

The Fortinet logo is displayed in the top left corner. It features the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is replaced by a red square with a white grid pattern. A registered trademark symbol (®) is located at the end of the word. The logo is set against a semi-transparent white rectangular background.

FORTINET®

A central 3D cube is illuminated with a bright blue glow. The letters "AI" are visible on two of its faces. The cube is positioned on a dark, textured surface that resembles a circuit board or a network map, with glowing blue lines and nodes. The background is a dark, blue-toned image of a circuit board with various components and traces.

Next-Gen Cybersecurity

Leveraging AI for Enhanced Threat Detection and Response

Daniel Ferreira

Manager Regional Sales | CyberSecurity Specialist

Artificial Intelligence took us to



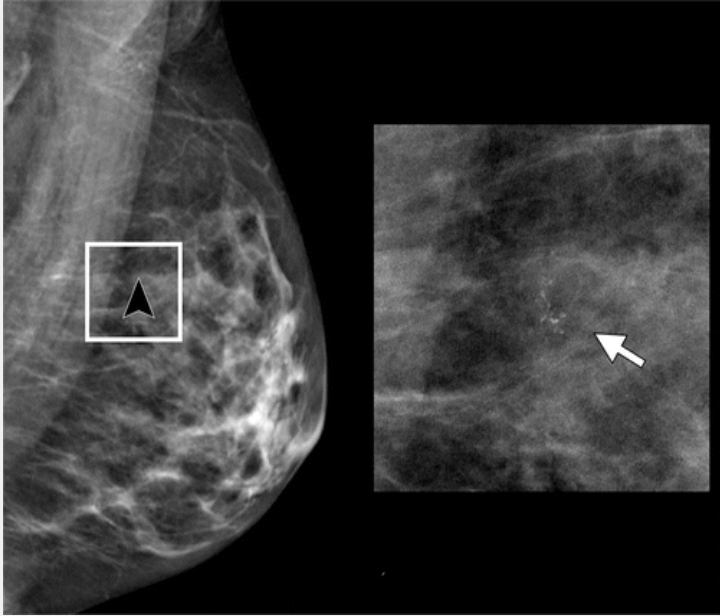
MARS

Perseverance rover in MARS!
The spaceship that transported it had choose the place to land!



UNLOCK the EARLY UNIVERSE

JamesWebb SpaceTelescope folded up for launch.
Webb Telescope aim is to unlock the early Universe!



EARLY BREST CANCER DETECTION

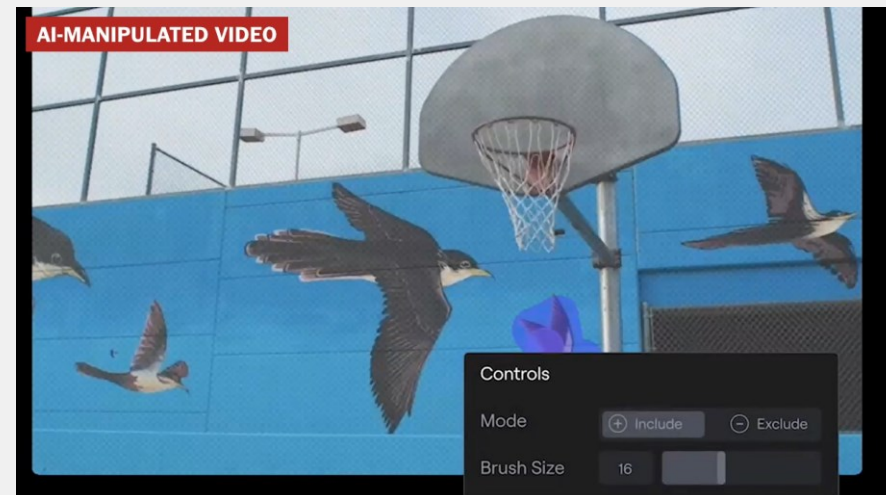
Radboud University, Advanced X-ray Tomographic Imaging w/ AI
AI Algoritms see cancer before any human can see!



But it didn't stop there!



But it didn't stop there!





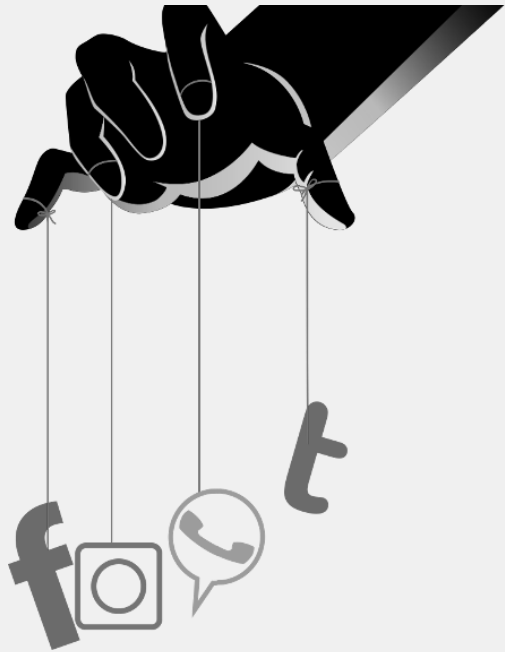
Uncontrolled, is going to far!

Hackers Steal \$25 million by Deepfaking



Artificial Intelligence Can be Misused!

Targeting people opinion by
Manipulating Information



Targeting people activities by
Disrupting Operations



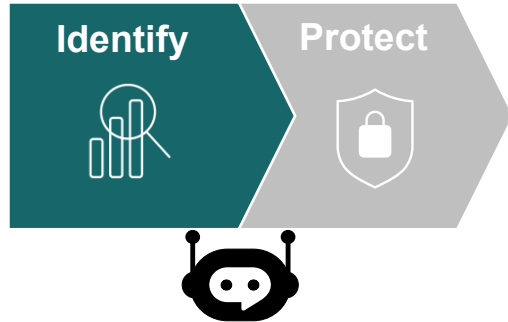


How does Artificial Intelligence Helps Cybersecurity Operations



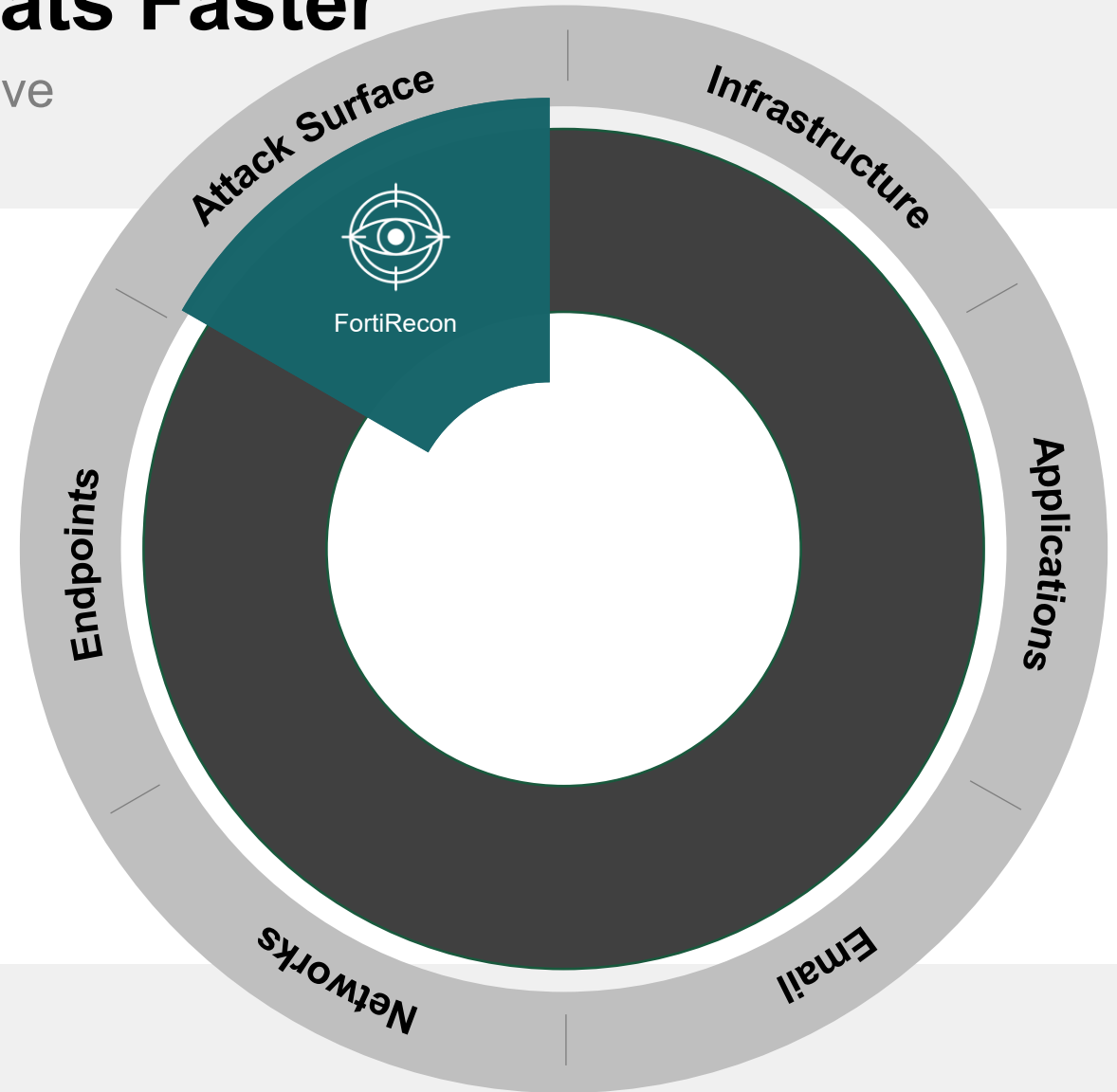
AI-Powered Security Operations Detects and Responds to Threats Faster

Alignment to NIST cybersecurity framework to improve risk management



AI CYBERSECURITY TASKS

- External Attack Surface Management
- Dark Web Threat Intelligence Collection
- Domain Monitoring and Protection
- Adversary Centric Intelligence



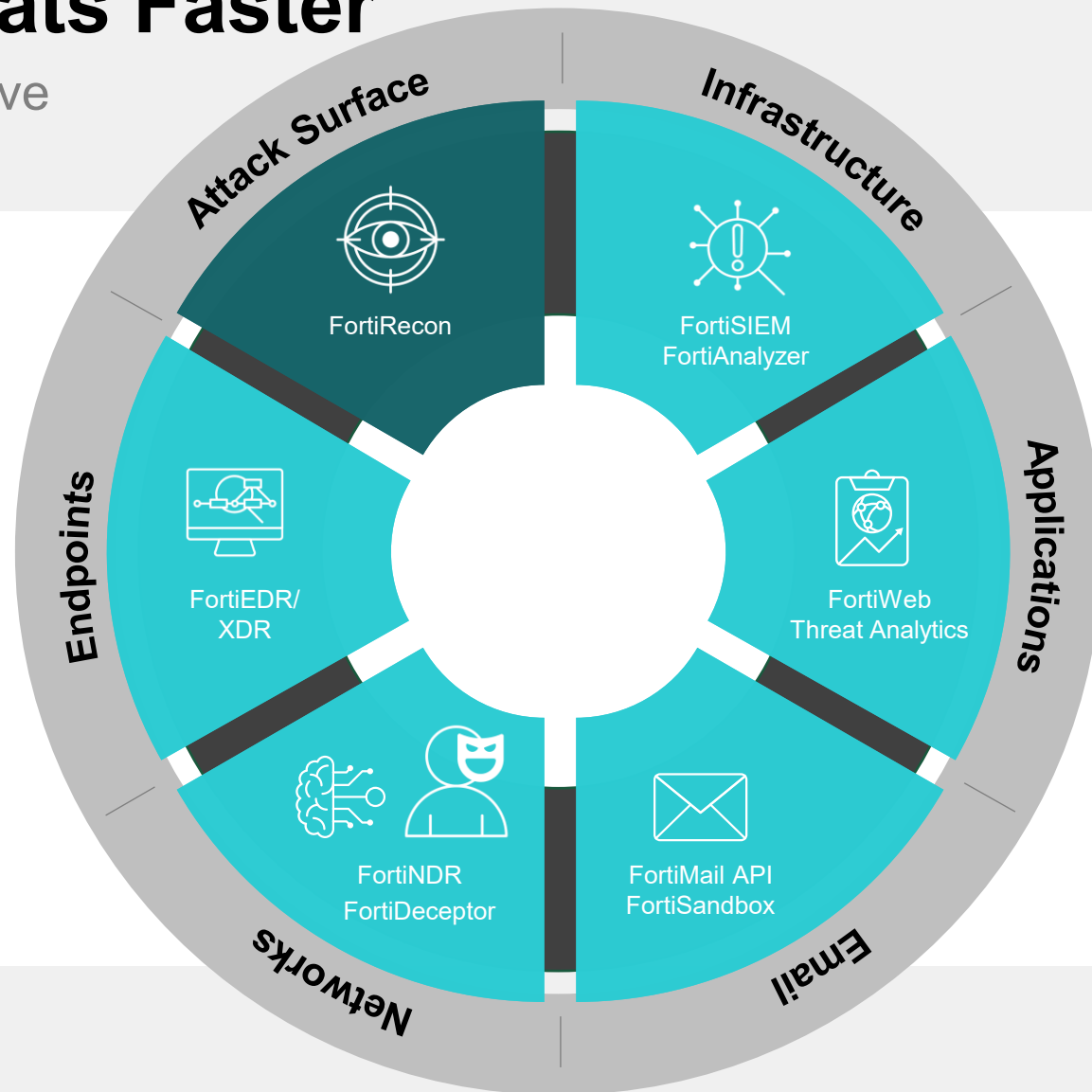
AI-Powered Security Operations Detects and Responds to Threats Faster

Alignment to NIST cybersecurity framework to improve risk management



AI CYBERSECURITY TASKS

- Accurate detection
- Attack Clustering for Attribution
- Dynamic Honeypotting
- Deceptive documentation generation



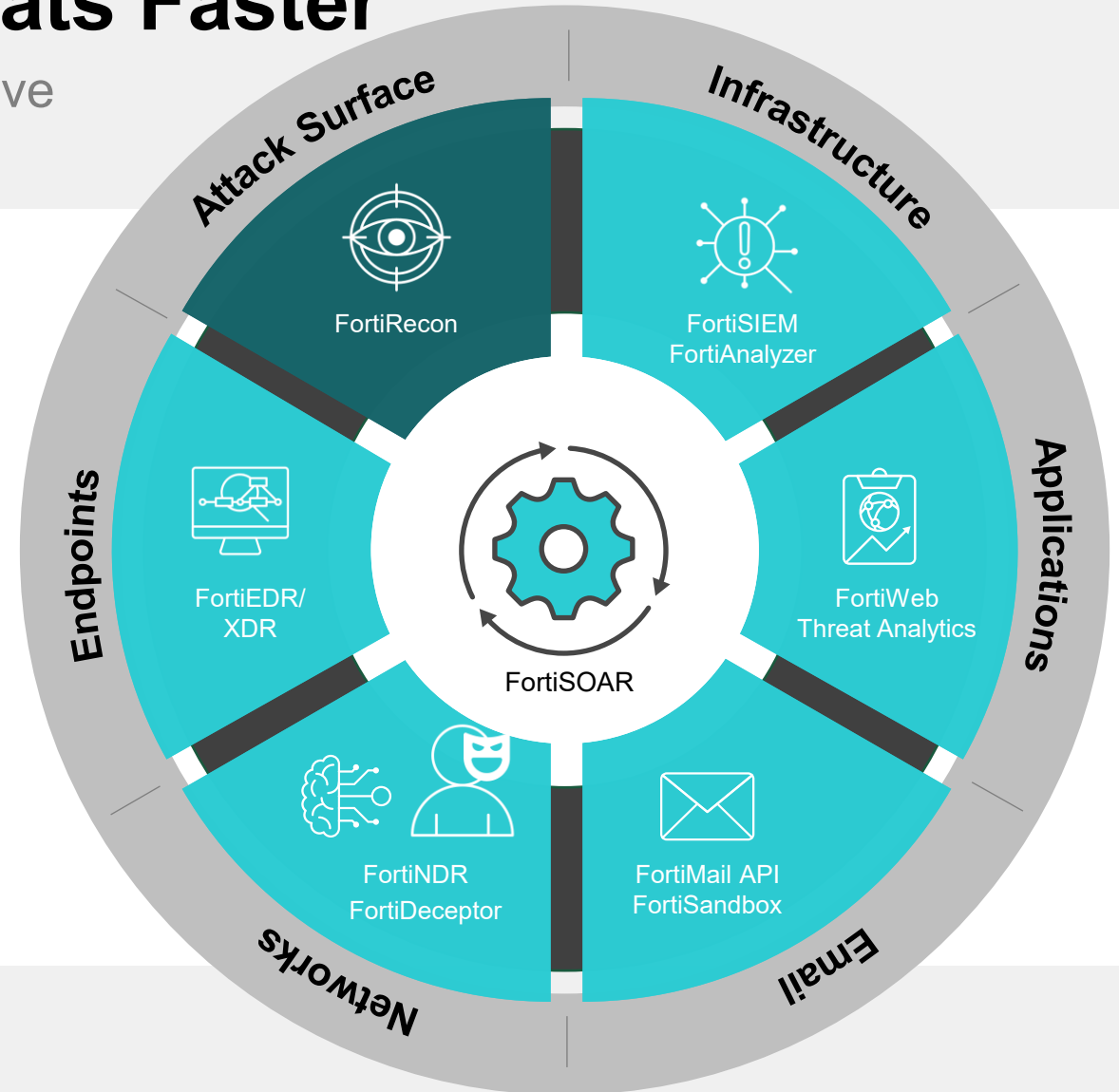
AI-Powered Security Operations Detects and Responds to Threats Faster

Alignment to NIST cybersecurity framework to improve risk management



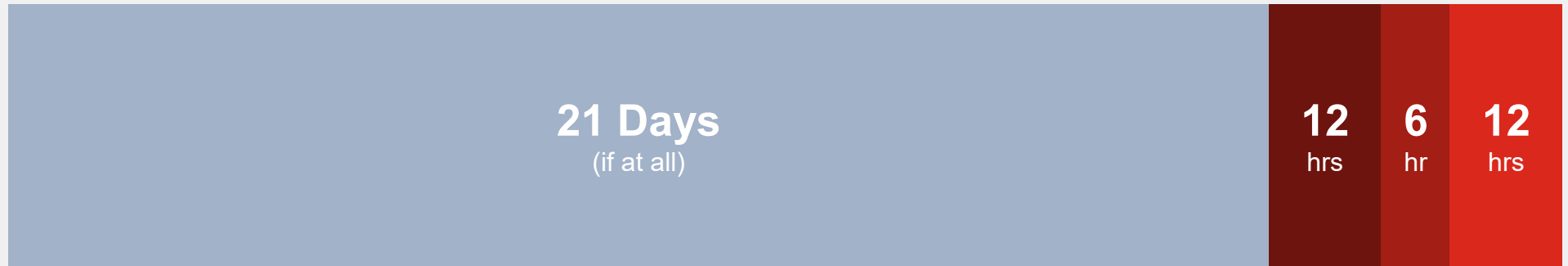
AI CYBERSECURITY TASKS

- Coordinated Alert Prioritization
- Action Planning
- Playbook creation
- Automated Detection and Response



Speed The Time to Fully Investigate and Remediate Incidents from 18.5 Hours to an Average of 10 Minutes.

Before



After

Fortinet SecOps Platform



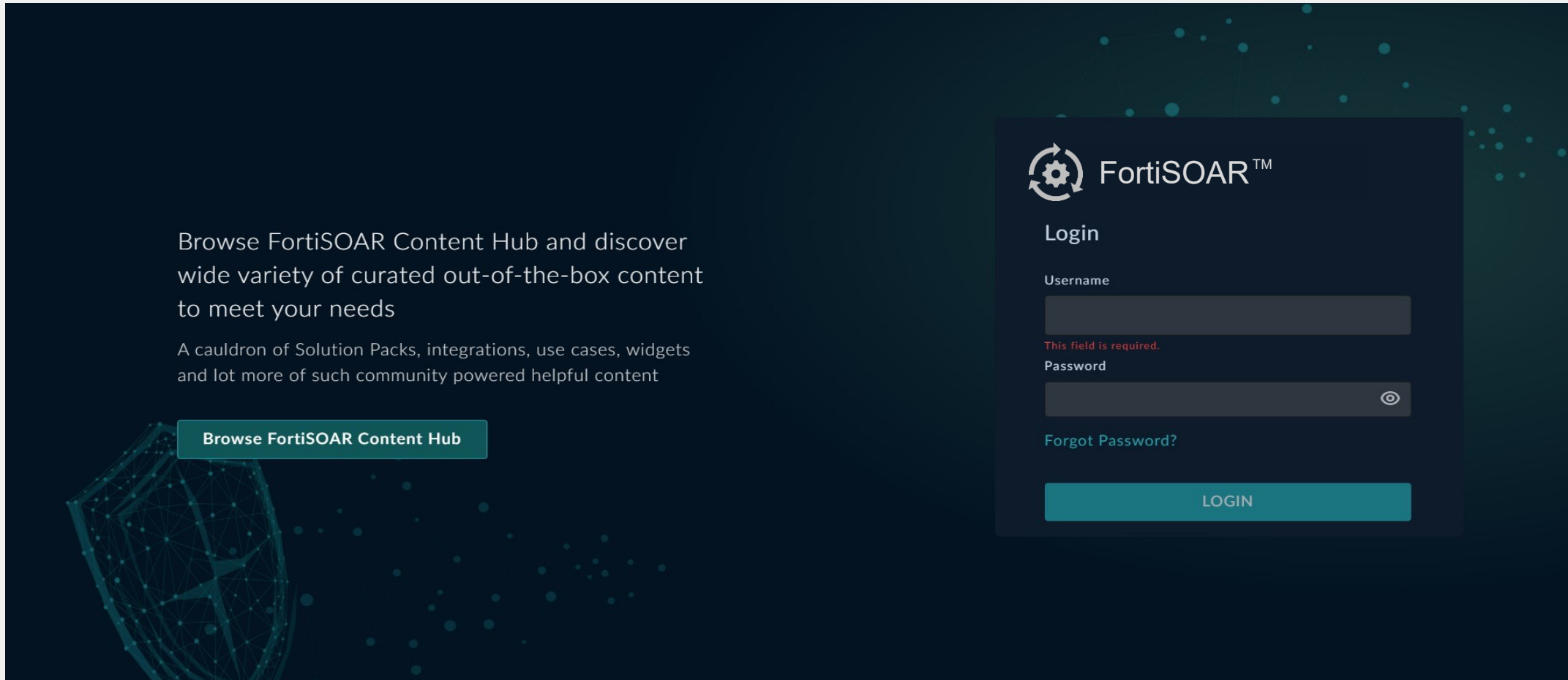
■ Time to Detect ■ Time to Contain ■ Time to Investigate ■ Time to Remediate



HOME

Supporting Cybersecurity Operations with AI

A day in the life of a Security Analyst



The image shows a dark-themed user interface for FortiSOAR. On the left, there is a section for the 'FortiSOAR Content Hub' with a button to 'Browse FortiSOAR Content Hub'. On the right, there is a 'Login' form with fields for 'Username' and 'Password', a 'Forgot Password?' link, and a 'LOGIN' button. The background features a stylized shield icon and a network diagram.

Browse FortiSOAR Content Hub and discover wide variety of curated out-of-the-box content to meet your needs

A cauldron of Solution Packs, integrations, use cases, widgets and lot more of such community powered helpful content

[Browse FortiSOAR Content Hub](#)

FortiSOAR™

Login

Username

This field is required.

Password

[Forgot Password?](#)

LOGIN



Supporting Cybersecurity Operations with AI

A day in the life of a Security Analyst

The screenshot displays the FortiSOAR Alerts interface. At the top, there's a search bar and navigation icons. Below the header, there are two tabs: "Open Alerts By Severity" and "Alerts By Type", both with refresh and dropdown icons. The "Open Alerts By Severity" tab is active, showing "Assign To: Me | All". Below the tabs, there's a section for "5 Items" with "+ Add" and "- Execute" buttons. The main area contains a table of alerts with columns for ID, Priority Weight, Severity, Assign To, Name, Source, Type, Status, Created On, Escalated, Ack SLA, and Response SLA. The table shows three alerts, all with a severity of "Low" and status of "Open".

ID	Priority Weight	Severity	Assign To	Name	Source	Type	Status	Created On	Escalated	Ack SLA	Response SLA
1	1	Low		Repeated Login Failure ...	FortiSIEM	Brute Force Atte...	Open	04/08/2023 10:...	No	Awaiting Action	Awaiting Action
2	1	Low		Repeated Login Failure ...	FortiSIEM	Brute Force Atte...	Open	04/08/2023 10:...	No	Awaiting Action	Awaiting Action
3	1	Low		Repeated Login Failure ...	FortiSIEM	Brute Force Atte...	Open	04/08/2023 10:...	No	Awaiting Action	Awaiting Action



Supporting Cybersecurity Operations with AI

A day in the life of a Security Analyst

The screenshot displays the FortiSOAR Alerts dashboard. At the top, there's a search bar and navigation icons. Below, the 'Alerts' section is active, showing 'Open Alerts By Severity' and 'Alerts By Type' filters. A table lists 5 items, with a white starburst highlighting a 'Critical' alert. The table columns include ID, Priority Weight, Severity, Assign To, Name, Source, Type, Status, Created On, Escalated, Ack SLA, and Response SLA.

ID	Priority Weight	Severity	Assign To	Name	Source	Type	Status	Created On	Escalated	Ack SLA	Response SLA
1	1	Low		Repeated Login Failure ...	FortiSIEM	Brute Force Atte...	Open	04/08/2023 10:...	No	Awaiting Action	Awaiting Action
2	1	Low		Repeated Login Failure ...	FortiSIEM	Brute Force Atte...	Open	04/08/2023 10:...	No	Awaiting Action	Awaiting Action
3	1	Low		Repeated Login Failure ...	FortiSIEM	Brute Force Atte...	Open	04/08/2023 10:...	No	Awaiting Action	Awaiting Action
4	20	Critical	CS Admin	Transfer of Malware Detected ...	FortiSIEM	Malware	Open	04/08/2023 10:...	No	Awaiting Action	Awaiting Action
5	20	Critical	CS Admin	Outbound Connection Attempt ...	FortiSIEM	Beconing	Open	04/08/2023 10:...	No	Awaiting Action	Awaiting Action



Supporting Cybersecurity Operations with AI

A day in the life of a Security Analyst

The screenshot displays the FortiSOAR interface. The top navigation bar includes the FortiSOAR logo, a search bar, and several utility icons (gear, list, notifications with a '2' badge, checkmark, another notification with a '1' badge, and a user profile). The main content area is split into two panels. The left panel shows an alert titled 'Alert-44 | Transfer of Malware Detected - Dragonfly 2.0' with a 'Critical' severity. Below the title, there are tags for 'fortisiem' and 'malware', and a '+ Add Tags' button. The alert details section includes 'SLA Details' with fields for 'Ack Due Data' (04/08/2023 02:46 PM), 'Ack Data' (04/08/2023 02:51 PM), 'Ack SLA' (Missed), 'Response Due' (04/08/2023 03:11 PM), 'Response Due' (Select Date), and 'Response S...' (Awaiting Action). The 'Description' section contains the text: 'Suspicious transfer of malware "TemplateAttack_dragonFly_2_0" (MD5: 722154a36f8ad758a7a) was detected involving resource "10.132.X.X\ADMIN\CVcontrolEngineer.docx" after a "read" operation.' Below this is a 'Fortinet FortiGuard Threat Intelligence Detection Summary' table.

Confidence	Web filter Category	IOC Category	AV Category	IOC Tag
High	None	None	Msoffice/Agent.ARP!.Tr.Didr	Dragonfly

The right panel is titled 'Workspace' and has tabs for 'Comments' and 'Recommendations'. At the bottom right of the workspace, there is a blue robot icon with white rays emanating from its head, representing an AI assistant, with a mouse cursor pointing at it.



Supporting Cybersecurity Operations with AI

A day in the life of a Security Analyst

The screenshot displays the FortiSOAR interface. On the left, a sidebar contains navigation icons. The main area shows an alert titled "Alert-44 | Transfer of Malware Detected – Dragonfly 2.0" with a "Critical" severity. Below the alert title, there are tabs for "Alert Details", "Playbooks", and "Audit Logs". The "Alert Details" tab is active, showing SLA details and a description of a suspicious malware transfer. A "Fortinet FortiGuard Threat Intelligence Detection Summary" table is also visible. On the right, an "Advisor" chat window titled "FortiSOAR AI Assistant" is open, displaying a conversation about the alert. The chat includes a greeting, a question about the alert, a detailed response with a breakdown of the incident, and a list of immediate steps to take.

Alert-44 | Transfer of Malware Detected – Dragonfly 2.0
Critical | Last Modified 04/08/2023 02:51 PM by Playbook

fortisiem X malware X + Add Tags

Alert Details Playbooks Audit Logs

SLA Details

Ack Due Data	04/08/2023 02:46 PM	Ack Data	04/08/2023 02:51 PM	Ack SLA	Missed
Response Due	04/08/2023 03:11 PM	Response Due	Select Date	Response S...	Awaiting Action

Description

Suspicious transfer of malware "TemplateAttack_dragonFly_2_0" (MD5: 722154a36f8ad758a7a) was detected involving resource "\10.132.X.X\ADMIN\CVcontrolEngineer.docx" after a "read" operation.

Fortinet FortiGuard Threat Intelligence Detection Summary

Confidence	Web filter Category	IOC Category	AV Category	IOC Tag
High	None	None	MOffice/Agent.ARP!.Tr.Didr	Dragonfly

Advisor
FortiSOAR AI Assistant

Hi there! How can I help you today?

Can you tell me more about this alert "Suspicious transfer of malware "TemplateAttack_dragonFly_2_0" (MD5: 722154a36f8ad758a7a) was detected involving resource "\10.132.X.X\ADMIN\CVcontrolEngineer.docx" after a "read" operation.

The alert describes a security incident involving a malware transfer. Here's a breakdown:

- Malware name:** TemplateAttack_DragonFly_2_0
- MD5 Hash:** 722154a36f8ad758a7a
- Resource involved:** \10.132.X.X\ADMIN\CVcontrolEngineer.docx (a network share and file)
- Operation:** Read (this file was accessed or possibly copied)
- Issue:** The alert indicates that a file, which matches the signature of a known malware 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.

Ask a question



Supporting Cybersecurity Operations with AI

A day in the life of a Security Analyst

The screenshot displays the FortiSOAR interface. The top navigation bar includes the FortiSOAR logo, a search bar, and several utility icons. The main content area is split into two panels. The left panel shows an alert titled "Alert-44 | Transfer of Malware Detected – Dragonfly 2.0" with a critical status. Below the alert title, there are tabs for "Alert Details", "Playbooks", and "Audit Logs". The "Alert Details" tab is active, showing SLA details and a description of a suspicious malware transfer. The right panel is titled "Advisor" and "FortiSOAR AI Assistant". It contains a text box with a question about the alert's relation to another alert, followed by an AI-generated response explaining the correlation between SMBv1 vulnerabilities and malware transfer. Below the response is a list of five recommended actions to respond to the alert.

FortiSOAR | Search

Alert-44 | Transfer of Malware Detected – Dragonfly 2.0
Critical Alert-44 | Transfer of Malware Detected – Dragonfly 2.0
Last Modified 04/08/2023 02:51 PM by Playbook

fortisiem X malware X + Add Tags

Alert Details | Playbooks | Audit Logs

SLA Details

Ack Due Data	04/08/2023 02:46 PM	Ack Data	04/08/2023 02:51 PM	Ack SLA	Missed
Response Due	04/08/2023 03:11 PM	Response Due	Select Date	Response S...	Awaiting Action

Description

Suspicious transfer of malware
"TemplateAttack_dragonFly_2_0" (MD5: 722154a36f8ad758a7a) was detected involving resource "10.132.X.X\ADMIN\CVcontrolEngineer.docx" after a "read" operation.

Fortinet FortiGuard Threat Intelligence Detection Summary

Confidence	Web filter Category	IOC Category	AV Category	IOC Tag
High	None	None	MSSOffice/Agent.ARP!.Tr.Didr	Dragonfly

Advisor
FortiSOAR AI Assistant

How can this be related to this alert also – "A suspicious packet sent. SMB Server Traffic contains NTLM-Authenticated SMBv1 Session. Activity was detected that indicates attempts to abuse the exploits in SMBv1"

The second alert relates to the first 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 a 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 exploit attempts.
3. Apply necessary patches to fix vulnerabilities in SMBv1 on any legacy systems using it.
4. Analyse logs to see if the detected SMBv1 activity corresponds with timing of malware transfer.
5. Continue with the incident response steps as outlined for the first alert.

Ask a question



Supporting Cybersecurity Operations with AI

A day in the life of a Security Analyst

The screenshot displays the FortiSOAR interface. At the top, the header shows 'FortiSOAR' and a search bar. A critical alert is visible: 'Alert-44 | Transfer of Malware Detected - Dragonfly 2.0', last modified on 04/08/2023 at 02:51 PM by Playbook. The alert details section shows a table with columns for 'Ack Data', 'Ack SLA', and 'Response Due'. Below this, a summary of the malware detection is provided, including the MD5 hash and the file name. A table at the bottom summarizes the detection details.

Confidence	Web filter Category	IOC Category	AV Category	IOC Tag
High	None	None	Msoffice/Agent.ARP!.Tr.Didr	Dragonfly

The FortiSOAR AI Assistant, 'FortiSOAR AI Assistant', is shown on the right side of the interface. It provides a detailed analysis of the malware actor, including the group name, origin, targets, tactics, and objectives. The assistant also offers further analysis and recommendations for sharing information with relevant security teams.

Automation menu items:

- Playbooks
- Connectors
- Data Ingestion
- Schedules
- SLA Templates

Fortinet FortiGuard Threat Intelligence Detection Summary

Group: DragonFly / Energetic Bear

Origin: Suspected to be stated sponsored with links to Russia

Targets: Primarily energy and industrial sectors, but they have been know to target other sectors as well.

Tactics: They use various cyber-espionage and sabotage tactics, including spear-phishing, watering hole attacks and exploiting vulnerabilities in industrial control systems and software.

Objective: Their main objectives typically include cyber espionage, obtaining sensitive information and disrupting industrial processes or energy supply.

Further analysis by cybersecurity experts would loikely provide more specific details on the threat actor's latest tools, techniques and procedures (TTPs). It is importante to share this information with relevant security teams and organizations involved in cyber threat intelligence for a more comprehensive response and prevention of future incidentes.

Ask a question

Supporting Cybersecurity Operations with AI

A day in the life of a Security Analyst

The screenshot displays the FortiSOAR user interface. On the left is a navigation sidebar with icons for various functions. The main area is split into two panels. The left panel, titled 'Playbooks', contains a descriptive text box and a list of triggers under the heading 'CHOOSE A TRIGGER'. The right panel, titled 'Advisor', shows a chat interface with the 'FortiSOAR AI Assistant'.

FortiSOAR

Search

Playbooks

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 users select a record and then select the playbook from the "Execute" list.
- On Create**
Triggered on the creation of records that match the specific criteria.
- On Updated**
Triggered on the updation of records that match the specific criteria.
- Referenced**
Triggered from another playbook using a "Reference Playbook" step or from a schedule.
- Custom API Endpoint**
Triggered from na API request to a custom endpoint.
- On Delete**
Triggered on the deletion of records that match the specified criteria.

Advisor

FortiSOAR AI Assistant

Hi there! How can I help you today? I can help generate [playbook Templates](#) for your common use cases. For help on best practices on asking questions that give best results, use "help" icon above.

I Have this alert - "Suspicious transfer of malware "TemplateAttack_ (...)" Can you help me to design a generic response playbook to investigate and mitigate such threats in the future.

Sure, let me build and share a playbook outline to review.

Ask a question

Supporting Cybersecurity Operations with AI

A day in the life of a Security Analyst

The screenshot displays the FortiSOAR interface. On the left is a navigation sidebar with icons for various functions. The main area is titled "Playbooks" and contains a flowchart titled "AI Generated Playbook. Needs Review". The flowchart consists of the following steps:

- Alert Triggered
- Extract Malware
- Search for ...
- Analyse Similar ...
- Get Reputation ..
- Is Malware Known
- If "No": Perform Further..
- If "Yes": Apply Known Miti..

On the right side of the interface is the "Advisor" chat window, titled "FortiSOAR AI Assistant". The chat history shows the following messages:

- AI Assistant: Hi there! How can I help you today? I can help generate [playbook Templates](#) for your common use cases. For help on best practices on asking questions that give best results, use "help" icon above.
- User: I Have this alert - "Suspicious transfer of malware "TemplateAttack_ (...)" Can you help me to design a generic response playbook to investigate and mitigate such threats in the future.
- AI Assistant: Sure, let me build and share a playbook outline to review.
- AI Assistant: Playbook template successfully generated! Please review.

At the bottom of the chat window is an input field labeled "Ask a question".



**THREAT
INTELLIGENCE
COLECTION**

**ACURATE
DETECTION
& ATTACK
ATRIBUTION**

**ACTION
PLANNING &
AUTOMATED
RESPONSE**

How does Artificial Intelligence Helps Cybersecurity Operations

**REDUCE
OPERATIONS
TOTAL COST**



FORTINET®