Kyberbezpečnosť s Mozgom
Ako AI (z)mení hru

Juraj Belko

Systems Engineering

SOC Maturity Modeling

In-house Operations

MATURITY

L1

Monitoring

Compliance

FortiAnalyzer

SIEM

SOCaaS

Forensics

AUTOMATION

SOC Maturity Modeling

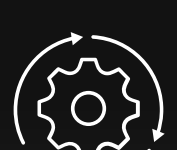
In-house Operations

MATURITY

L2

Automation

Out-of-the-box



SOAR

Sandbox

Deception

Playbook-aaS

L1

Monitoring

Compliance

FortiAnalyzer

SIEM

SOCaaS

Forensics

AUTOMATION

SOC Maturity Modeling

In-house Operations

MATURITY

L3

TDIR
End-to-end

EDR/XDR | NDR | GRC | Threat Hunting

L2

Automation
Out-of-the-box

SOAR | Sandbox | Deception | Playbook-aaS

L1

Monitoring
Compliance

FortiAnalyzer | SIEM | SOCaaS | Forensics

AUTOMATION

Pain Points

Alert Fatigue

Too many alerts & false positives - can result in being already exploited (and unaware)

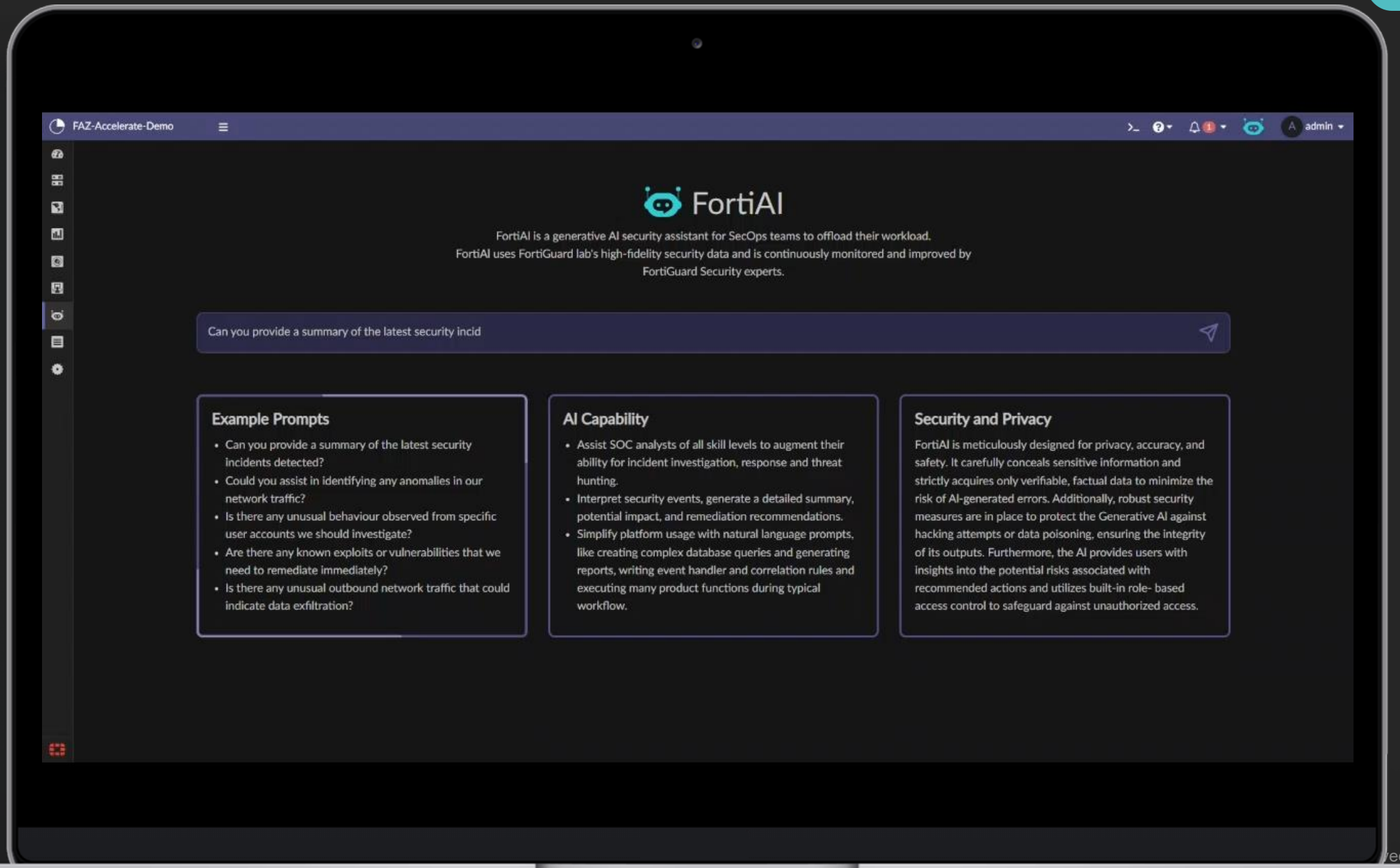
Skills Shortage

Skilled resources are scarce and tools are complex

Attack Sophistication

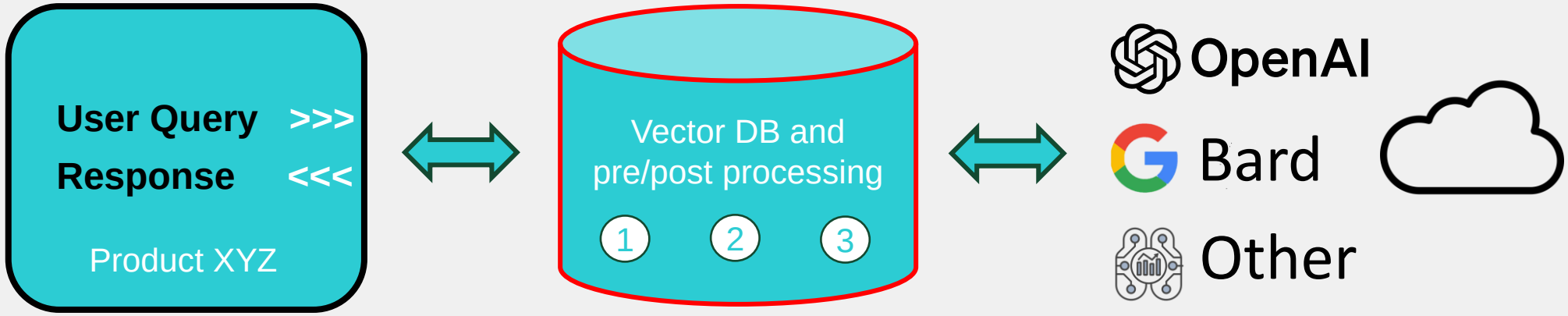
Ransomware is the biggest digital threat


LLM! LLM!
LIGHTYEAR
EVERYWHERE
eme.org


FAZ-Accelerate-Demo
admin
FortiAI
FortiAI is a generative AI security assistant for SecOps teams to offload their workload.
FortiAI uses FortiGuard lab's high-fidelity security data and is continuously monitored and improved by FortiGuard Security experts.
Can you provide a summary of the latest security incid
Example Prompts
Can you provide a summary of the latest security incidents detected?
Could you assist in identifying any anomalies in our network traffic?
Is there any unusual behaviour observed from specific user accounts we should investigate?
Are there any known exploits or vulnerabilities that we need to remediate immediately?
Is there any unusual outbound network traffic that could indicate data exfiltration?
AI Capability
Assist SOC analysts of all skill levels to augment their ability for incident investigation, response and threat hunting.
Interpret security events, generate a detailed summary, potential impact, and remediation recommendations.
Simplify platform usage with natural language prompts, like creating complex database queries and generating reports, writing event handler and correlation rules and executing many product functions during typical workflow.
Security and Privacy
FortiAI is meticulously designed for privacy, accuracy, and safety. It carefully conceals sensitive information and strictly acquires only verifiable, factual data to minimize the risk of AI-generated errors. Additionally, robust security measures are in place to protect the Generative AI against hacking attempts or data poisoning, ensuring the integrity of its outputs. Furthermore, the AI provides users with insights into the potential risks associated with recommended actions and utilizes built-in role- based access control to safeguard against unauthorized access.

Are my private date safe?

RAG (Response Augmented Generation)



1 **Augmentation**

Vendor and **security intel**, product detail, and **examples** to **augment** the **AI engine** and add **contextual accuracy**

2 **Query Transformation**

Adds complete query **detail needed** to elicit an accurate contextual AI response

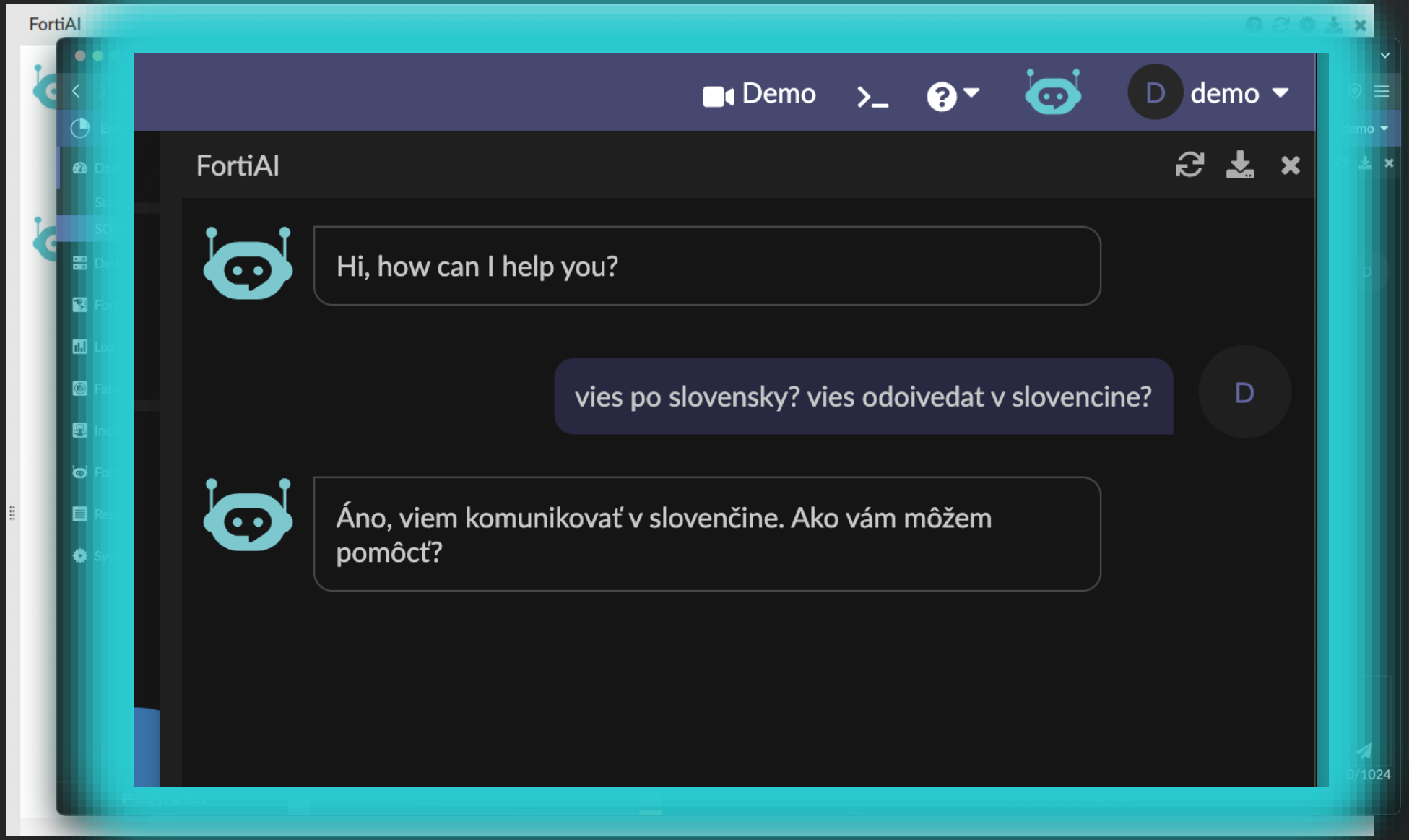
3 **Response Shaping**

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.
The assistant does not itself share or provide access to customer data.

What can you help me?




FORTINET