

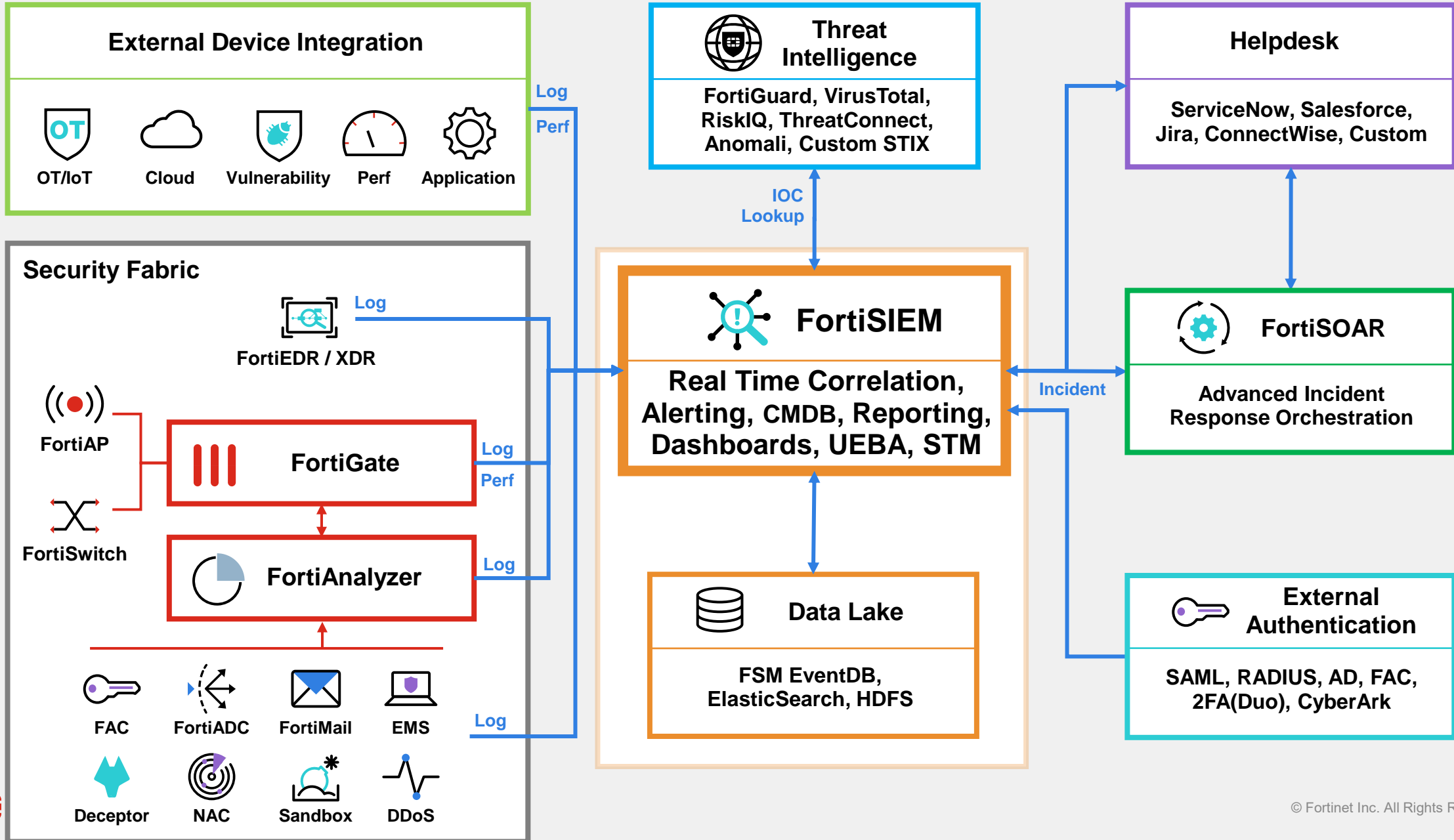


Využitie generatívnej AI v SOC nástrojoch

Systems Engineer
Juraj Belko

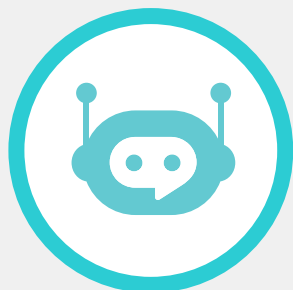


SOC - Key Integration Areas and How They Integrate



Typy užívateľov a ich reálne potreby

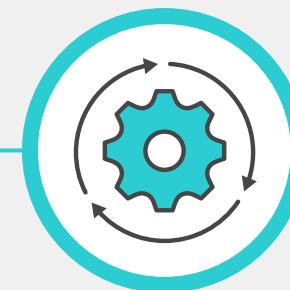
Každý typ má svoje špecifické



FortiAI

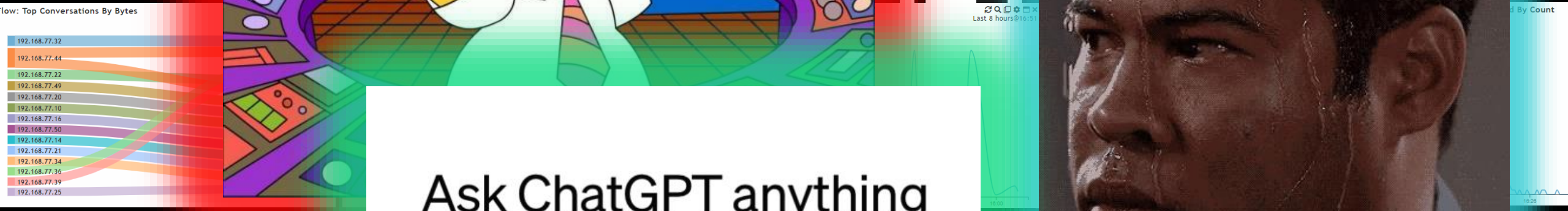
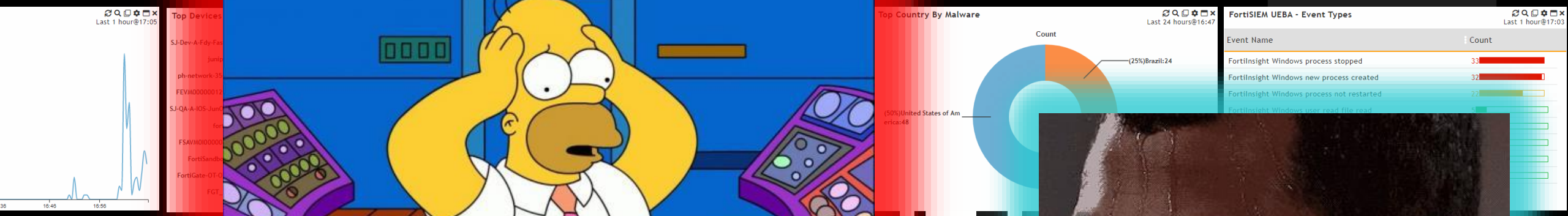
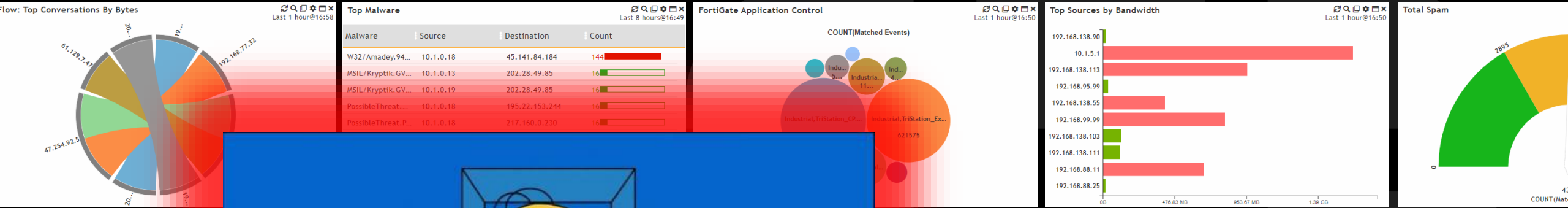
- Ešte n
- Proakt
- Po inc
- Po auc
- Zohľac

SECURITY MANAGERS BE LIKE



FortiSOAR

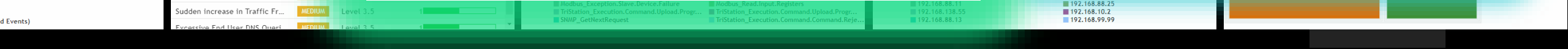
rýchlo



Ask ChatGPT anything

Redigez une note de remerciement

Recommend an easy potluck dish





FortiAI is a generative AI security assistant for FortiAnalyzer to help you troubleshoot high-fidelity security data and to continuously enhance security reports.

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 behavior 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

- Analyze SOC analysts' chat prompts to suggest prompts for incident investigation, response and the testing.
- Interpret security events, generate a detailed and potential impact, and remediation recommendations.
- Simplify platform usage with natural language and the creating complex dashboard queries and generate reports, writing event handler and correlation rule including more granular functions being applied workflow.

FortiAI



Hi, how can I help you?

I was reported with the incident that with a very large data transaction. Could you please check which incident is about that?



The incident reported with "very large data transaction" has been found. Here are the details:

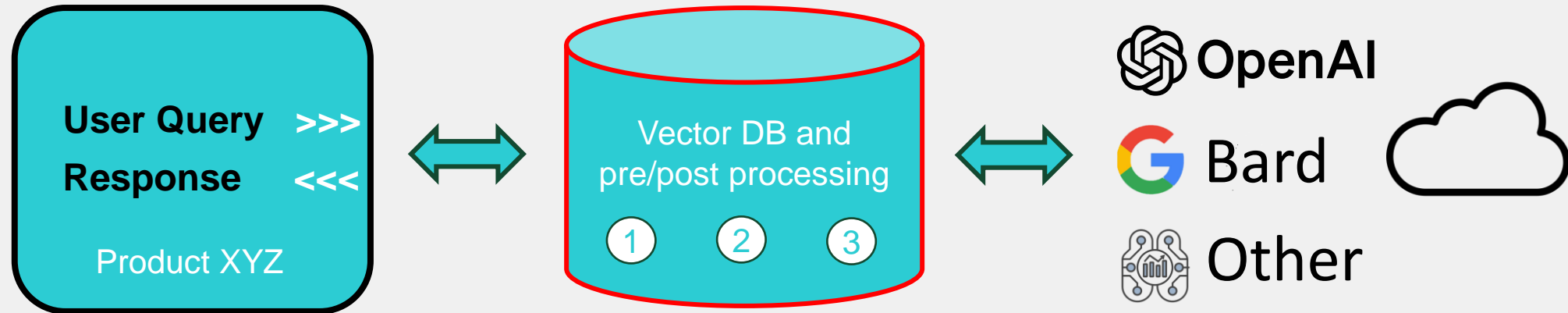
- **Incident ID:** IN00000003
- **Endpoint:** 192.168.50.20 (mail.vsb-ocommunitysde.club)
- **Category:** Scans / Probes / Attempted Access
- **Severity:** High
- **Status:** Draft
- **Description:** Large data transaction, please investigate!
- **Reporter:** Admin
- **Create Time:** 2024-03-22 09:00

Ask a question or request to start analyzing cybersecurity data from FortiAnalyzer



Are my private data safe?

RAG (Response Augmented Generation)



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

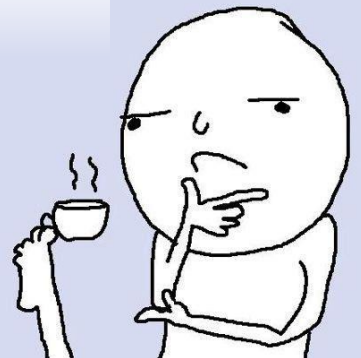
2 **Query Transformation**
Adds complete query **detail needed** to elicit an accurate contextual AI response

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.



Top Questions

Generate Alert Summary

Automatically generate a concise summary using AI for quick insights and response.

Generate Response Recommendations

Retrieve tailored response recommendations based on the alert details to guide effective incident resolution.

Generate Investigation Report

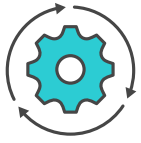
Automatically compile an investigation report summarizing actions taken and finding related to the alert.

MITRE ATT&CK Insights

Gain actionable insights into the alert's Tactics, Technique, & potential threat actor behaviours through the lens of MITRE...

Type a message





Beyond The Fabric Story

Enabling Seamless Investigation Experience and Detection To Response Story



A large collection of partner logos is displayed in a grid-like fashion. The logos include: elastic, ANOMALI, Symantec, McAfee, MySQL, LogRhythm, CISCO, paloalto NETWORKS, Radar, RSA, ArcSight, CYLANCE, amazon web services, {REST API}, IMAP, Microsoft Active Directory, Carbon Black, SentinelOne, Check Point, FORTINET, PHISHME, PostgreSQL, f5, IBM, splunk, tenable, Nessus, Tor, JIRA, QUALYS, servicenow, cuckoo, slack, Microsoft, virus total, Microsoft System Center Operations Manager, Exchange, NETWITNESS, REVERSING LABS, have i been pwned, MISP Threat Sharing, THREATQ, Twitter, and HYBRID.

