



FORTINET®



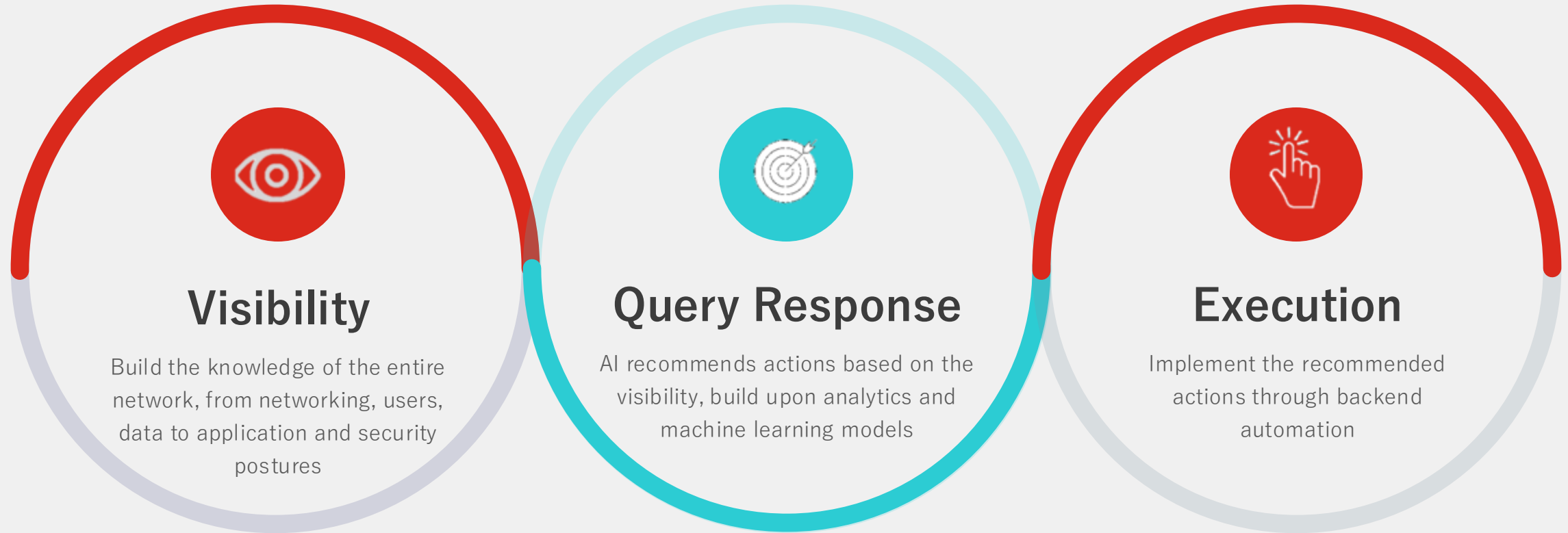
Fortinet AI:

Why work harder when you can work smarter

Joel Gooding - Systems Engineer



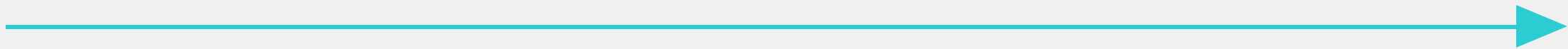
What AI within Cybersecurity can do



Fortinet Security Fabric

FSBP and Playbooks

Converged Network and Automation



Fortinet AI: Applies AI where They Fit Best

Leverage multiple AI technologies. Leverage the large threat landscape. Leverage Fortinet platform and fabric integrations



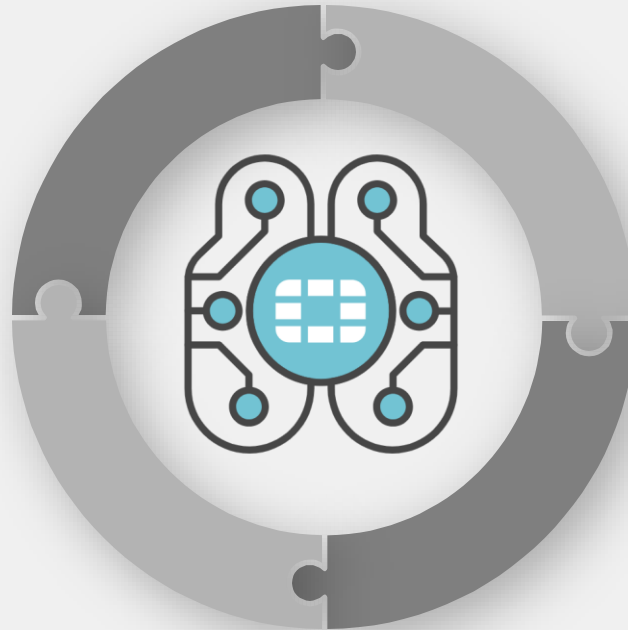
AI for Threat Detection

AI and ML to continuously train the models to improve accuracy and speed in threat detection



AI for Networking

Moving towards a self-healing network model.



AI For Data Protection

Detect and prevent data leakage when Large Language Model (LLM) deployed in cloud applications,

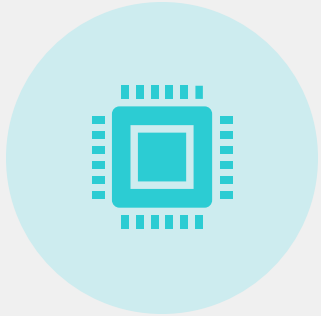


AI for NoC and SoC

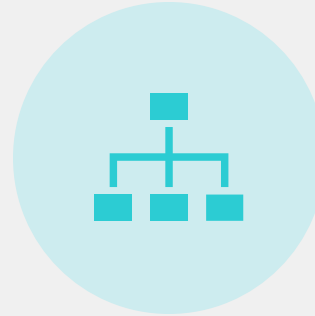
Harness network and security operation with FortiAI Advisor in FortiSIEM, FortiSOAR, FortiManager and FortiAnalyzer

GenAI Adoption in Network Operation

A transformative force in cybersecurity, with both significant potential and notable challenges



By 2025, **20%** of initial network **configurations** will utilize GenAI, up from nearly 0% in 2023.



By 2026, **60%** of network operations personnel will rely on GenAI for **Day 2 management**, up from less than 5% in early 2024.



GenAI can reduce **troubleshooting** time, **installation** time, and site visits by up to **25%**.



Network **performance and availability** improvements could enhance end-user productivity by up to **25%**.

Why GenAI for security operations?

The typical SOC suffers from



Lack of expert staffing



Over-burdened analysts



Insufficient threat investigations



Elevated risk of serious breach



GenAI technology can

- Provide analysts with immediate cybersecurity intel and best practices
- Be seamlessly embedded into SecOps product workflows
- Be tuned and curated for context-aware, accurate, and directly actionable information

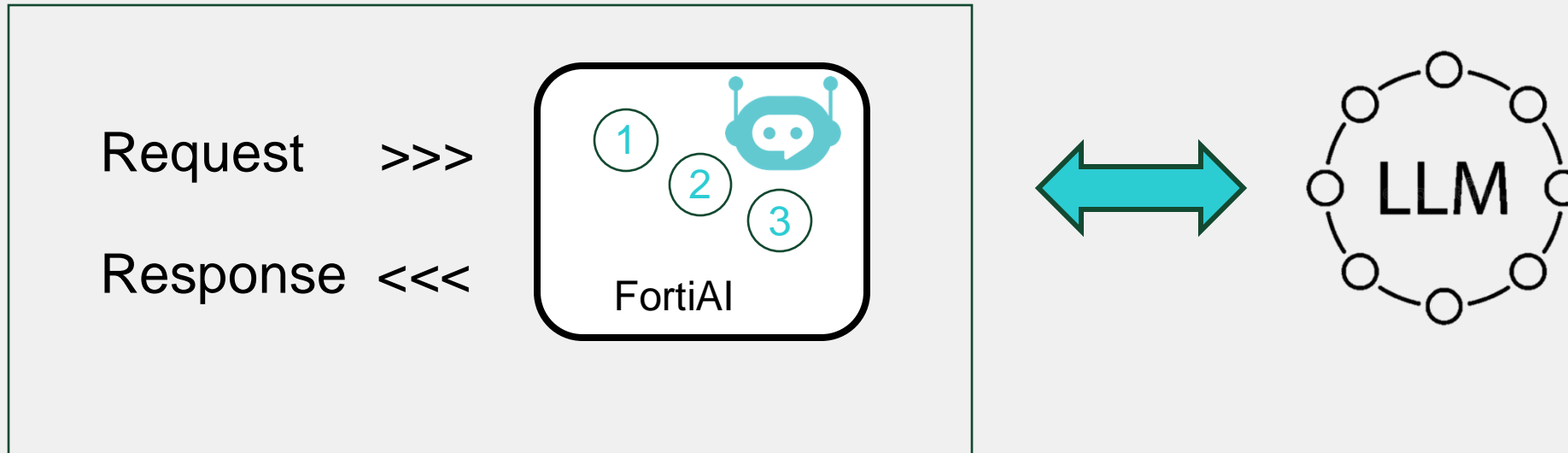


Extended GenAI will...

Guide, simplify, and automate security analyst activities

Power analysts to make optimal decisions, rapidly respond to threats, and save time on complex tasks

FortiAI – How it works..what about PRIVACY?



1 Augments GenAI Intel
Provides DB of Fortinet intel, product detail, and examples to augment the AI engine

2 Transforms Queries
Adds complete query detail needed to elicit an accurate contextual AI response

3 Shapes Responses
Builds out a complete, relevant, and actionable user response

Security & Privacy

Cloud AI engine data sharing is limited to explicit customer interaction content. Sensitive information can be automatically masked before sharing. FortiAI does not itself share or provide access to customer data.



Overview

Advisor

PREVIEW

FortiSOAR AI Assistant

Hi there! How can I help you today?

What are a few fundamental incident response suggestions to address Data Leakage resulting from "Policy Violation" -> External File Sharing?

1. Identify the Leak: Confirm the data leakage incident and identify the specific data involved.
2. Contain the Leakage: Immediately cease the unauthorized file sharing by revoking access permissions or disabling the sharing links.
3. Assess the Impact: Evaluate the sensitivity of the leaked data and determine the potential impact on the organization.
4. Notify Stakeholders: Inform relevant stakeholders, including management, legal, and affected clients, according to regulatory requirements and company policy.
5. Investigate and Remediate: Conduct a thorough investigation to understand how the policy violation occurred and implement measures to prevent future incidents, which may include enhancing technical controls, updating policies, and providing additional employee training.
6. Document: Record all actions taken for legal, regulatory, and future reference.
7. Review and Revise Policies: Analyze existing data protection and sharing policies, then amend them as necessary to strengthen security protocols and compliance.
8. Monitor: Implement ongoing monitoring to detect and prevent similar incidents in the future.

Ask a question

Type a message

Severity ...

Medium

Medium

Medium

Medium

Medium

Medium

Medium

and by Sev

Inbound insecure protocol traffic detected

Search attribute name...

Incident ID : 366
Incident Title : Inbound cleartext password usage from 222.1
Rule Name : Inbound insecure protocol traffic detected
Event Type : PH_RULE_CLEARTEXT_PWD_INBOUND
Severity Category : **Medium**
First Occurred : 1 Minute
Last Occurred : 1 Minute
Category : Security
Subcategory : Credential Access
Tactics : Credential Access
Technique : Stolen Credentials: Credentials in Files
Organization : Super
Reporting IP : FG24002913800441
Reporting IP : 192.168.1.1

Analyze this log and tell me what action to take

What blocking activities will help contain this incident?

Create a report of events per critical incident of the last 30 days

Get the latest known vulnerabilities in my environment

The **benefits** of automating AI in **cybersecurity**:



Ongoing learning



Discovering unknown
threats



Vast data volumes



Improved vulnerability
management



Enhanced overall
security posture



Better detection
and response

How can we ensure privacy? > AI Security and Privacy Training

Actively engage with employees to understand and address concerns how AI works.

Train all users on ethics, responsibility, and legal issues such as warranty, license, and copyright.

Update security awareness training to include GenAI related threats. Voice cloning and image cloning, as well as in anticipation of increased spear phishing attacks

Any adopted GenAI solutions should include training for both DevOps and cybersecurity for the deployment pipeline to ensure AI safety and security assurances.



FORTINET®