Detekce kybernetických útoků se Splunk SIEM

Rok Informatiky 2024

13.06.2024, Telč

splunk>

ALEF

cisco Partner

Hello

Jan Hrubý
Splunk Business Unit Manager

Lukáš Mečíř
Splunk SIEM/Security Expert

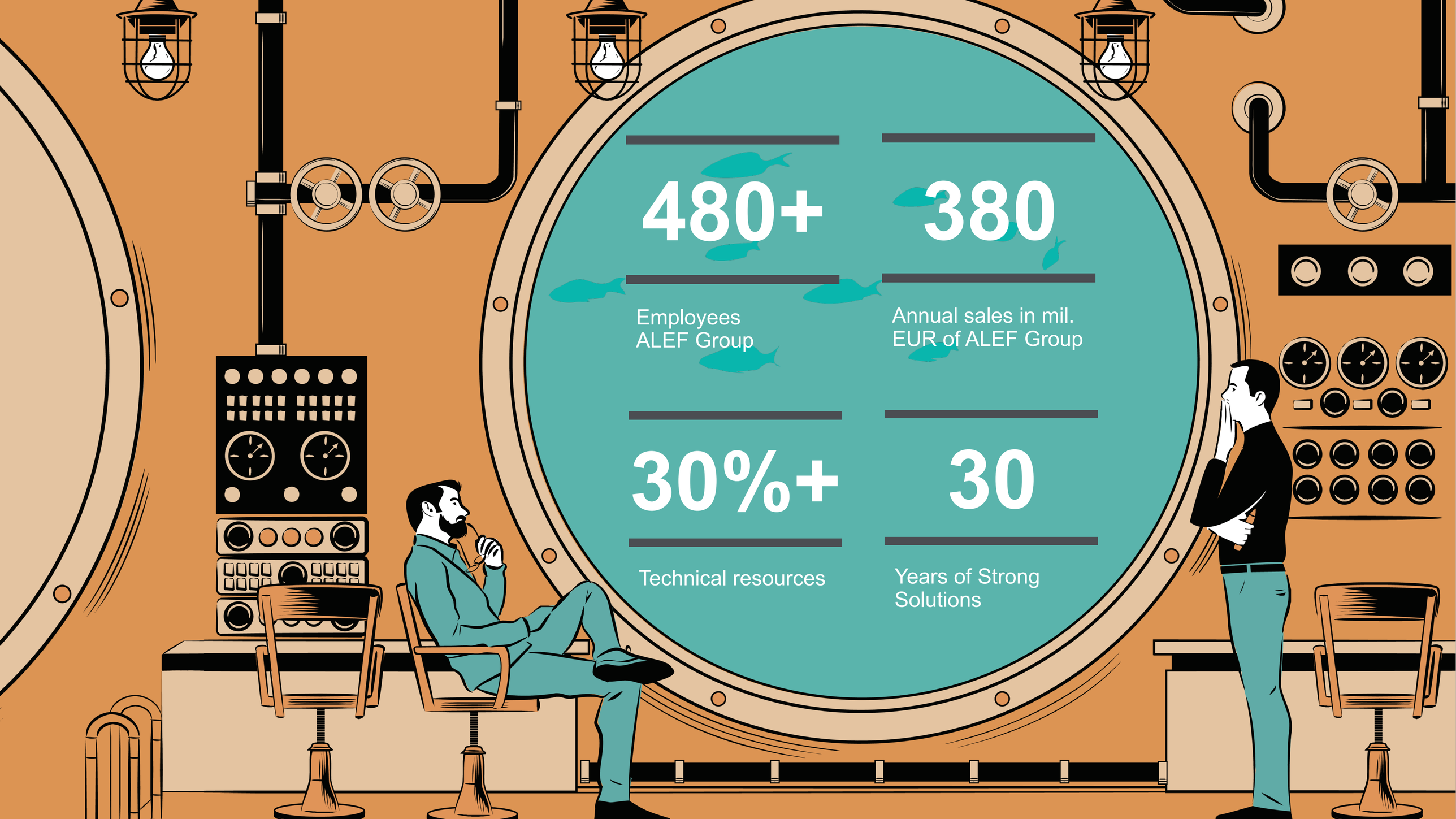
splunk> ACCREDITED — Splunk Accredited Sales Rep I

splunk> CERTIFIED — Splunk Enterprise Security Certified Admin

splunk> CERTIFIED — Splunk Enterprise Certified Admin

splunk> CERTIFIED — Splunk Enterprise Certified Architect

splunk> Partnerverse SELL ELITE


480+
Employees
ALEF Group
380
Annual sales in mil.
EUR of ALEF Group
30%+
Technical resources
30
Years of Strong
Solutions

Splunk & Cisco

…co přináší toto spojení zákazníkům?

Lepší ochrana proti kybernetickým hrozbám.
Lepší observabilita.
Lepší síťová bezpečnost.
Pokročilejší využití AI.
Lepší ceny.

Co to je?


15%
business critical data
25% zastaralá data
60%
Dark Data
splunk>
Sběr, analýza a vizualizace dat v reálném čase
https://thinkleaf.net/blog

Pro koho to je?

Naši klienti

Česká Spořitelna

Finanční instituce

Produkty:

- Splunk Enterprise
- Splunk Enterprise Security

Use Cases:

- Security
- IT

Klíčové výzvy

Zvýšení odolnosti celého systému tak, aby uměl čelit moderním výzvám. Obrovské množství různých technologií. Různá oddělení, různé potřeby informací. Nedostatek kapacit v rámci SOC týmu. Cílem bylo celý provoz zefektivnit.

Klíčové výsledky:

- Zvýšení odolnosti
- Konsolidace nástrojů
- V tuto chvíli je v plánu další rozvoj směrem ke snížení false positives prostřednictvím RBA (Risk Based Alerting) a automatizace (SOAR)
- Další rozvoj mimo securitu (směrem do byznys analýzy – chování zákazníků, nabídky na míru; compliance AML atd.)

Technická univerzita v Košiciach

Produkty:

- Splunk Enterprise
- Splunk Enterprise Security

Use Cases:

- Security
- IT

Klíčové výzvy

Cílem projektu bylo zvýšit úroveň kybernetické bezpečnosti v IT infrastruktuře Technické univerzity v Košicích. K dosažení tohoto cíle bylo použito nasazení systému SIEM (Security Information and Event Management). Byl vybrán SIEM Splunk jako systém, který se dlouhodobě umisťuje na nejvyšších příčkách v hodnocení SIEM systémů (Gartner Magic Quadrant).

Klíčové výsledky:

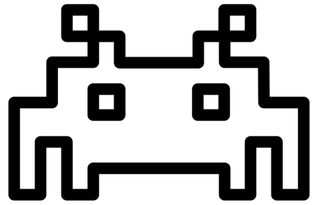
- Zvýšení odolnosti
- Konsolidace nástrojů

Proč Splunk SIEM?

Výzvy SOC týmů

Je těžké najít relevantní informace ve velkém množství dat

Pracovníkům SOCu chybí kontext při vyšetřování událostí



I díky AI se hrozby vyvíjí velice rychle

Dopady těchto výzev

3+

hodiny průměrně strávené analytiky při vyšetřováních altertu

41%

alertů je ignorováno, protože analytici nemají dostatečnou kapacitu nebo správný kontext pro jejich vyšetřování

25+

SOC typicky využívá více než 25 různých bezpečnostních nástrojů, z nichž každý vykonává různé činnosti v rámci detekce, vyšetřování a reakce

[1] - Splunk State of Security Report;

NIS2 požadavky

- **1) Detekce kybernetických bezpečnostních událostí**

- **2) Hlášení kybernetických bezpečnostních událostí**
  - Do **24 hodin** (včasné varování)
  - Do **72 hodin** (prvotní posouzení)
  - Do **30 dnů** (závěrečná zpráva)
  - Vyšší režim - **všechny** incidenty
  - Nižší režim - pouze **významné** incidenty

- **3) Řešení kybernetických bezpečnostních událostí**

Splunk & NIS2

NIS2 požadavek	Splunk řešení
Detekce událostí a incidentů	Splunk Enterprise Security
	Splunk Security Essentials
	Splunk Enterprise Security Content Update
	Splunk Risk Based Alerting
Vyšetřování, hlášení událostí a incidentů	Splunk Incident Workbench
	Splunk Risk Based Alerting
	Splunk SOAR
Řešení incidentů	Splunk Enterprise Security
	Splunk SOAR

Čím je Splunk SIEM jiný?

Není to „krabice“ - je to řešení budoucnosti

- **Příjem jakýchkoli** dat a podpora nasazení v multi-cloud, hybridním nebo on-prem prostředí (MS je jen v cloudu například)
- **Data-driven SIEM –** Detekce bezpečnostních hrozeb na základě pokročilé analýzy všech typů dat pomocí pokročilých korelačních pravidel s využitím AI
- **1600+ přednastavených detekcí:** Přednastavené detekce sladěné s průmyslovými rámci, jako je například **MITRE ATT&CK.**
- **Neomezená customizace –** používá otevřené standardy, umožňuje vývoj zákaznických řešení bez nutnosti účasti výrobce.

Risk Based Alerting (RBA): o 50% snížení false positives

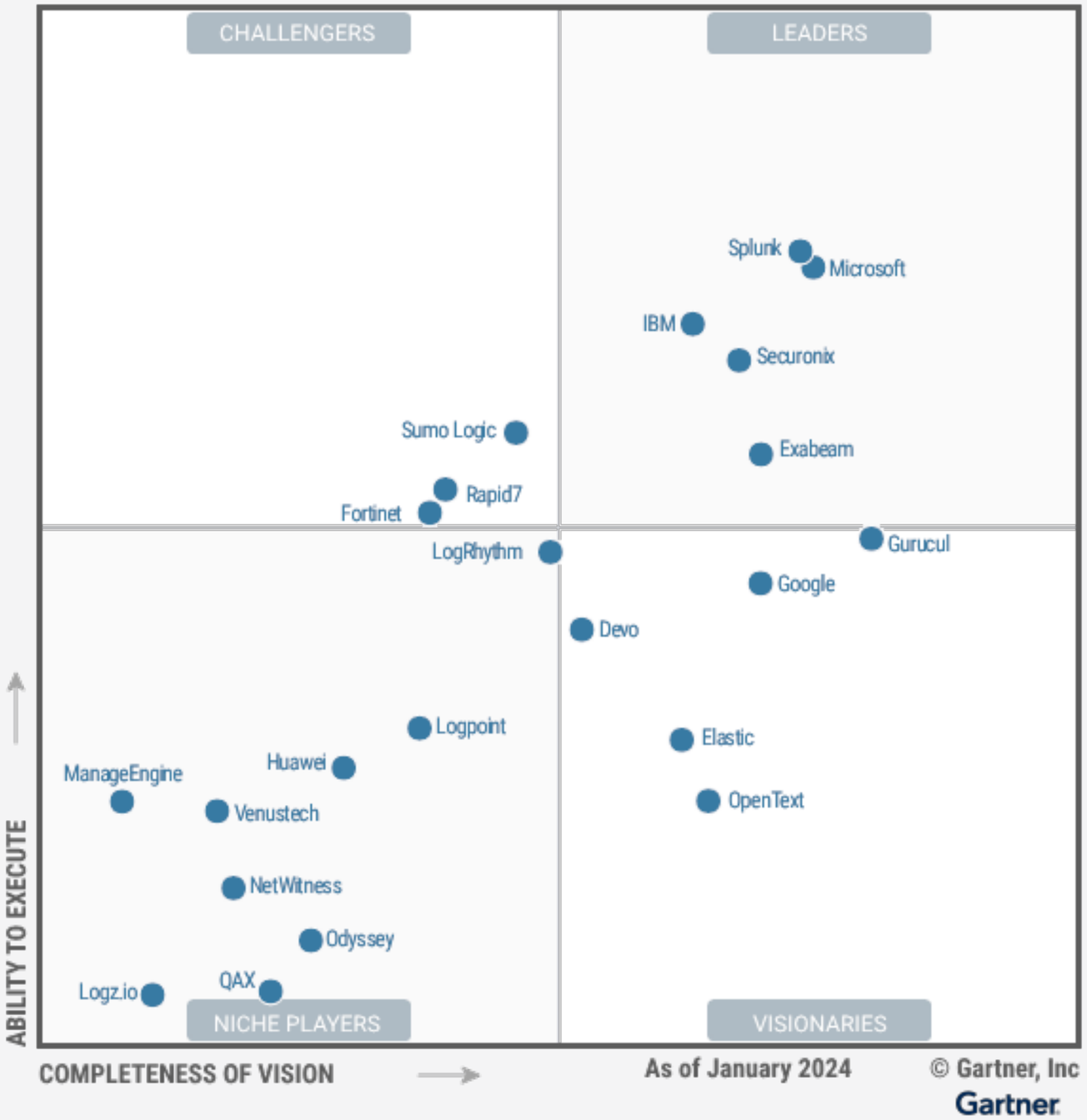
Automatizace procesů SOC (SOAR)

Až 4x rychlejší odpověď na incidenty

Splunk je tržním lídrem...

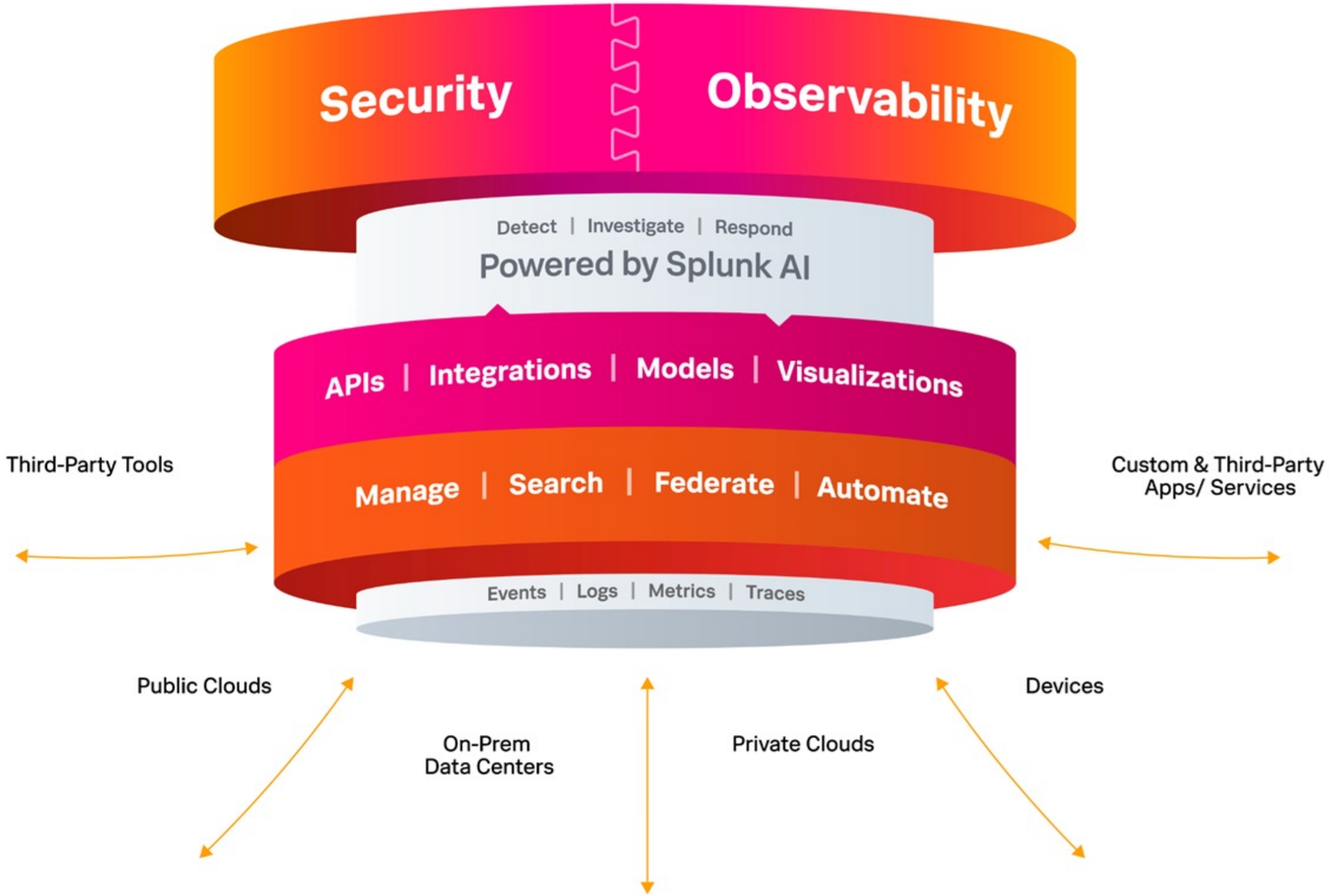
2024 Gartner Magic Quadrant for Security Information and Event Management

- Splunk je označen jako „Leader“ po desáté v řadě



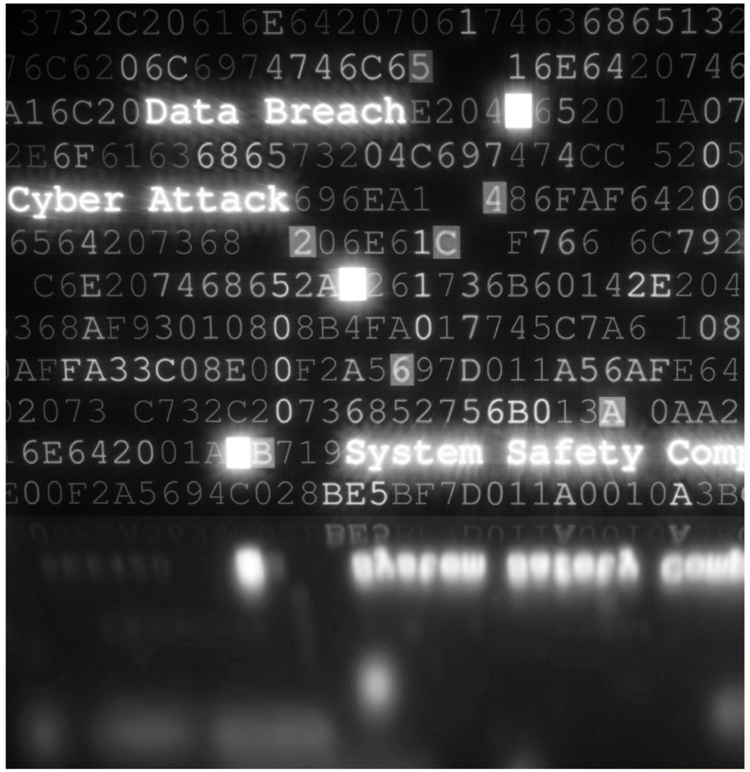
Jak to celé funguje?

Architektura Splunku



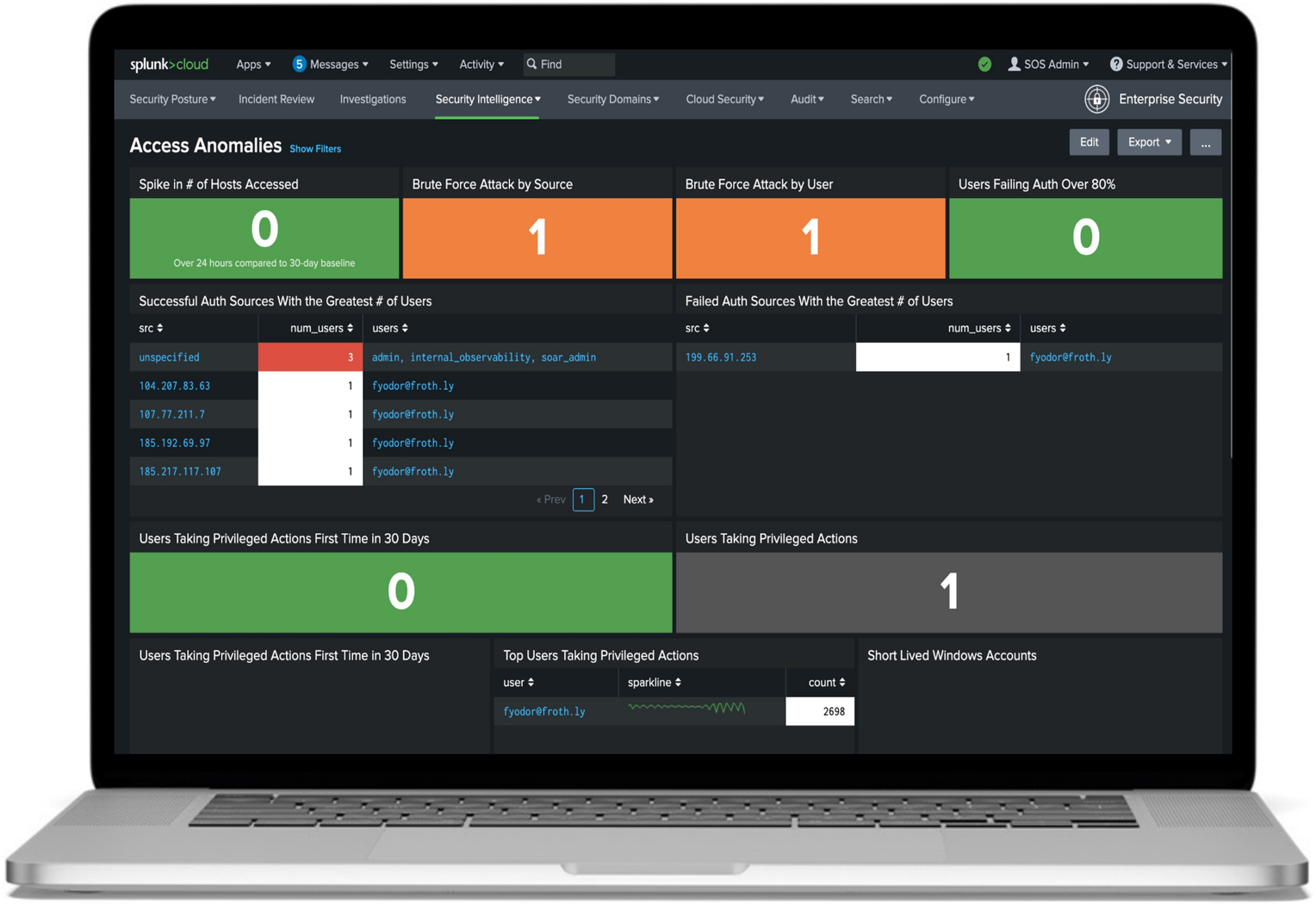
Splunk Enterprise Security (SIEM)

- **Platforma** pro ukládání, normalizaci a analýzu libovolných dat z libovolného zdroje.
- **Schema-on-read** a distribuované ukládání dat pro rychlé a flexibilní získání informací.
- **Analýza chování založená na ML** pro detekci neznámých a pokročilých útoků.
- **Risk-based alerting** pro generování kvalitních a snadno zpracovatelných alertů.
- **Integrovaná threat intelligence** pro dodatečné a kontextuální informace související s hrozbami a alerty.



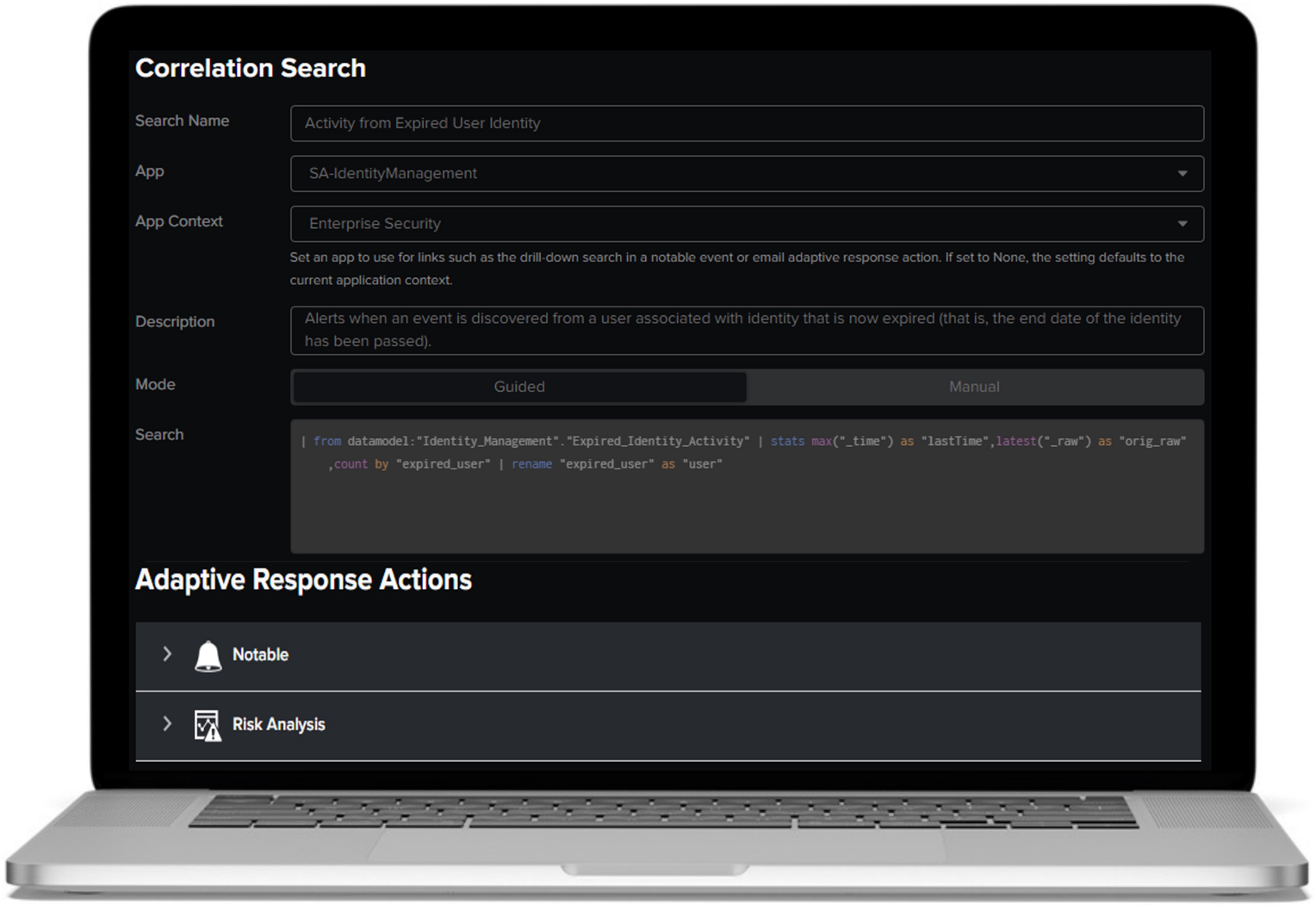
Splunk UEBA

- Baselining, detekce anomálií
- Obousměrná výměna informací mezi ES a UEBA
- Detekce napadených stanic a uživatelských účtů
- Zjišťování aktivity podezřelých uživatelských účtů



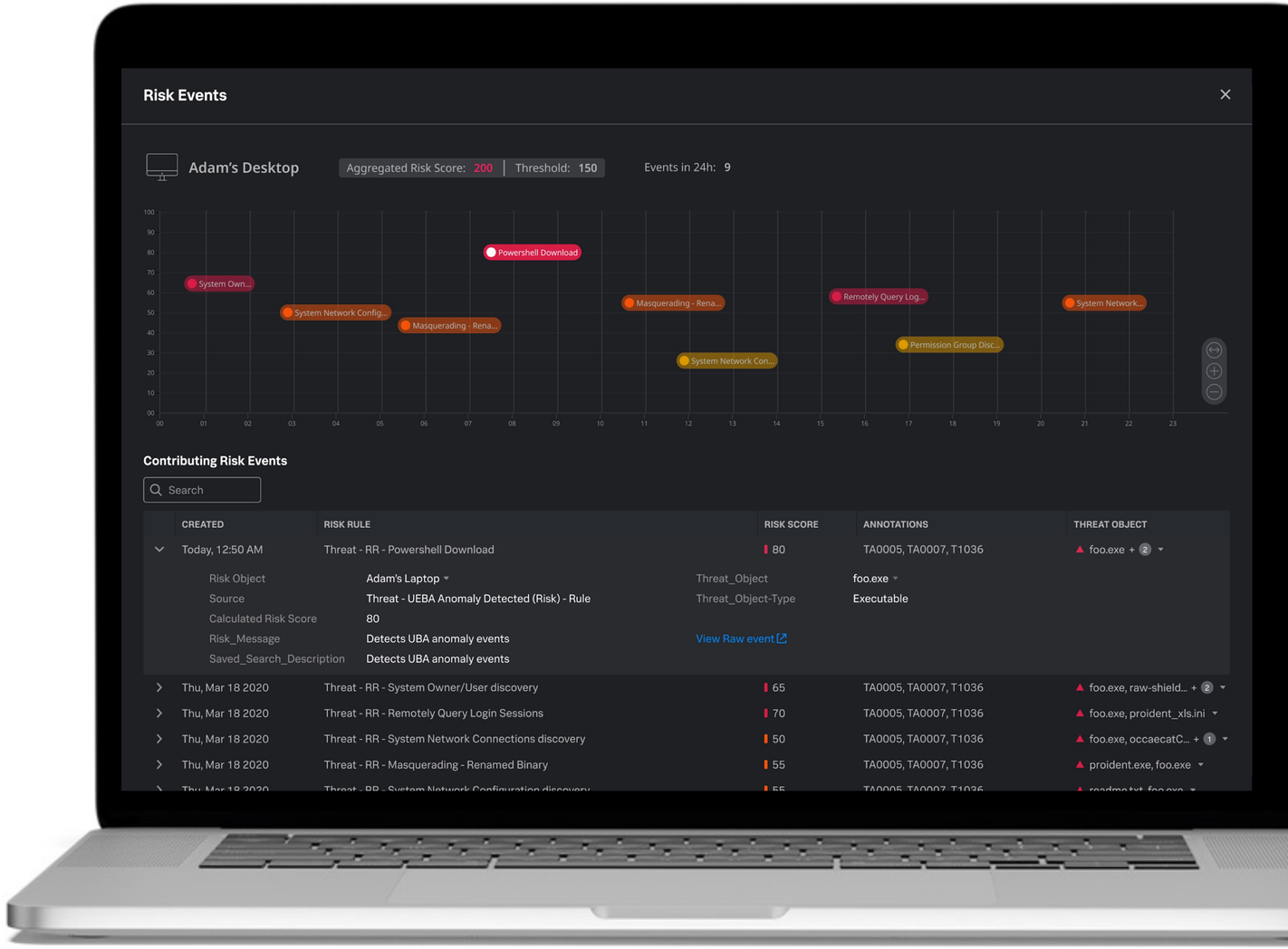
Splunk detection

- 1400+ detekčních pravidel, z toho 100+ cloudových
- Automatická reakce na incident
- Atomické alerty - chybí „big picture“



Risk Based Alerting

- „Big-picture“ na daném assetu (uživatel, server…)
- Timeline zaznamenaných událostí
- Mapování událostí na bezpečnostní frameworky (MITRE ATT&CK, NIST, CIS 20, and Kill Chain)



Risk Based Alerting

Risk object - user PC, risk treshold = 100

7:55

Email s neobvyklým Subjectem – risc score **40**

8:02

MS Word spuštěný z Outlooku– risc score **20**

8:03

Web browser spuštěný z Wordu – risc score **20**

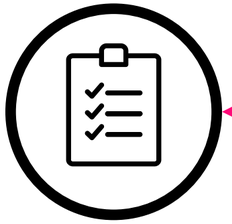
8:03

IDS blokuje odchozí provoz– risc score **40**

Aggregated risk score **>100**

Risk Incident Rule:
Generate alert for any user or system that exceeds a risk score of 100 in a 24-hour period

Risk alert



MITRE ATT&CK & Custom matrix

Alert	Source	Tactic	Score
Non-standard Port Activity	Netflow	TA0011	10
Potential C2 Activity	Web	TA0011	25
Noisy IDS Alert	IDS	TA0001	15
New Registry Startup Key	EDR	TA0003	30
New Scheduled Task Created	EDR	TA0002	35

- Detekce množství a/nebo souslednosti Techiques and tactics

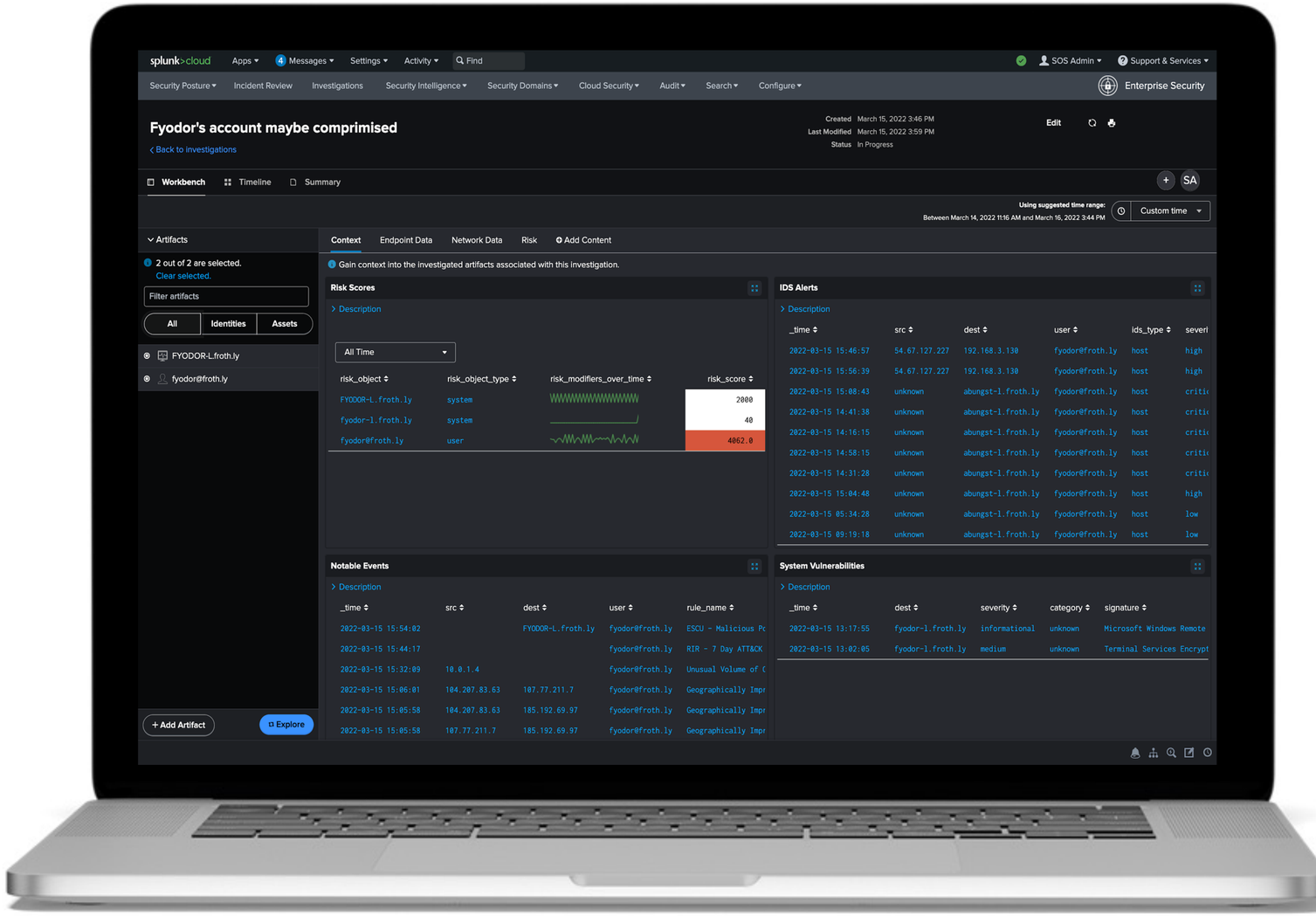
- Custom matice TTPs pro vytvoření RBA detekcí

Insider Threat Matrix

Proactive Messures	Initial Discovery	Collection	Exfiltration	Business Impact
DLP Enforcement	Browsing Job Sites	Downloads from Application	Upload to 3rd Party File Share	Bulk Delete Files
Prevent Backups to Unapproved Storage Locations	Employee Facing Disiplinary Actions	Downloads from Internal File Share	External Email with Attachments	Destruction of Physical Device
Employee Awareness	Pending Termination/Resignation	Downloads from Email	Upload to Removable Storage Device	Changing Service Account Password

Incident Workbench

- Nástroj pro vyšetřování incidentů
- Vše na jednom místě
- Kooperace, timeline



Další užitečné zdroje a nástroje

SURGe Rapid Response

splunk.com/en_us/surge.html

SURGe poskytuje technické pokyny a návody (blogy, články a webové semináře), jak rychle a přesně reagovat na aktuální kybernetické útoky.

SSE: MITRE ATT&CK Analytics Advisor

splunkbase.splunk.com/app/3435

Integrovaný MITRE ATT&CK v SSE umožňuje identifikovat mezery v zabezpečení infrastruktury a poskytnout informace pro nasazení detekčních pravidel

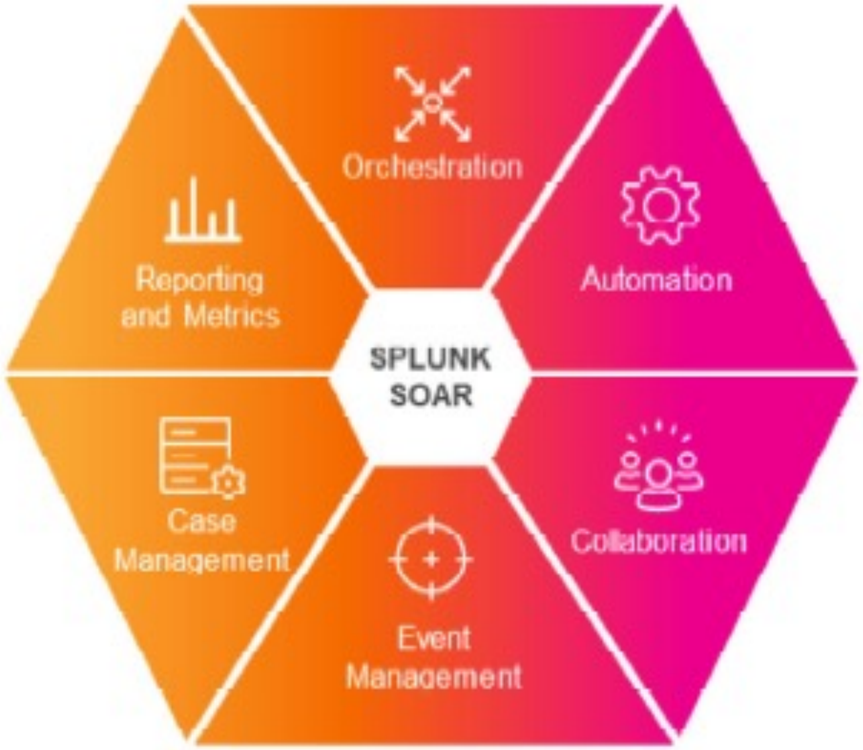
Enterprise Security Content Update (ESCU)

research.splunk.com

Balíčky, obsahující detekční pravidla, metodologii a další obsah pro detekci, vyšetřování a reakci na aktuální hrozby (update každé 2 týdny)

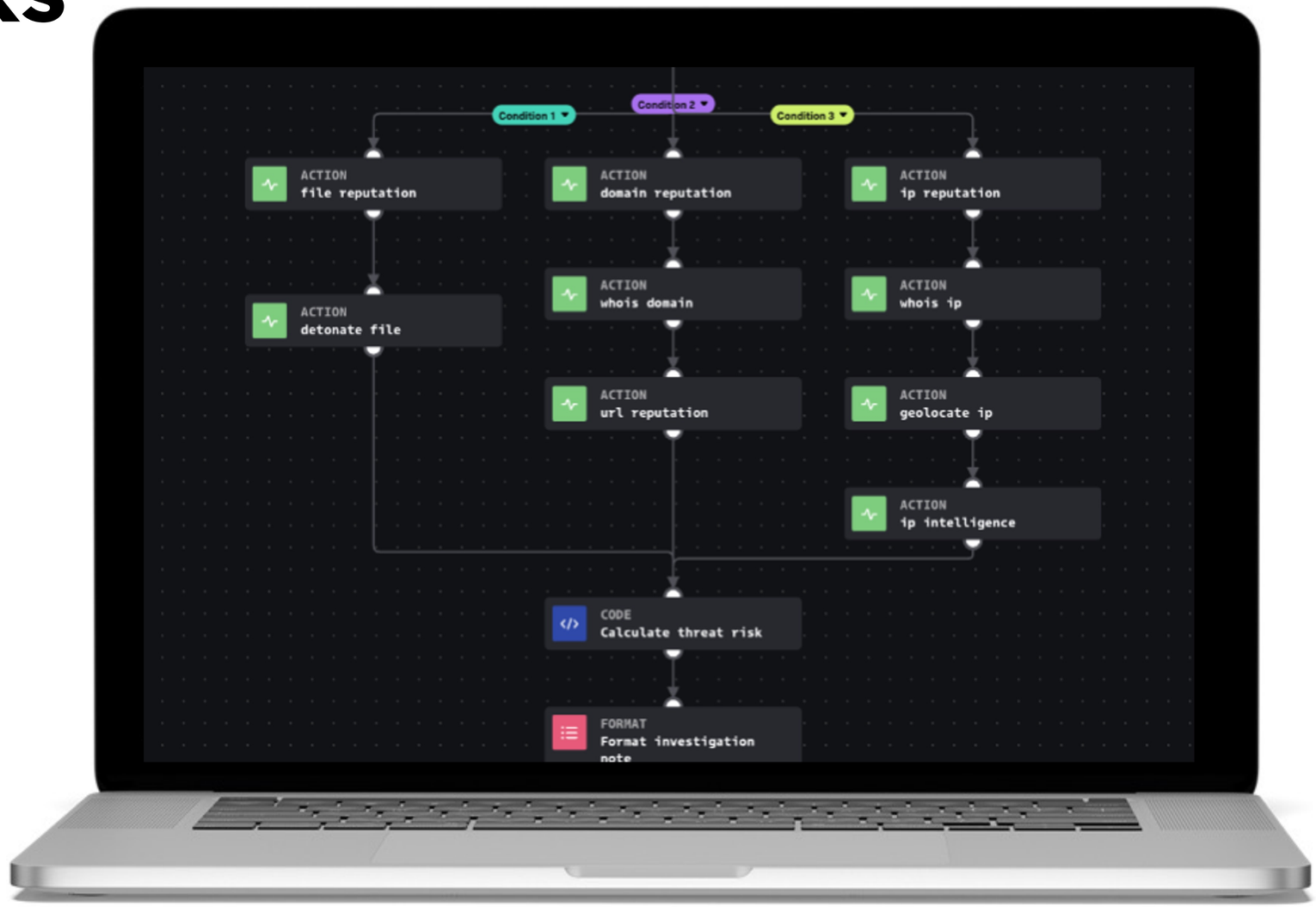
Splunk SOAR

- **Automatizace** - playbooky
- **Orchestrace** – automatická reakce na incident
- **Event management** - třídění událostí, verifikace a eskalace událostí
- **Spolupráce** - sdílení informací, zachování kontextu, ML, mobilní aplikace
- **Case management** - Standart Operation Procedures
- **Reporting** - status, výkonnost, efektivita, revize uzavřených případů, ROI



SOAR - playbooks

- Získání informací o rozsahu incidentu
- Reakce na incident - vyřešení

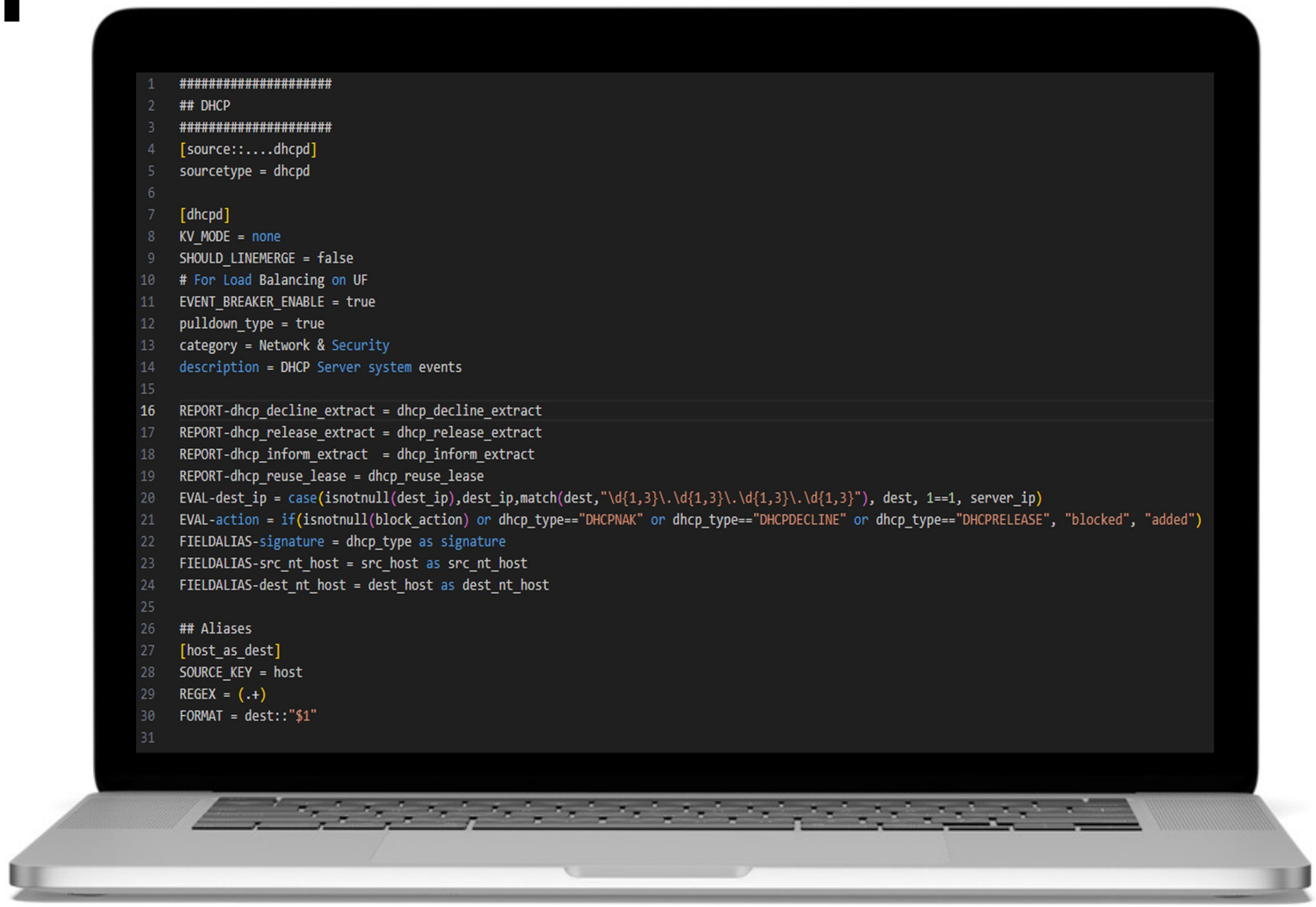


SOAR - orchestrace

- 380+ externích systémů
- 3400+ akcí

Přizpůsobitelnost

- Splunk je otevřený systém
- Založený na obecných standardech, technologiích a formátech
- Umožňuje snadný vývoj vlastního obsahu
- Třeba i pro NIS2…



Děkujeme