

AI SOC konzultant

rychleji, kvalitněji, levněji

Tomáš Hlavsa

12. 5. 2025

AtoS EVIDEN

SIEM.....jasně, každý ho má.....no joALE

- Dnešní SIEM - SOC koncepty spoléhají převážně na **ruční analýzu** detekovaných incidentů
- Což je **časově náročný** a na lidskou chybu náchylný přístup
- Skutečnou výzvou je **prioritizace incidentů** se zaměřením na false positives.
- **Reálné hrozby** mohou být přehlédnuty, nebo jejich analýza zpožděna díky této neefektivitě
- Přičemž díky lidskému faktoru zůstává nevyužita **existující Knowledge base** historických incident či postupů, které již vůči danému incident již byly uplatněny



Když do toho vstoupí AI

AI SOC Consultant:

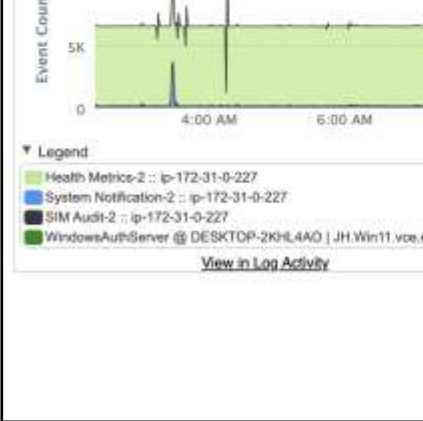
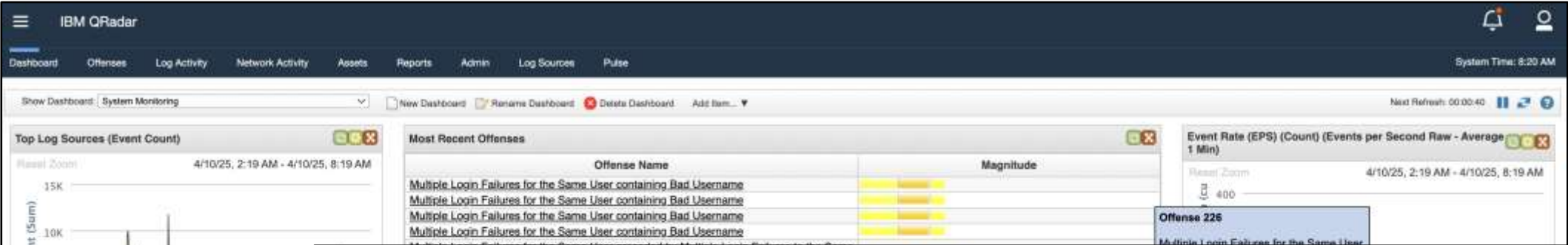
- Vyvinut v Atos/Eviden ČR
- Běží lokálně s využitím **cloud-based** LLM modelů.
- Napojení na SIEM API kdy **extrahuje offenses**.
- Obsahuje **kontrolní mechanismy** předcházející výstupům “mimo context” Aby si AI nevymýšlelo 😊

AI workflow (AI Pipeline):

- Framework automatizující workflow s použitím AI
- Umožňuje spouštění vícečetných AI demonů s různými sadami API připojení a různých knowledge base
- Používá přístup “**agentic AI**”



Standardní přístup



IBM QRadar

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Admin

Log Sources

Pulse

System Time: 8:20 AM

Offenses

My Offenses

All Offenses

By Category

By Source IP

By Destination IP

By Network

Rules

All Offenses > Offense 204 (Summary)

Offense 204

Summary

Display

Events

Flows

Actions

Print

Magnitude		Status	Relevance	0	Severity	5	Credibility	3
Description	Multiple Login Failures from the Same Source containing Bad Username	Offense Type	Source IP					
Source IP(s)	101.126.18.31	Event/Flow count	19 events and 0 flows in 3 categories					
Destination IP(s)	172.31.8.37	Start	Mar 22, 2025, 9:53:43 AM					
Network(s)	Net-10-172-192-Net 172.16.0.0	Duration	2d 14h 11m 55s					
		Assigned to	Unassigned					

Offense Source Summary

IP	101.126.18.31	Location	China
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	2	Events/Flows	41

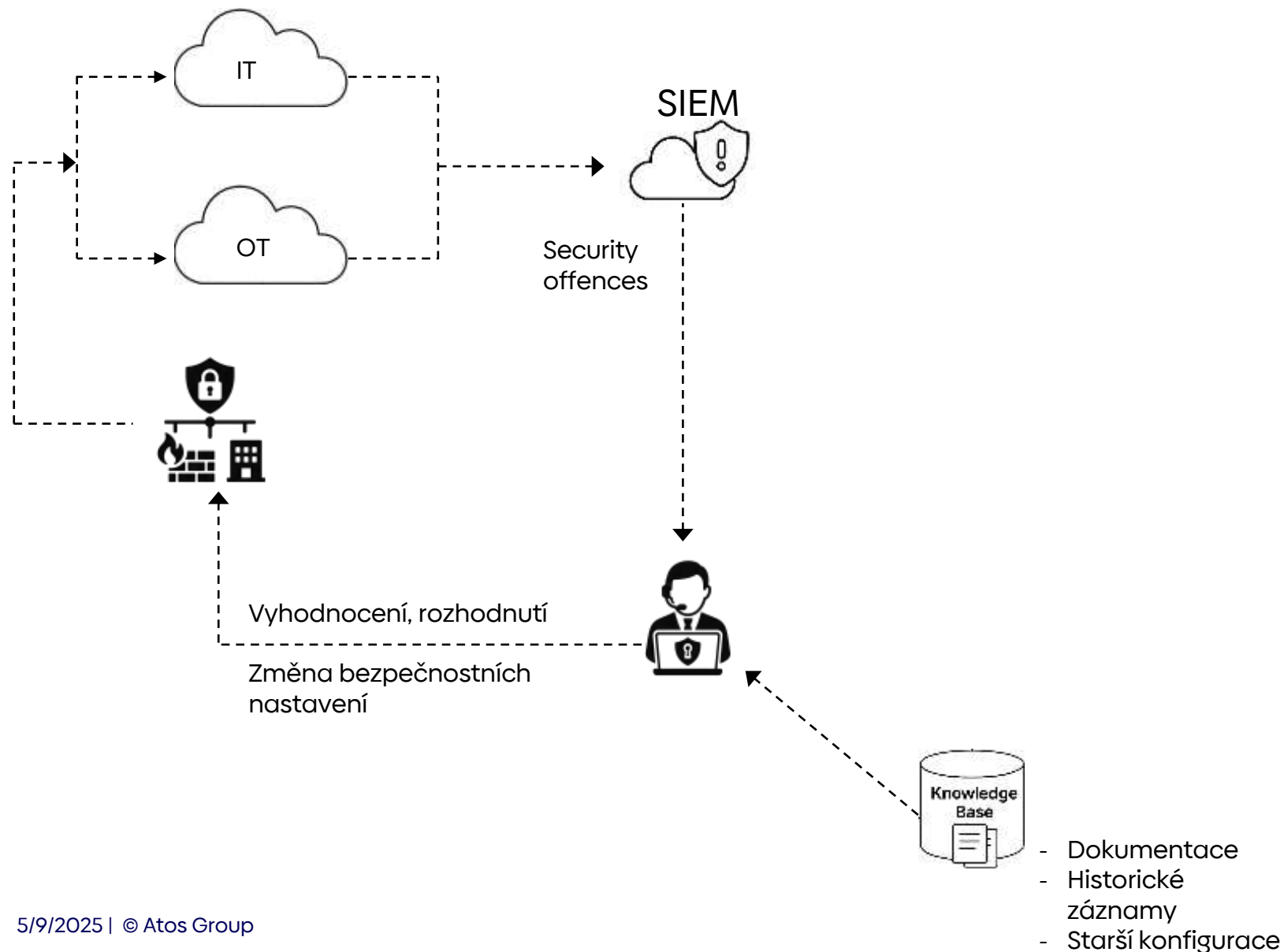
Last 5 Notes

Notes	Username	Creation Date
No results were returned.		

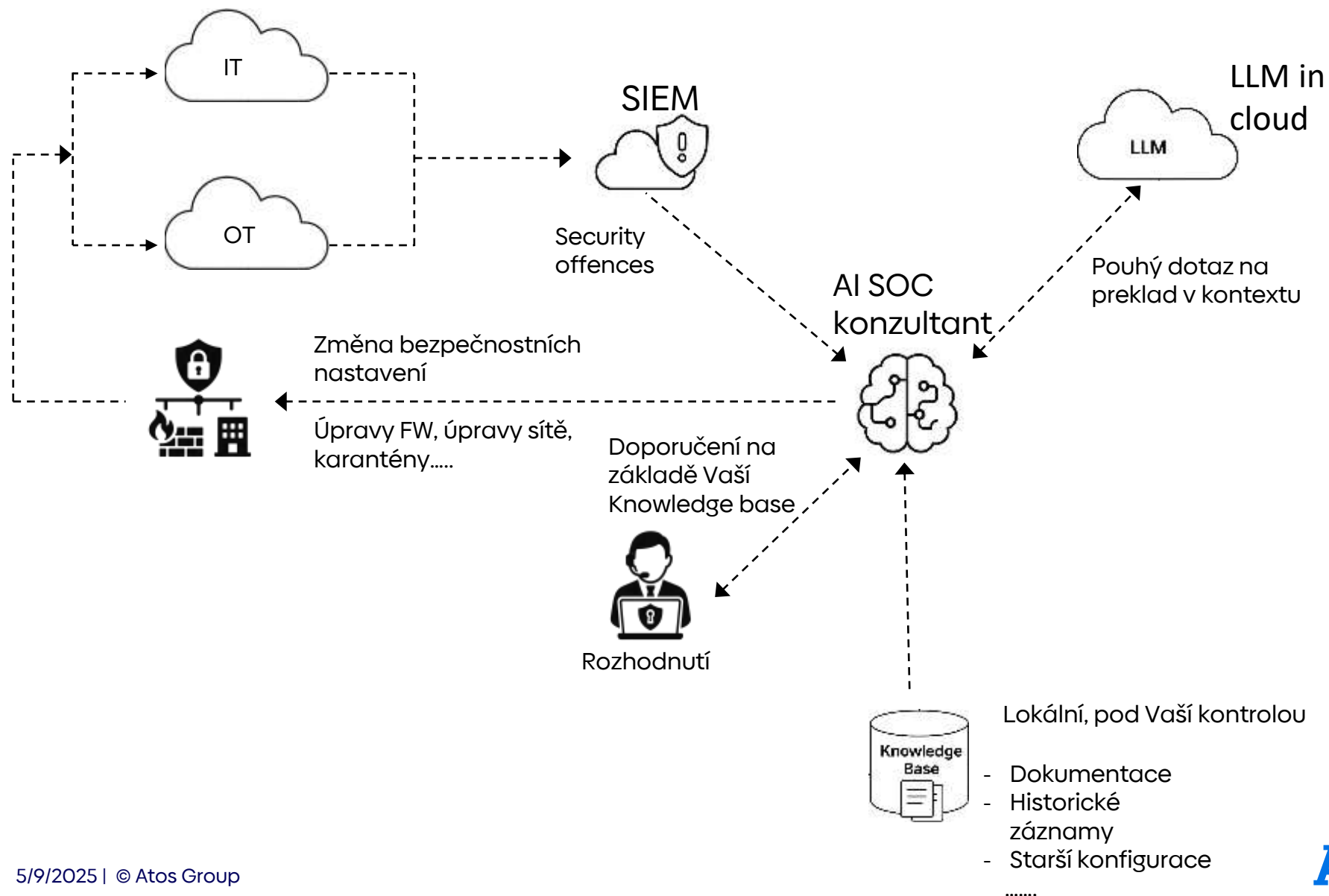
Last 5 Search Results

Magnitude	Started On	Ended On	Duration	Events/Flows
-----------	------------	----------	----------	--------------

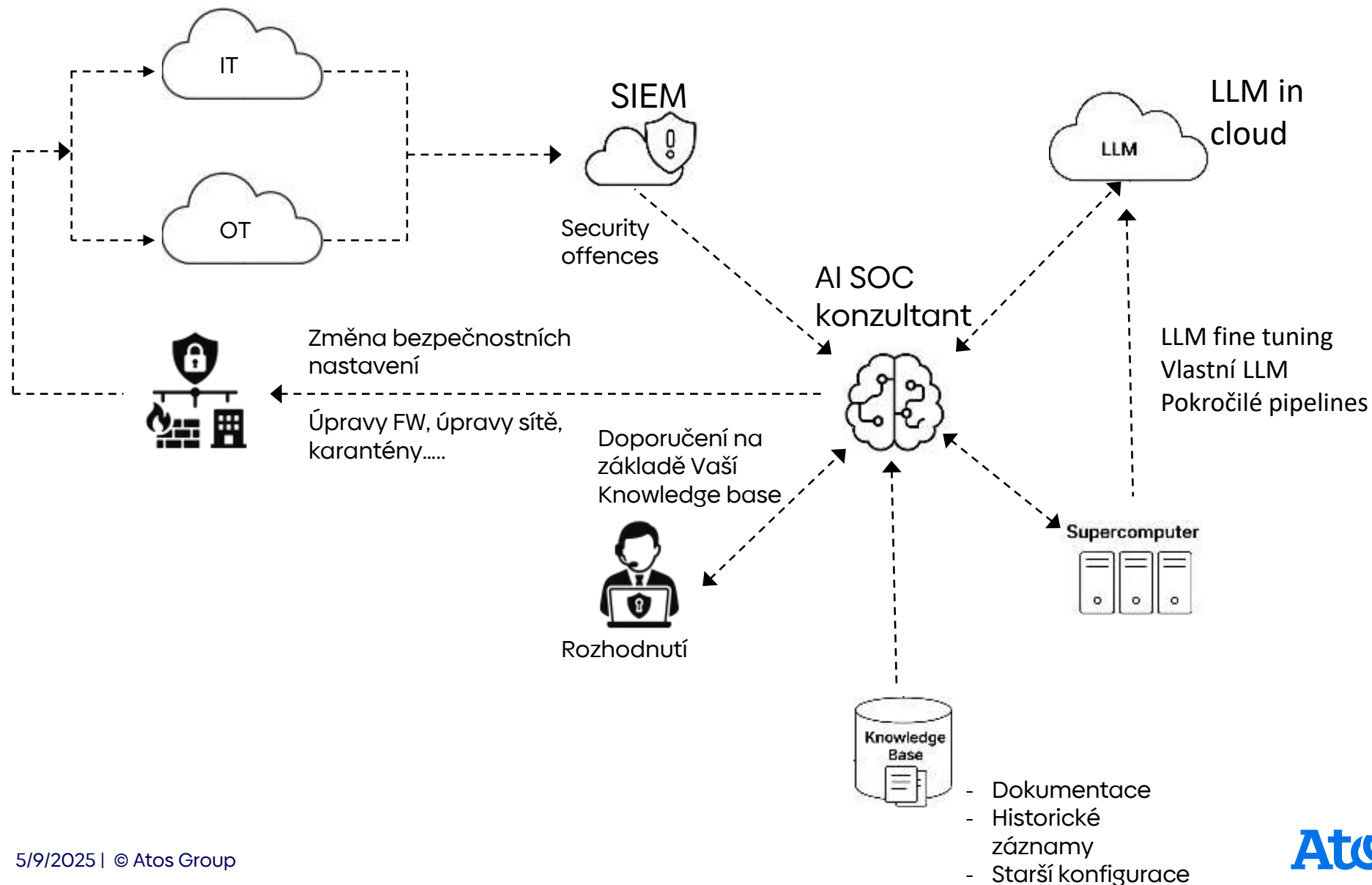
Jak AI SOC konsultant reálně pomáhá



Jak AI SOC konzultant reálně pomáhá



A když přidáte vysoký výpočetní výkon?

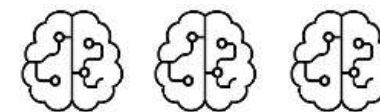
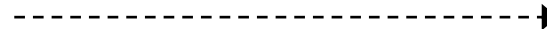


Využití expertů se mění

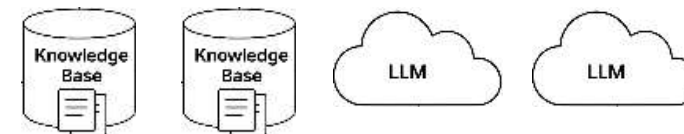
Dnešní SOC jsou proškolení, motivovaní lidé se zájmem o bezpečnostní problematiku



Budoucí SOC bude vyžadovat znalost a odpovědnost pro rozhodování + expertizu k ladění AI / LLM / RAG



AI assistants



Změna -> Výzva -> nikoliv Hrozba

Dopady použití AI pro podporu rozhodování

Preference využití lokální knowledge base
(aby si AI nevymýšlelo)

Automatizace bezpečnostních zásahů
(rychlost, nevznikají zpoždění)

Kontinuita činností, analytici si nemusejí
složitě předávat případy

Rozvoj AI je motivací pro zaměstnance,
kteří chtějí věci zlepšovat

AI doplňuje chybějící experty

LIVE DEMO

```
mimic@Tomass-MacBook-Air-3 ~ % cd Desktop
mimic@Tomass-MacBook-Air-3 Desktop % sudo ssh ubuntu@3.71.94.233 -i Tomas-Hlavsa-SOC_ed.pem
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1027-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Fri May 2 15:19:27 UTC 2025

System load:  0.07          Processes:      108
Usage of /:   23.7% of 18.3GB Users logged in:    0
Memory usage: 38%          IPv4 address for enX0: 172.31.8.252
Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

21 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri May 2 15:16:32 2025 from 89.190.87.250
ubuntu@ip-172-31-8-252:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
DROP all -- 103.130.157.74 anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
ubuntu@ip-172-31-8-252:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
DROP all -- 103.130.157.74 anywhere
DROP all -- 103.130.157.74 anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
ubuntu@ip-172-31-8-252:~$
```

Hot Secure https://3.71.94.233

AI Docs Consultant IPv6: 17

- Offense Source: 223.130.11.165
- Status: OPEN

6. Incident ID: 229

- Severity: 6
- Description: Multiple Login Failures to the Same Destination preceded by Multiple Login Failures from the Same Source containing Bad Username.
- Categories: SSH Login Failed, Remote Access Login Failed, Misc Login Failed
- Event Count: 28
- Offense Source: 223.76.99.246
- Status: OPEN

7. Incident ID: 228

- Severity: 6
- Description: Multiple Login Failures to the Same Destination preceded by Multiple Login Failures from the Same Source containing Bad Username.
- Categories: SSH Login Failed, Remote Access Login Failed, Misc Login Failed
- Event Count: 34
- Offense Source: 185.129.119.21
- Status: OPEN

8. Incident ID: 219

- Severity: 6
- Description: Multiple Login Failures to the Same Destination preceded by Multiple Login Failures from the Same Source containing Bad Username.
- Categories: SSH Login Failed, Remote Access Login Failed, Misc Login Failed
- Event Count: 31
- Offense Source: 223.76.99.246
- Status: OPEN

These incidents indicate repeated login failures, which could signify potential unauthorized access attempts. If you need further details or actions regarding any of these incidents, please let me know!

block source IP 103.130.157.74

The source IP 103.130.157.74 has been successfully blocked. Please remember to monitor the network for any further unusual traffic patterns and consider investigating any internal hosts that may have interacted with this IP.

Otázky?

+420 604 290 196
tomas.hlavska@eviden.com

Atos EVIDEN