settings

FORTINET

Incidents

MITRE ATT&CK@ MITRE ATT&CK@ ICS

31
Total

Severity

High 28 Medium 3 Low 0

31

Status

New 29 Analysis 1 Closed: Remediated 1 Response 0 Review 0 Closed: False Positive 0

31

Category

Unauthorized Access 28 Scans / Probes / Attempts 2 Uncategorized 1 Denial of Service (DoS) 0 Malicious Code 0 Improper Usage 0

28
Total

Outbreak Alerts

High 28 Medium 0 Low 0

Create New Edit Delete Analysis Enrich Block More

All

Show Charts Search...

Name	Severity	Affected Endpoint	Status	Incident Number	Incident Date / Time	Last Update Date / Time	Incident Reporter	Incident Category	MITRE Tech ID
☐ Default-Risky-Destination-Detection-By-Threat happened at Android_1f4c87433fa346288fb6f6379516d846	Medium	192.168.0.113 (Android_1f4c8...	New	IN00000031	2025-02-28 14:06:42	2025-02-28 14:06:43	admin	Uncategorized	T1021.004 T1071.001 T1071.004
☐ Default-Recon-Activity-By-Endpoint happened at PC01.int.lab.local	Medium	10.0.1.150 (PC01)	Analysis	IN00000030	2025-02-27 10:17:28	2025-02-27 12:07:17	admin	Scans / Probes / Atten	T1595.001
☐ Default-Recon-Activity-By-Endpoint happened at DC01	Medium	10.0.1.11 (DC01)	Closed: Remediated	IN00000029	2025-02-26 15:53:49	2025-02-26 16:00:16	admin	Scans / Probes / Atten	T1595.001
☐ Outbreak Alert - CISAtop20_PRC2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.67.7.230	New	IN00000025	2025-02-25 21:11:33	2025-02-25 21:11:55	202502251000000060/Auto-Raised	Unauthorized Access	T1059 T1083 T1125 T1140
☐ Outbreak Alert - Log4j2 Vulnerability Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.67.7.230	New	IN00000026	2025-02-25 21:11:33	2025-02-25 21:11:55	202502251000000062/Auto-Raised	Unauthorized Access	T1140 T1190 T1210 T1592
☐ Outbreak Alert - Routinely Exploited Vulnerabilities 2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.67.7.230	New	IN00000027	2025-02-25 21:11:33	2025-02-25 21:11:55	202502251000000061/Auto-Raised	Unauthorized Access	
☐ Outbreak Alert - Lazarus RAT Attack Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.67.7.230	New	IN00000028	2025-02-25 21:11:33	2025-02-25 21:11:55	202502251000000065/Auto-Raised	Unauthorized Access	T1003 T1003.005 T1033 T108
☐ Outbreak Alert - CISAtop20_PRC2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.133	New	IN00000021	2025-02-18 21:11:09	2025-02-18 21:11:31	202502181000000066/Auto-Raised	Unauthorized Access	T1059 T1083 T1125 T1140
☐ Outbreak Alert - Routinely Exploited Vulnerabilities 2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.133	New	IN00000022	2025-02-18 21:11:09	2025-02-18 21:11:31	202502181000000067/Auto-Raised	Unauthorized Access	
☐ Outbreak Alert - Lazarus RAT Attack Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.133	New	IN00000023	2025-02-18 21:11:09	2025-02-18 21:11:31	202502181000000071/Auto-Raised	Unauthorized Access	T1003 T1003.005 T1033 T108
☐ Outbreak Alert - Log4j2 Vulnerability Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.133	New	IN00000024	2025-02-18 21:11:09	2025-02-18 21:11:31	202502181000000068/Auto-Raised	Unauthorized Access	T1140 T1190 T1210 T1592
☐ Outbreak Alert - CISAtop20_PRC2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.67.7.141	New	IN00000017	2025-02-11 21:11:46	2025-02-11 21:12:13	202502111000000055/Auto-Raised	Unauthorized Access	T1059 T1083 T1125 T1140
☐ Outbreak Alert - Log4j2 Vulnerability Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.67.7.141	New	IN00000018	2025-02-11 21:11:46	2025-02-11 21:12:13	202502111000000057/Auto-Raised	Unauthorized Access	T1140 T1190 T1210 T1592
☐ Outbreak Alert - Lazarus RAT Attack Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.67.7.141	New	IN00000019	2025-02-11 21:11:46	2025-02-11 21:12:13	202502111000000060/Auto-Raised	Unauthorized Access	T1003 T1003.005 T1033 T108
☐ Outbreak Alert - Routinely Exploited Vulnerabilities 2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.67.7.141	New	IN00000020	2025-02-11 21:11:46	2025-02-11 21:12:13	202502111000000056/Auto-Raised	Unauthorized Access	
☐ Outbreak Alert - Routinely Exploited Vulnerabilities 2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.224	New	IN00000013	2025-02-04 21:10:58	2025-02-04 21:11:25	202502041000000061/Auto-Raised	Unauthorized Access	
☐ Outbreak Alert - Lazarus RAT Attack Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.224	New	IN00000014	2025-02-04 21:10:58	2025-02-04 21:11:25	202502041000000065/Auto-Raised	Unauthorized Access	T1003 T1003.005 T1033 T108
☒ Outbreak Alert - CISAtop20_PRC2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.224	New	IN00000015	2025-02-04 21:10:58	2025-02-04 21:11:25	202502041000000060/Auto-Raised	Unauthorized Access	T1059 T1083 T1125 T1140
☐ Outbreak Alert - Log4j2 Vulnerability Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.224	New	IN00000016	2025-02-04 21:10:58	2025-02-04 21:11:25	202502041000000062/Auto-Raised	Unauthorized Access	T1140 T1190 T1210 T1592
☐ Outbreak Alert - Routinely Exploited Vulnerabilities 2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.167	New	IN00000009	2025-01-28 21:10:11	2025-01-28 21:10:37	202501281000000060/Auto-Raised	Unauthorized Access	
☐ Outbreak Alert - CISAtop20_PRC2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.167	New	IN00000010	2025-01-28 21:10:11	2025-01-28 21:10:37	202501281000000059/Auto-Raised	Unauthorized Access	T1059 T1083 T1125 T1140
☐ Outbreak Alert - Log4j2 Vulnerability Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.167	New	IN00000011	2025-01-28 21:10:11	2025-01-28 21:10:37	202501281000000061/Auto-Raised	Unauthorized Access	T1140 T1190 T1210 T1592
☐ Outbreak Alert - Lazarus RAT Attack Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	3.124.123.167	New	IN00000012	2025-01-28 21:10:11	2025-01-28 21:10:37	202501281000000064/Auto-Raised	Unauthorized Access	T1003 T1003.005 T1033 T108
☐ Outbreak Alert - Routinely Exploited Vulnerabilities 2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	54.93.254.186	New	IN00000005	2025-01-21 21:11:58	2025-01-21 21:12:25	202501211000000056/Auto-Raised	Unauthorized Access	
☐ Outbreak Alert - Log4j2 Vulnerability Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	54.93.254.186	New	IN00000006	2025-01-21 21:11:58	2025-01-21 21:12:25	202501211000000057/Auto-Raised	Unauthorized Access	T1140 T1190 T1210 T1592
☐ Outbreak Alert - Lazarus RAT Attack Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	54.93.254.186	New	IN00000007	2025-01-21 21:11:58	2025-01-21 21:12:25	202501211000000060/Auto-Raised	Unauthorized Access	T1003 T1003.005 T1033 T108
☐ Outbreak Alert - CISAtop20_PRC2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	54.93.254.186	New	IN00000008	2025-01-21 21:11:58	2025-01-21 21:12:25	202501211000000055/Auto-Raised	Unauthorized Access	T1059 T1083 T1125 T1140
☐ Outbreak Alert - CISAtop20_PRC2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	18.194.95.86	New	IN00000001	2025-01-14 21:11:15	2025-01-14 21:11:41	202501141000000145/Auto-Raised	Unauthorized Access	T1059 T1083 T1125 T1140
☐ Outbreak Alert - Routinely Exploited Vulnerabilities 2022 Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	18.194.95.86	New	IN00000002	2025-01-14 21:11:15	2025-01-14 21:11:41	202501141000000146/Auto-Raised	Unauthorized Access	
☐ Outbreak Alert - Log4j2 Vulnerability Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	18.194.95.86	New	IN00000003	2025-01-14 21:11:15	2025-01-14 21:11:41	202501141000000147/Auto-Raised	Unauthorized Access	T1140 T1190 T1210 T1592
☐ Outbreak Alert - Lazarus RAT Attack Event-Handler: Attack Apache.Log4j.Error.Log.Remote.Code.Execution detected	High	18.194.95.86	New	IN00000004	2025-01-14 21:11:15	2025-01-14 21:11:41	202501141000000150/Auto-Raised	Unauthorized Access	T1003 T1003.005 T1033 T108

FortiAnalyzer: Detail incidentu

FAZVM64-KVM

Dashboards

Device Manager

FortiView

Log View

Fabric View

Incidents & Events

Incidents

Event Monitor

Event Handlers

Indicators

Outbreak Alerts

Automation

Log Parsers

Safeguarding

FortiAI

Reports

System Settings

Incident Analysis

Medium

Default-Recon-Activity-By-Endpoint happened at DC01 IN00000029

Edit Layout

Export Incident

Enrich

Block

Execute Playbook

Run Report

Quarantine

Refresh

Incident Summary

Incident Number

IN00000029

Incident Name

Default-Recon-Activity-By-Endpoint happened at DC01

Incident Date / Time

2025-02-26 15:53:49

Incident Update Date / Time

2025-02-26 16:00:16

Incident Category

Scans/Probes/Attempted Access

Mitre Tech ID

T1595.001 Scanning IP Blocks

Click to select

1 entry selected

Severity

Medium

Status

Closed: Remediated

Affected Endpoint

10.0.1.11 (DC01)

Description

Default-Recon-Activity-By-Endpoint happened at DC01

Affected Endpoint/User

Affected Endpoint/User

No related user available.

Last Seen

2025-02-26 15:53:49

Topology

DC01

Addresses

MAC: bc:24:11:85:c4:dd
IP: 10.0.1.11

Operating System

Windows 10

Comments

A

POST

Affected Assets

Endpoint	User	IP Address	MAC Address
DC01	N/A no enough info	10.0.1.11	bc:24:11:85:c4:dd

Incident Timeline

From 2025-02-26 15:24:09 To 2025-02-26 15:24:04 (Total 1 Event)

14:55

15:00

15:05

15:10

15:15

15:20

15:25

15:30

15:35

15:40

15:45

15:50

15:55

16:00

16:05

16:10

16:15

16:20

Reset Zoom

Events

View Logs

Search in Log View

Delete

Event	Count	Severity	Last Occurrence	Handler	Indicators
IP scanning on Port: 443 detected	58	Medium	2025-02-26 15:24:04	Default-Recon-Activity-By-Endpoint	

Audit History

2025-03-03 13:57:42

Now

Incident Updated

By: admin

Executed Playbooks

Playbook	Status	Trigger
Quarantine Endpoint by FortiOS	Success	admin
Quarantine Endpoint by FortiOS	Success	admin
Quarantine Endpoint by FortiOS	Failed	admin

Incident Updated

By: admin

Close



FortiAnalyzer: Playbooky

FAZVM64-KVM

Dashboards

Device Manager

FortiView

Log View

Fabric View

Incidents & Events

Incidents

Event Monitor

Event Handlers

Indicators

Outbreak Alerts

Automation

Log Parsers

Safeguarding

FortiAI

Reports

System Settings

FortiNET

SummaryActive ConnectorsPlaybookPlaybook Monitor

+ Create New

⌂ Run

✎ Edit

📄 Clone

🗑 Delete

🟢 Enable

🔴 Disable

⋮ More

☐	Name	Description	Status	Cr
☐	Get IP Reputation	Playbook to get IP reputation report through VirusTotal connector	🟢Enabled	01
☐	Get Domain Reputation	Playbook to get domain reputation report through VirusTotal connector	🟢Enabled	01
☐	Get URL Reputation	Playbook to get URL reputation report through VirusTotal connector	🟢Enabled	01
☐	Incident - Run Report	Playbook to generate incident report	🟢Enabled	05
☐	Enrich Incident with Vulnerability List	Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.	🟢Enabled	La
☐	Update Asset and Identity Database	Playbook to automatically update FortiAnalyzer Asset and Identity database with endpoint and user information from EMS	🟢Enabled	La
☐	EMS - Get Endpoint Process	Playbook to get endpoint process	🟢Enabled	05
☐	Quarantine Endpoint by EMS	Playbook to quarantine endpoint by EMS connector	🟢Enabled	03
☐	Indicator Enrichment	Enrich indicator with different connectors	🟢Enabled	03
☐	Enrich Incident with Software Inventory	Playbook to get software inventory from endpoint by EMS Connector and attach to incident.	🟢Enabled	La
☐	Compromised Host Incident	Playbook to create incident on FortiAnalyzer for detected compromised hosts by IoC feature.	🟢Enabled	La
☐	Quarantine Endpoint by EMS - AI	Playbook to quarantine endpoint by EMS connector - AI	🟢Enabled	05
☐	Unquarantine Endpoint by EMS	Playbook to unquarantine endpoint by EMS connector	🟢Enabled	La

Choose from Playbook Templates

New Playbook created from scratch
Custom build playbook to get started

Attach Endpoint Vulnerability list to incident
Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.

Compromised Host Incident
Playbook to create incident on FortiAnalyzer for detected compromised hosts by IoC feature.

Critical Intrusion Incident
Playbook to create incident on FortiAnalyzer for detected critical intrusions by IPS

Enrich Incident with Process List
Playbook to get running processes on endpoint by EMS connector and attach to incident.

Enrich Incident with Software Inventory
Playbook to get software inventory from endpoint by EMS Connector and attach to incident.

Enrich Incident with Vulnerability List
Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.

Quarantine Endpoint by EMS
Playbook to quarantine endpoint by EMS connector

Quarantine Endpoint by FortiOS
Playbook to quarantine endpoint by FOS connector providing MAC address or FortiClient UID

Run AV Scan on Endpoint
Playbook to run AV scan on Endpoint by EMS Connector

Run Vulnerability Scan on Endpoint
Playbook to run vulnerability scan on endpoint.

Unquarantine Endpoint by EMS
Playbook to unquarantine endpoint by EMS connector

Update Asset and Identity Database
Playbook to automatically update FortiAnalyzer Asset and Identity database with endpoint and user information from EMS

FortiAnalyzer: Konektory

FAZVM64-KVM

Dashboards

Device Manager

FortiView

Log View

Fabric View

Incidents & Events

Incidents

Event Monitor

Event Handlers

Indicators

Outbreak Alerts

Automation

Log Parsers

Safeguarding

FortiAI

Reports

System Settings

SummaryActive ConnectorsPlaybookPlaybook Monitor

+ Create New

Edit

Delete

Clone

Fortinet Connectors (9)

FortiOS Connector

Enables seamless integration with FortiOS for centralized management and

FortiOS

0 device connected4 devices disconnected

Local Connector

The Local Connector facilitates communication and data exchange between FortiAnalyzer and

Local Host

FortiGuard Connector

Provides connectivity to FortiGuard services for accessing real-time threat intelligence feeds, security

FortiGuard

FortiAuthenticator Co...

Integrates FortiAuthenticator with other Fortinet products to centralize and manage

FortiAuthenticator

FortiCasb Connector

Facilitates integration with FortiCASB for centralized visibility and control over cloud applications,

FortiCASB

FortiClient EMS Conn...

Allows seamless integration with FortiClient EMS for centralized management and

FortiClient EMS

Third Party Connectors (1)

VirusTotal Connector

Allows FortiAnalyzer to use VirusTotal's threat intelligence services. This enables FortiAnalyzer to

VirusTotal

Create New Fabric Connector - Select Connector Type (1/2)

Please choose a connector type

Search...

Security Fabric (8)

FortiClient EMS

FortiMail

FortiCASB

FortiAuthenticator

FortiWeb

FortiSandbox

vSphere

Microsoft Management Activity API v1.0.1

ITSM (4)

ServiceNow Connector

Slack Connector

MS Teams Connector

Generic Connector

Next

Cancel

FORTINET

FortiAnalyzer: FortiAI

- Generativní AI, umí pomoci v oblasti analýzy logů a SecOps práce
- Interpretace security eventů, generuje souhrn, vyhodnotí potenciální dopad a poskytne případná doporučení k nápravě
- Umí pomoci vytvářet složité databázové dotazy, reporty, event handlers a SIEM detekční pravidla
- Podpora 30+ jazyků včetně češtiny!





Hi, how can I help you?

ukaz mi hrozby za posledni 2 hodiny

A



Hrozby za poslední 2 hodiny byly zobrazeny na stránce Fortiview -> Top Threats.

Možné další akce:

1. Zhrnout události
2. Vytvořit Event Handler

Pokud budete potřebovat další informace nebo akce, dejte mi vědět.

o jaké kategorie se jednalo?

A



Za poslední 2 hodiny byly zaznamenány následující kategorie hrozeb:

Kategorie	Počet incidentů	Úroveň	Hrozby
Blocked Connection	7973	High	blocked-connection
Malicious Websites	9	High	quickerapparently.com, supportsentparticle.com, experttrafficcounter.com, unseenreport.com
Phishing	1	High	cdn.show-sb.com
Failed Connection	3757	Low	failed-connection
Pornography	13	Low	ei.phncdn.com, ht-cdn2.adtng.com, pornhub.com, cdn1-smalling.phncdn.com

Profesionální kybernetická doporučení:

1. **Blokované připojení a neúspěšné připojení:** Proveďte analýzu blokováných a neúspěšných připojení, abyste zjistili, zda jsou legitimní nebo je třeba provést další opatření.
2. **Malicious Websites a Phishing:** Ujistěte se, že máte nasazený aktuální firewall a podpisy pro detekci škodlivých webů a phishingových útoků. Proveďte školení uživatelů o bezpečné práci s internetem.
3. **Pornografie:** Použijte filtry obsahu pro kontrolu přístupu k nevhodným webovým stránkám, aby nedocházelo k narušení pracovní morálky a bezpečnosti.

Máte zájem o bližší analýzu některé z kategorií nebo další akce?



pro škodlivé stránky za poslední 2 hodiny.

Můžeme nyní pokračovat s analýzou nalezených škodlivých stránek. Pokud potřebujete další akce nebo konkrétní informace, dejte mi vědět.

vytvor event handler pro nalezene hrozby za posledni 2 hodiny

A



Event Handler pro detekci nalezených škodlivých stránek za poslední 2 hodiny byl úspěšně vytvořen.

Detaily Event Handleru

- **Název:** Malicious Websites Detection
- **Popis:** Detekce a sledování škodlivých webových stránek za poslední 2 hodiny
- **MITRE Technique ID:** T1071.001 (Application Layer Protocol)
- **Pravidlo:**
 - **Název:** Malicious Websites Log Monitoring
 - **Skupina:** appcat
 - **Filtrované kategorie:** Malicious Websites za poslední 2 hodiny
 - **Typ logu:** Web Filter

Pokud budete potřebovat další akce nebo informace, dejte mi vědět.

nastav aby v pridate detekce danym eventhandler byly zablokovany souvisejici cilove adresy

A



Event Handler pro detekci nalezených škodlivých stránek s automatickou karanténou souvisejících cílových adres byl úspěšně vytvořen.

Detaily Event Handleru

- **Název:** Malicious Websites Detection and Quarantine
- **Popis:** Detekce a sledování škodlivých webových stránek za poslední 2 hodiny a automatická karanténa souvisejících cílových adres
- **MITRE Technique ID:** T1071.001 (Application Layer Protocol)
- **Pravidlo:**
 - **Název:** Malicious Websites Log Monitoring and Quarantine
 - **Skupina:** appcat
 - **Filtrované kategorie:** Malicious Websites za poslední 2 hodiny
 - **Typ logu:** Web Filter

Při detekci bude nyní automaticky prováděna karanténa souvisejících cílových adres. Pokud máte další požadavky nebo potřebujete další informace, dejte mi vědět.

Kdy nasadit FortiAnalyzer? Úplně VŽDY!

Každý zákazník s FortiGatem

- Nabízet i pro malé instalace FortiAnalyzer VM Free Trial licenci (3 zařízení, 2 ADOMy, 1GB/den)
- Trial obsahuje i 1 roční IOC licenci a SOC funkce
- Bez technické podpory

Pro pokrytí logování nejen Fortinet portfolia

- FortiGate, FortiClient, FortiAP, FortiSwitch, Cisco IOS, Aruba, CheckPoint, Palo Alto, Sophos, Juniper, Zscaler, Windows, Ubuntu, Syslog...atd.
- V základě rychlý přehled aktuální situace, vyhledávání, analýza, archivace logu a pokročilý reporting

Pro začínající SOC

- Odlehčené SIEM funkce – Incident a Event management, korelace, parsery, event handlers
- Základní SOAR Automatizace – vzorové playbooky na karanténu, blokaci, alerting,...atd.
- Umělá inteligence – FortiAI



FortiAnalyzer: MSSP režim

ISP provozuje logování jako službu pro své zákazníky

- Jednoduchá implementace – 1 IP adresa z pohledu zákazníka
- Zákazník získá:
 - Spolehlivě centrálně uložené logy, přehledy, pravidelný reporting
 - Volitelně možnost náhledu na logy
 - SOC funkce a automatizaci
 - Blokace IP na FortiGatu, karanténa klienta – FortiClient, FortiSwitch, FortiAP
 - Automatické notifikace emailem nebo zprávou na MS Teams, Slack
- Typicky VM řešení – onprem VMware, Hyper-V, KVM
- Jednoduché licencování a škálovatelnost – GB/day licenční model



FortiAnalyzer: Licencování

- Platforma VM, Cloud, HW box
- GB/day licenční model
- VM - perpetual nebo subskripce

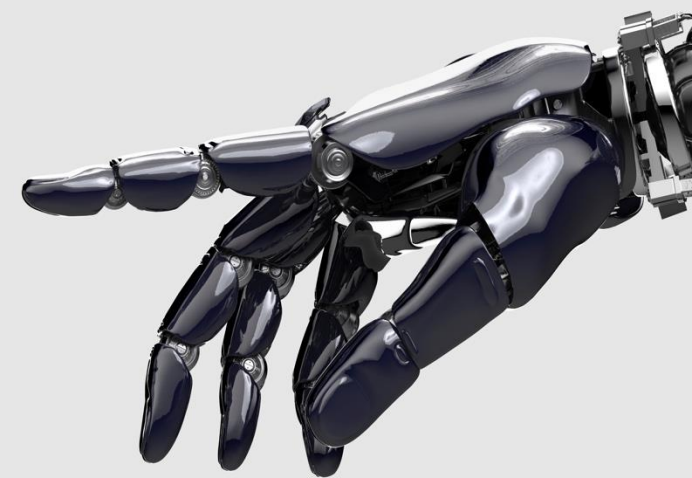
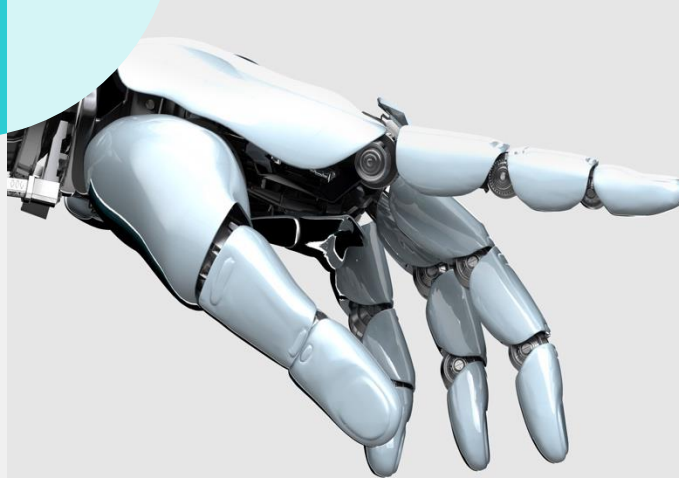
Nejvýhodnější je VM subskripce obsahuje přehledy, logy, reporting, IOC + SOC funkce

- GB/day
- IOC & Outbreak Detection,
- Security Automation Service
- FortiCare Premium Support
- Pouze 5 ADOM, další možno dokoupit



Představení: 24/7 Security Monitoring

Více proaktivních schopností
pro zdokonalování vašich
bezpečnostních operací a
zmírnění obav z napadení a
kompromitace



24/7 Bezpečnostní monitoring s FortiGuard SOCaaS



Fortinet Security Experts



AI-Powered Technologies



FortiGuard Labs



Predictable Pricing



Rapid Deployment

Alert Acknowledgment

2.5

Minutes

Triage Critical Alerts

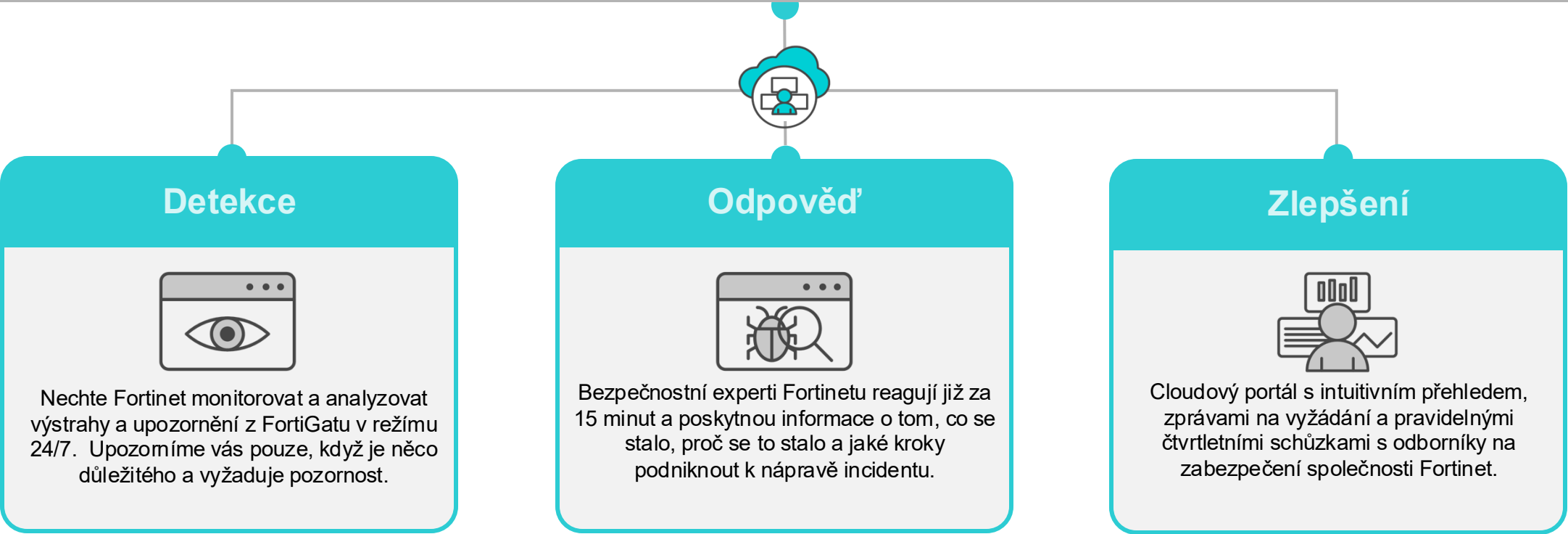
5-12

Minutes

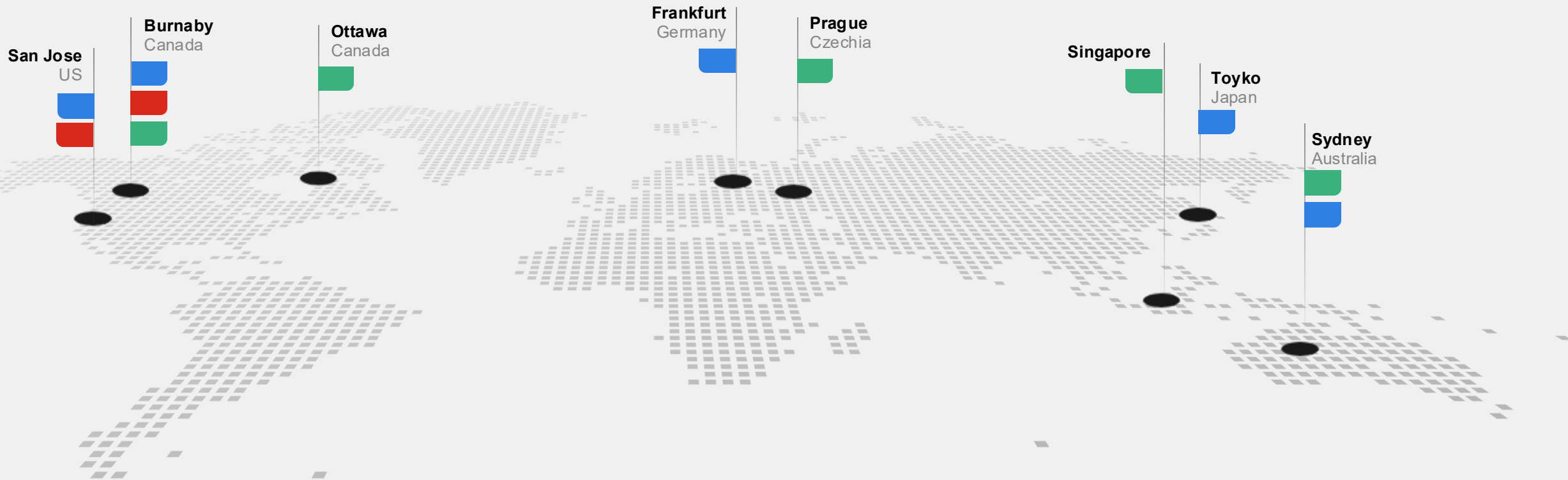
Average

15

Minutes MTTR



FortiGuard SOCaaS: Global Security Operation and Data Centers



Global Response Teams

- SOC
- Data Center
- Disaster Recover

Critical Escalation Times

- P1, Priority 1: 15 minutes
- P2, Priority 2: 45 minutes
- P3, Priority 3: 90 minutes
- P4, Priority 4: 6 hours



99.99%
Availability

24x7x365
Service Hours

Unlimited
Log Capacity

FortiGate & Security Fabric logs
Ingest Log Data

Fast & Simple
Onboarding



FortiGuard SOCaaS: Fortinet Experti, Technologie a Threat Informace

Automatizovaná reakce na incidenty

Incident Monitoring Management



Logy

FortiGate, FortiSASE, FortiClient, FortiEDR a telemetrická data



Bezpečnostní události

Mapování na MITRE a detekční pravidla v cloudové FortiAnalyzeru



Korelace výstrah

FortiSOAR vedoucí platforma orchestrace a automatizace pro snížení false positive



Analýza

Fortinet experti analyzují a eskalují incidenty



Incident

Notifikace zákaznického SOCu



FortiGuard SOCaaS: Komunikace v reálném čase s Fortinet experty

Reakce když je potřeba



Rychlá odezva

Eskalace potvrzených problémů již za 15 minut s upozorněním na telefon, e-mail a cloudový portál SOCaaS



Spolupráce s Fortinet odborníky

Podrobné instrukce krok za krokem:

- Co se stalo – Proč – Dopad – Kroky k nápravě



Komunikace v reálném čase

24/7 podpora pro jakékoliv dotazy

The screenshot displays the FortiGuard SOCaaS portal interface. At the top, there's a navigation bar with 'Alerts' and 'Support' tabs. The main content area shows an alert titled 'Alert-73684' with a 'Medium' severity. The alert description states: 'Fortinet SOC has detected Device Logging Issue for SOC-FGT10 (FGVM04TM21004343) / FGVM SLTM21002681.' The 'Analysis And Recommendation' section provides details about the logging status for two devices, including their names, IP addresses, platforms, and serial numbers. A 'Comments' sidebar on the right shows a search bar, a table with alert details (Severity: Medium, Type: Logging, Detection Time: 2023-01-09 08:13:32 +00:00), and a confidentiality notice. Below the notice, a comment from 'Max' is visible, dated January 9, with a link to the incident response page. At the bottom, there's a table with columns for 'URL', 'Enriched', and 'High', showing a URL 'https://start...' and a 'Malicious Websites' status.

FortiGuard SOCaaS: Pravidelné týdenní reporty

Snadné sledování všeho na čem se pracuje nebo pracovalo

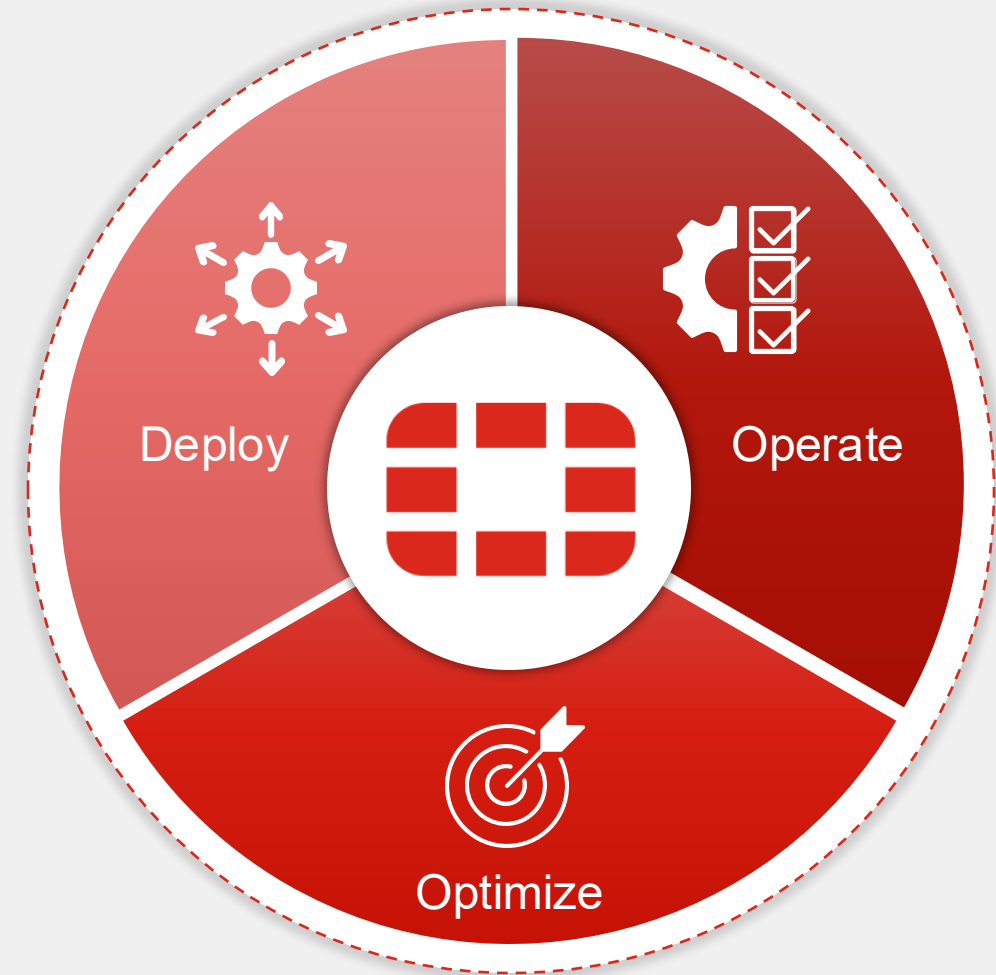
ID	TENANT	CREATED ON	RESOLVED DATE	NAME	STATUS	TYPE	SEVERI...	DESCRIPTION	CLOSURE NOTES
7208		03/11/2022 06:15 PM	03/15/2022 02:44 PM	Malware Activity detected from	Closed (Risk Accepted)	Malware	High	Malware detection in Sandbox detected Malware Action = quarantinefailed File Name = C:\Users\...\AppData\Local\Packages\microso ft.windowscommunicationsapps_8wekyb3d8bbw e\LocalState\Files\50\28\Attachments\Baw чвет нополнен. - DzMNa37mTnCxobr4jeFDRqcgUByVAhdSEI86wfk IZYPW1UJKIX[2639].html	BYOD PC has been ban from network
7109		03/02/2022 06:18 PM	03/15/2022 02:19 PM	Malware Activity detected from	Closed (Risk Accepted)	Malware	High	Malware detected on host	ran full malware scan, no malware detected.
7068		02/23/2022 09:12 PM	03/15/2022 02:17 PM	Malware Activity detected from	Closed (Risk Accepted)	Malware	High	Unhandled malware detections for files in	ran full malware scan, no malware detected, PC is clean
6742		01/09/2022 11:18 PM	03/11/2022 10:45 AM	FCT detected unhandled malware from	Closed (Risk Accepted)	Malware	High	FCT detected unhandled malware from	user was not connected to ems (possibly why the file failed to quarantine) confirmed with user that file is no longer there full av scan results are clean
7274		03/18/2022 06:30 PM	03/21/2022 03:20 PM	Malware Activity detected from	Closed (Resolved)	Malware	High	Unhandled malware declared in	file was quarantined and removed
7054		02/22/2022 07:54 PM	03/16/2022 10:22 AM	Malware Activity detected from	Closed (Resolved)	Malware	High	Quarantine failed for	manual scan via EMS came clean, archiving the case.
7275		03/18/2022 07:03 PM	03/21/2022 04:37 PM	High Risk Traffic detected from	Closed (Risk Accepted)	High Risk Traffic	Medium	CryptoMiner detected on	this is FGD one time event
7270		03/18/2022 12:57 AM	03/21/2022 09:14 AM	Malicious Email detected from	Closed (Risk Accepted)	Malicious Email	Medium	Virus detected in mail from	was a test
7259		03/16/2022 04:06 PM	03/22/2022 12:11 PM	High Risk Traffic detected from	Closed (Risk Accepted)	High Risk Traffic	Medium	Potential dataexfil from	was a test
7228		03/14/2022 05:51 PM	03/17/2022 12:15 PM	High Risk App Usage detected from	Closed (Risk Accepted)	High Risk App	Medium	Tor app detected	The traffic is being blocked by our FW. We are not able to find the owner of this IP.
7198		03/10/2022 11:36 PM	03/15/2022 02:41 PM	Botnet traffic detected to CnC server: related to	Closed (Risk Accepted)	High Risk Traffic	Medium	Fortinet SOC has repeatedly detected Botnet traffic attempts Sunburst from to	Endpoint Quarantine, ongoing investigation



Managed FortiGate Service



- Specializovaný tým odborníků je k dispozici 24/7
- Zjednodušení a optimalizace síťové správy a aktivit.



Managed FortiGate Service: Co všechno za vás uděláme?



Device Provisioning

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



Change Management

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



System Hardening

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



FortiSIEM Platform

SaaS, Virtual Appliance and Hardware Appliance

