Prediktivní bezpečnost s využitím AI

Tomáš Hlavsa

13. 5. 2025

Atos EVIDEN

Proč je prediktivní bezpečnost stále podceňována?

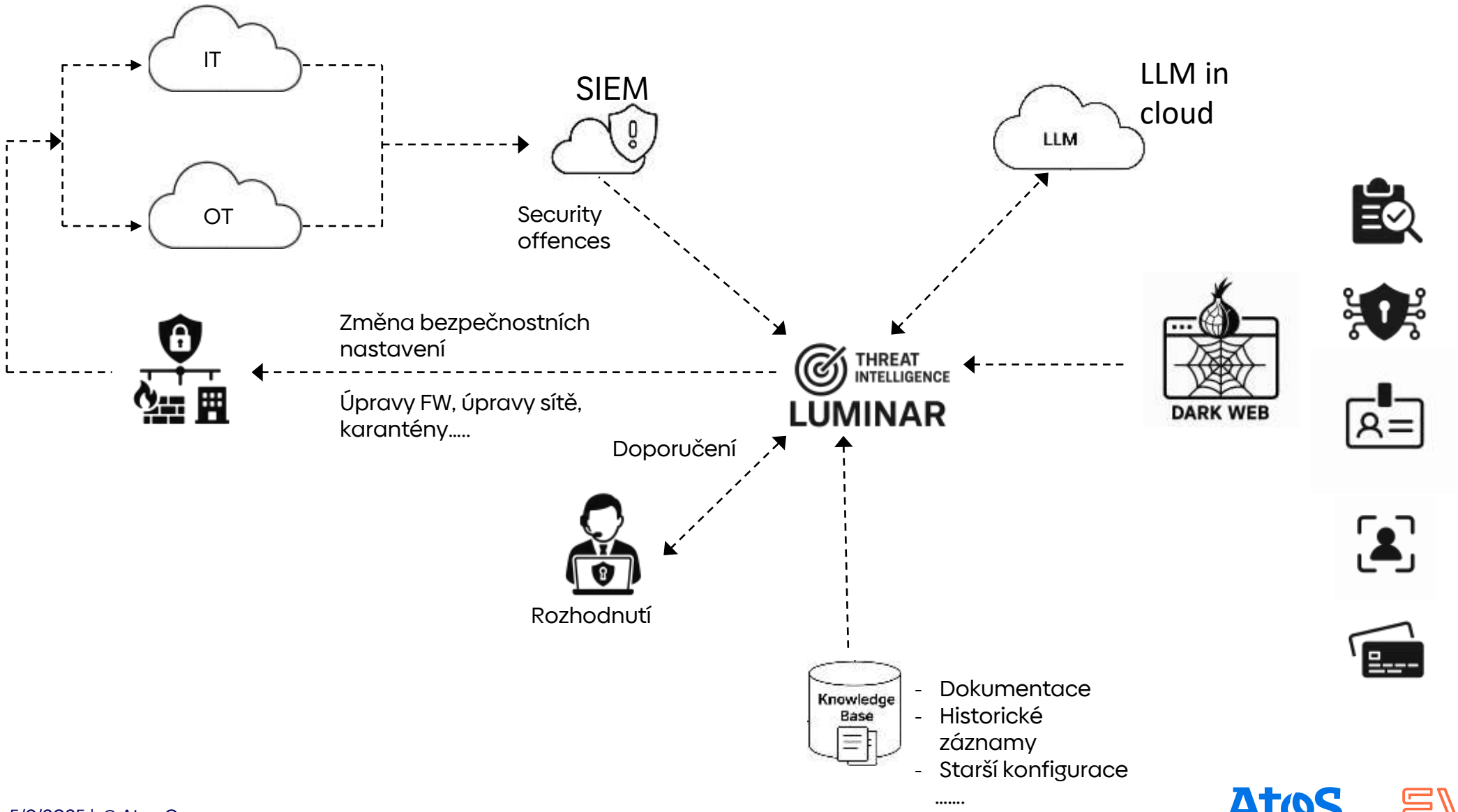
- **Reaktivní přístup stále převládá -** Firmy často řeší bezpečnostní incidenty až po jejich vzniku, místo aby jim předcházely.

- **Nedostatečné využití dat z minulých incidentů -** Organizace často nesbírají nebo neanalyzují bezpečnostní data, která by mohla pomoci **předvídat** budoucí útoky.

- **Slabá kybernetická hygiena a školení zaměstnanců -** Lidé zůstávají nejslabším článkem = chybí prevence na úrovni uživatelů.

- **Přesvědčení, že “nás se to netýká”**
  Mylný pocit bezpečí vede k tomu, že firmy zanedbávají proaktivní přístup.

Jak AI reálně pomáhá s výkonem bezpečnosti



Potřebujeme Cyber Threat Intelligence AI?

- **Proaktivní platforma pro kybernetickou Threat Intelligence (CTI)**, která pomáhá odhalit hrozby dříve, než zasáhnou vaši organizaci.
- Nabízí **globální přehled o hrozbách**, nejen monitoring v rámci vlastní sítě – sleduje útoky odkudkoli na světě.
- Posiluje **kybernetickou odolnost organizace** tím, že odhaluje i dosud neznámé hrozby.
- Pomáhá zjistit, **kdo útočí, jaké nástroje používá a co plánuje**, což umožňuje přesnější a včasnější reakci.

ale především

Integrovaný AI konzultant může detekované, či předvídané hrozbě zamezit **dříve než se začne dít**

Personalizovaný monitoring a sběr informací

Prioritní monitorované požadavky definované v plánu.

- Domény
- VIPs
- IT Infrastruktura

Cílený sběr s rozsáhlým pokrytím ze všech vrstev webu

- Komeční zdroje
- Proprietární zdroje
- Online platformy

Generování kontextualizovaných nálezů

- Obohacení monitorovacích plánů
- Korelace
- Vizualizace
- Analýza

Modulární přístup

Moduly

- Attack surface management
- Threat actor analysis
- Compromised credentials
- Vulnerability intelligence
- Credit card fraud mitigation
- Investigative portal

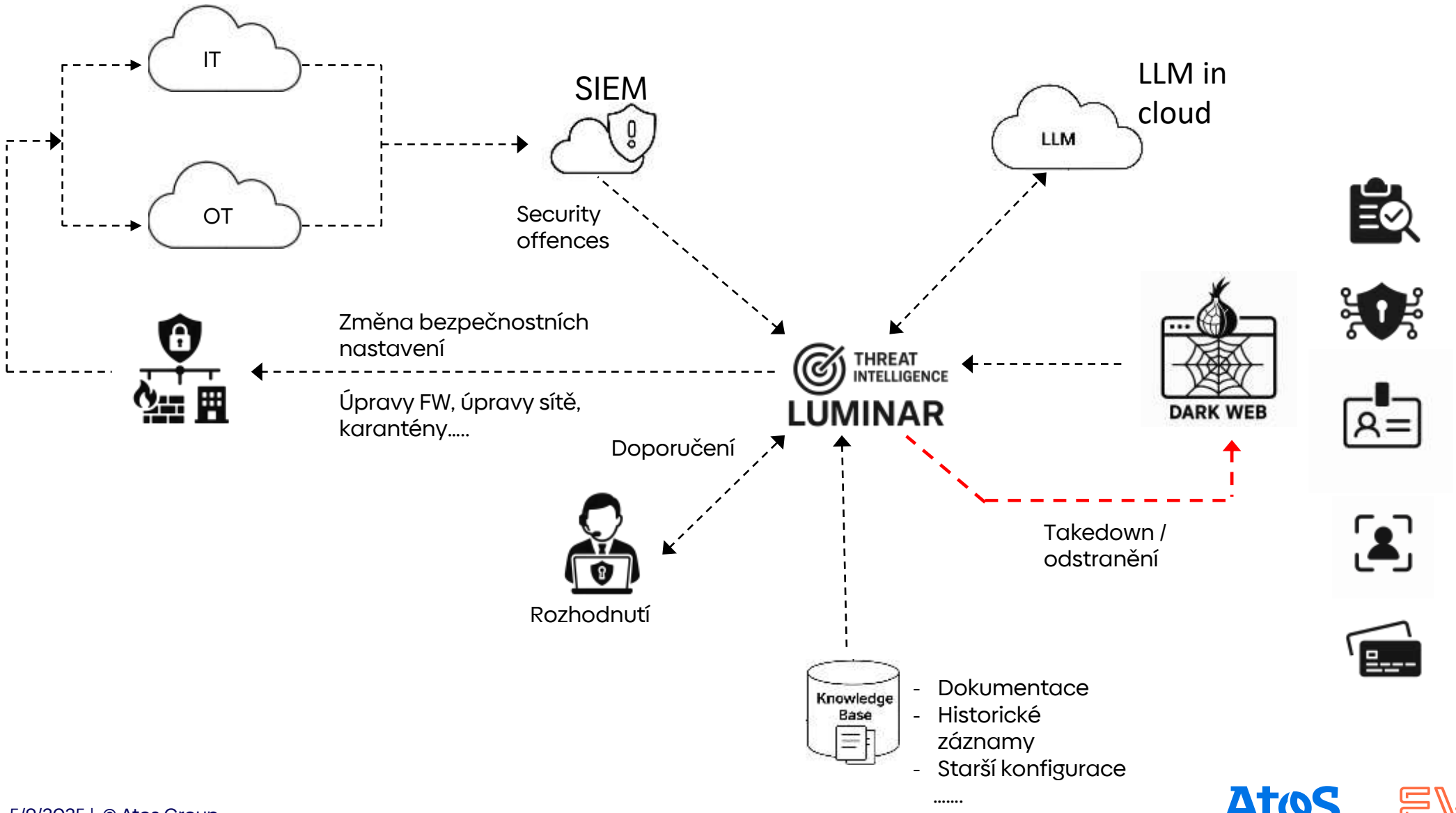
Funkce

- Executive dashboards
- Customer threat data leak
- Automated reporting
- Early warnings

S čím reálně Threat Intelligence AI pomáhá?

- **Podezření na únik dat** - například sledováním darknetu, fór nebo infikovaných systémů, kde se mohou objevit odcizené informace.
- **Nedostatek odborníků** - Naši analytici vykompenzují nedostatek bezpečnostních specialistů – poskytují přehledy, analýzy a doporučení, které urychlují rozhodování.
- **Kritičnost zranitelností** - Nástroje threat intelligence pomáhají vyhodnocovat aktuální zranitelnosti
- **Možnost Takedown**

Takedown?



Otázky?

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

Atos EVIDEN