Tech Club webinář

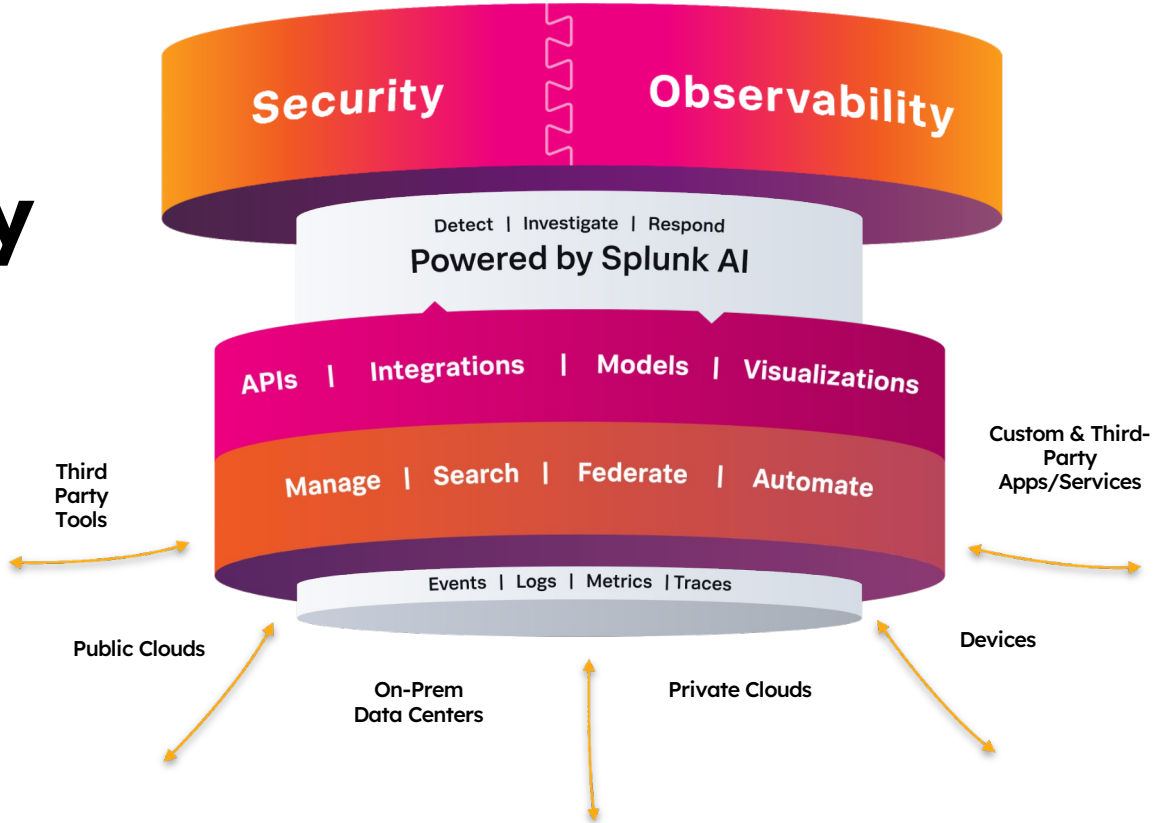
Bezpečnost a Splunk
Přehled produktů a řešení

Artem Bryksa
Solutions Engineer

29. dubna 2025

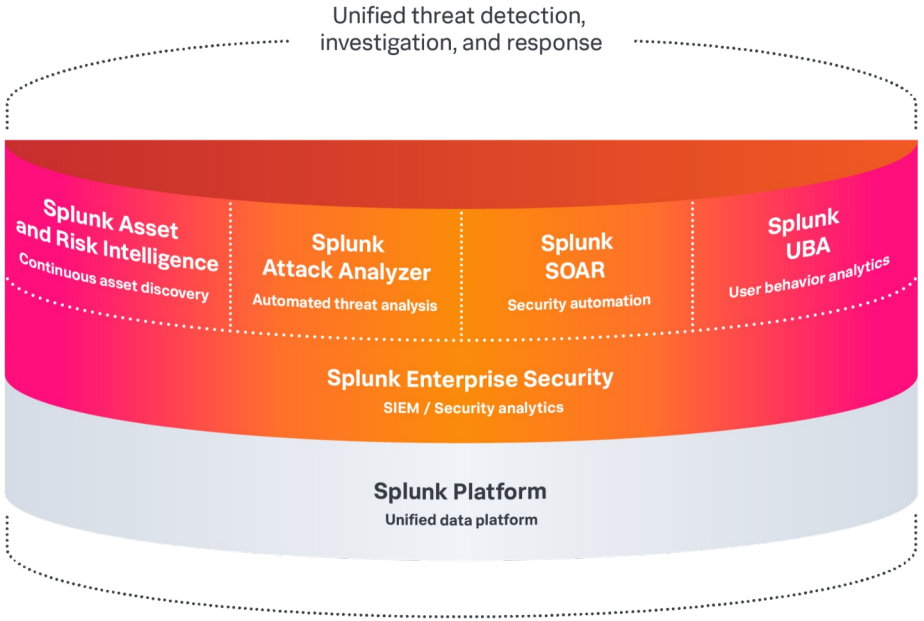
splunk>
a CISCO company

Sjednocená Security a Observability Platforma



Splunk Security

SOC budoucnosti poháněný sjednoceným TDIR řešením



Third-party tools | Cisco User/ Cloud/ Breach/XDR | Talos | Networking | IT/OT | Applications | Clouds | Data centers

Integrace pro ochranu celé vaší digitální stopy

Threat intelligence

Zlepšete obranu proti známým a neznámým hrozbám

Splunk +
Cisco Talos

Bezpečnostní výstrahy a kontext

Zrychlete detekci, vyšetřování a reakci

Splunk +
Cisco Security Cloud App

Secure AI

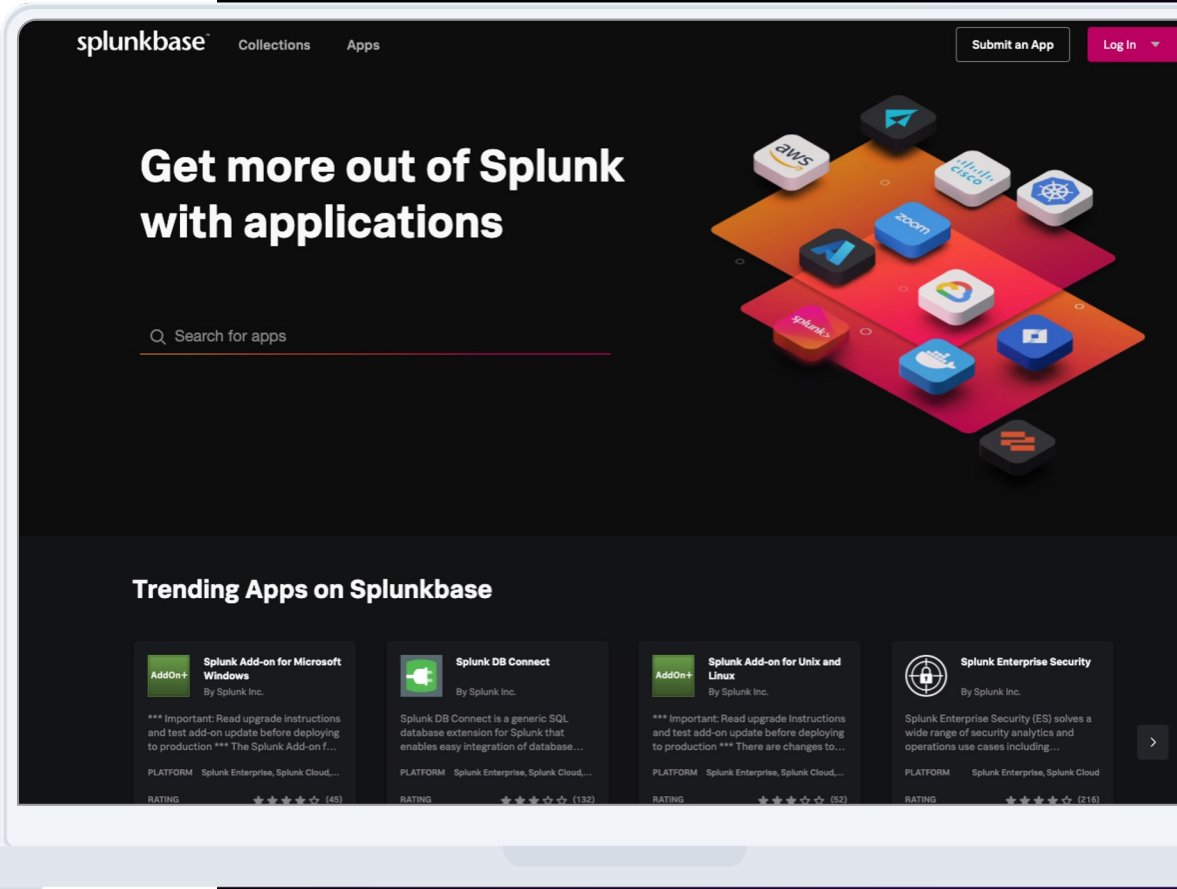
Získejte ochranu při budování, používání a inovacích pomocí umělé inteligence

Splunk +
AI Defense

Splunk aplikace a přídavky

https://splunkbase.splunk.com

- 2100+ aplikací a přídavků
- Předem vytvořená vyhledávání, reporty, vizualizace a integrace
- Stahujte aplikace a přizpůsobte je podle svých požadavků
- Rychlý čas k získání hodnoty z vašich dat
- Vytvářejte a přispívejte svými vlastními aplikacemi!

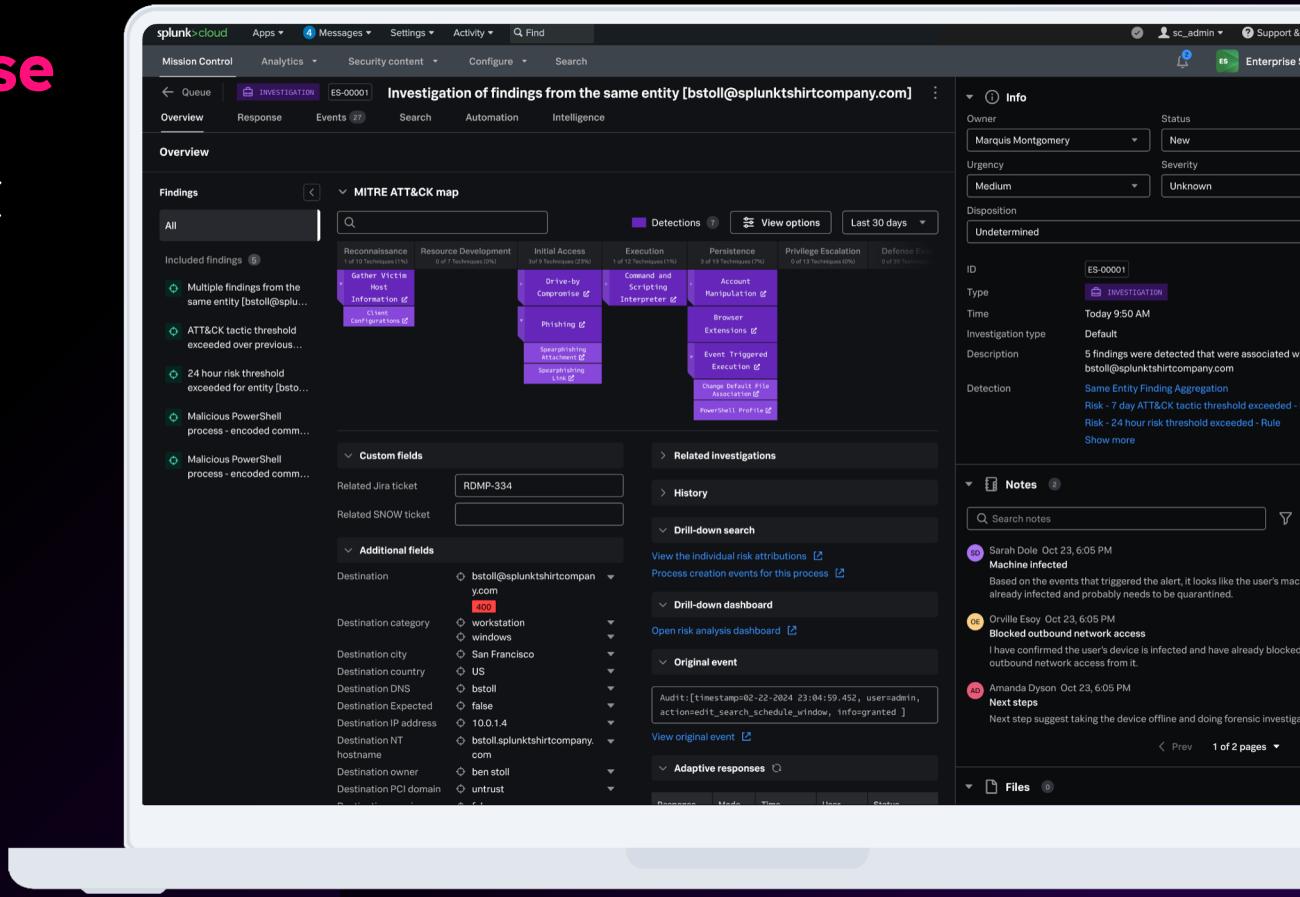


Splunk Enterprise Security

Detekujte na čem záleží, zkoumejte holisticky a reagujte rychle

Splunk Enterprise Security
Posilte svůj SOC

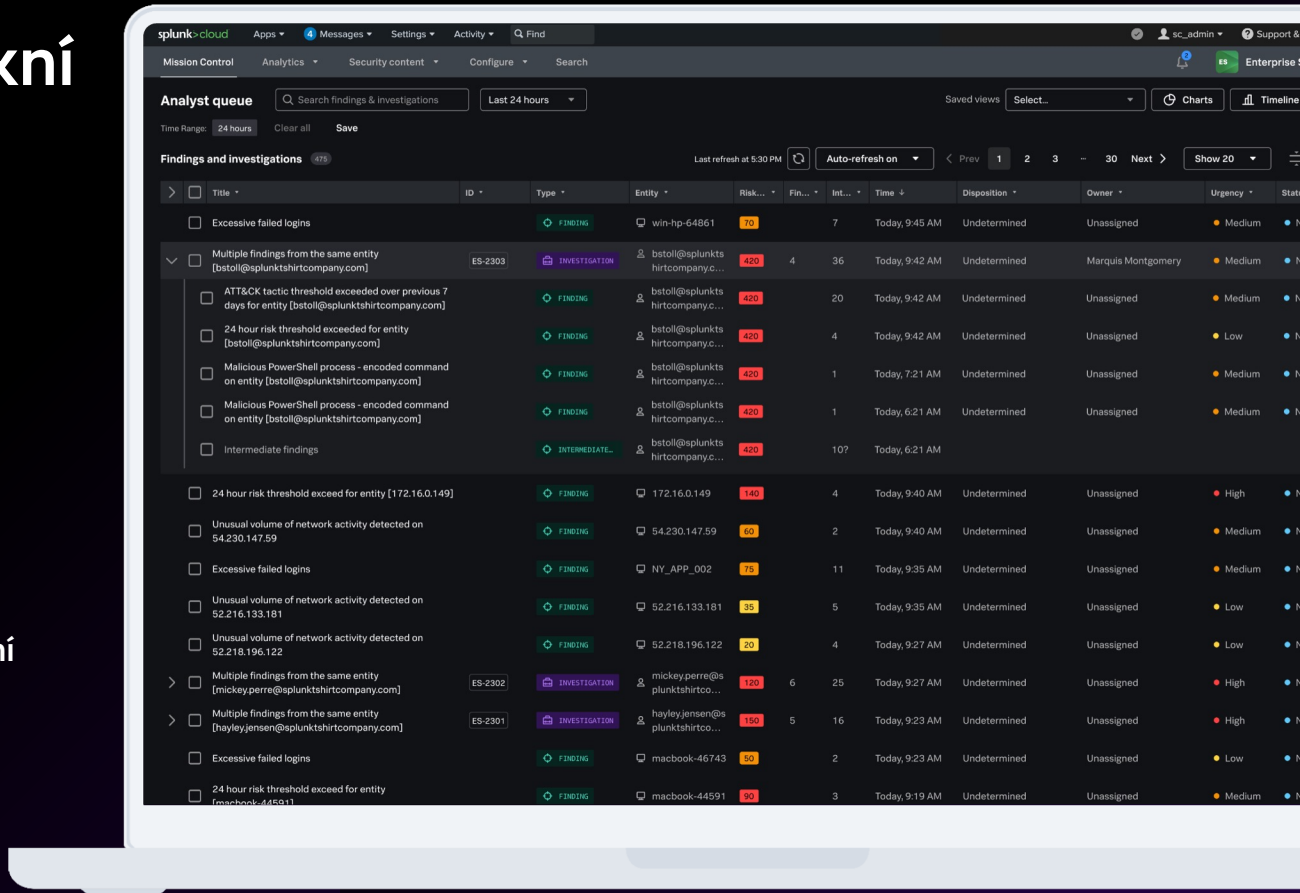
- Získejte komplexní přehled
- Podpořte přesné detekce
- Podpořte provozní efektivitu



Získejte komplexní přehled

Získejte přehled nad datovým šumem

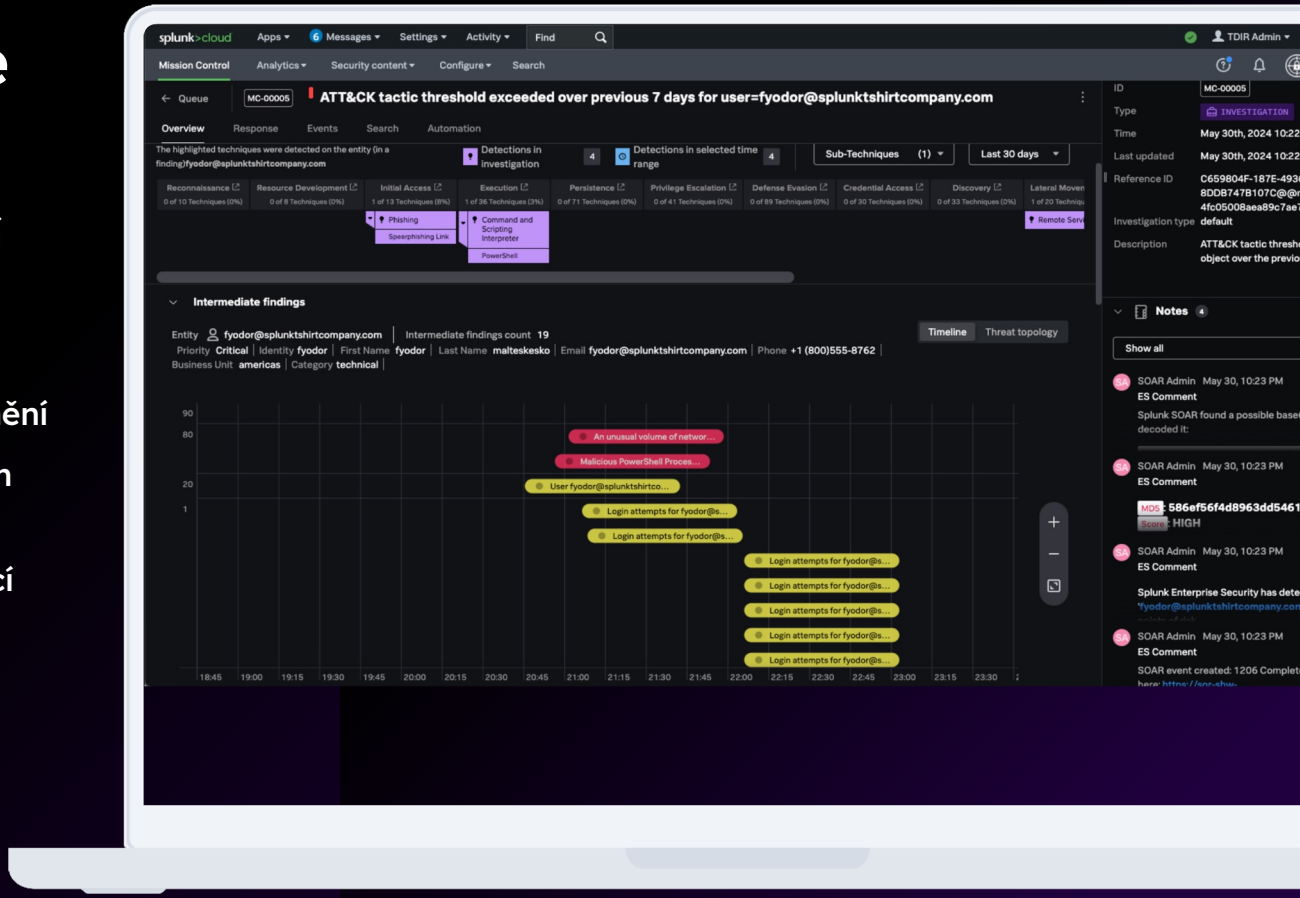
- Jedinečný, komplexní přehled
- Orientujte se v upozorněních
- Snadno získejte přehled
- Dosáhněte nákladově efektivní optimalizace



Podpořte přesné detekce

Zefektivněte vyšetřování a zvyšte produktivitu

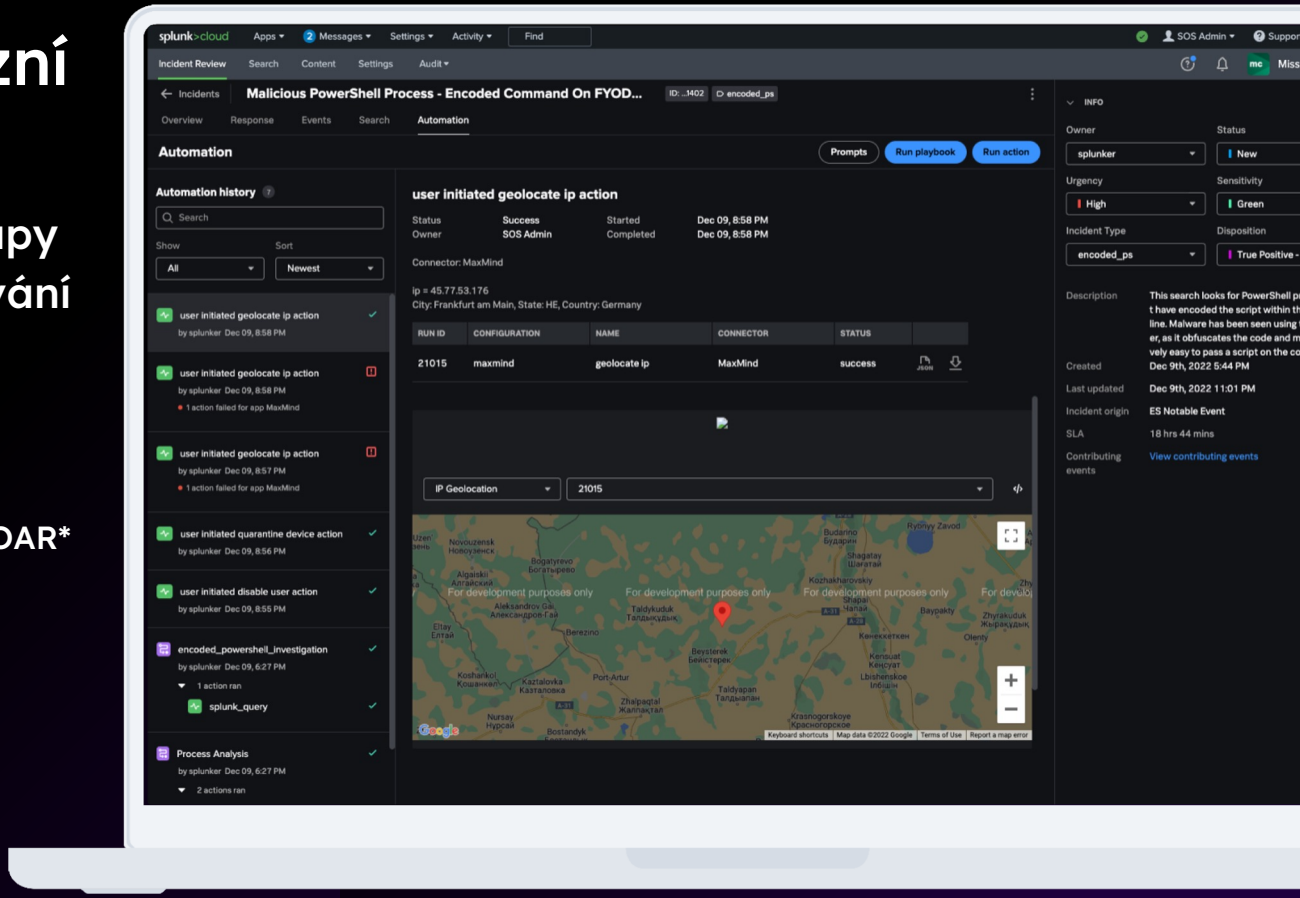
- Výrazně snižte objem upozornění
- Využijte více než 1 700 předem připravených detekcí
- Automatické verzování detekcí
- Vylepšené možnosti detekce



Podpořte provozní efektivitu

Sjednoťte pracovní postupy detekce hrozeb, vyšetřování a reakce (TDIR)

- Jednotné, moderní pracovní prostředí
- Nativní integrace se Splunk SOAR*
- Provádějte pracovní postupy reakce



*Vyžadovaná Splunk SOAR license

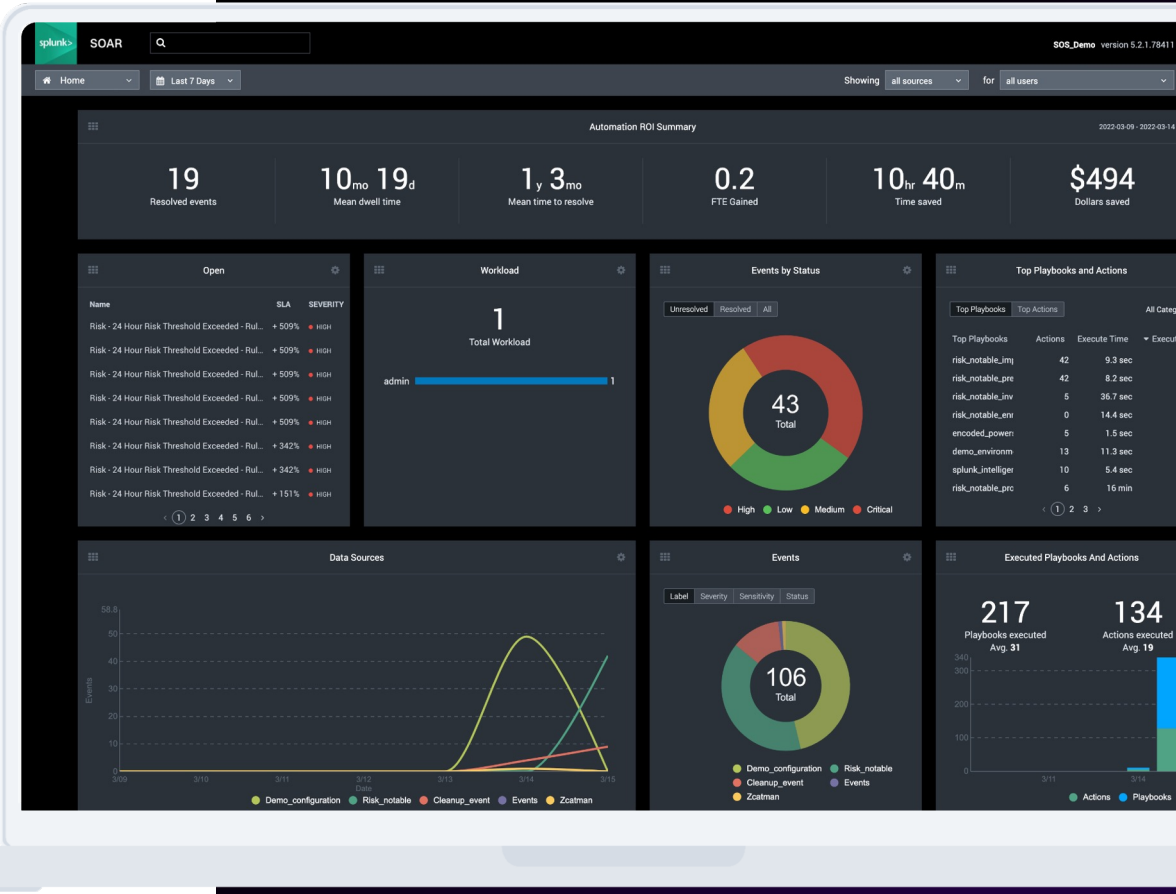
Splunk SOAR

Pracujte chytřeji
Reagujte rychleji
Posilte svůj SecOps

Vneste řád do chaotického SOC

Zefektivněte vyšetřování a zvyšte produktivitu

- Zvyšte využití vašeho bezpečnostního systému
- Vyvíjejte snadno aplikace
- Vizualizujte a ověřujte efektivitu SOC



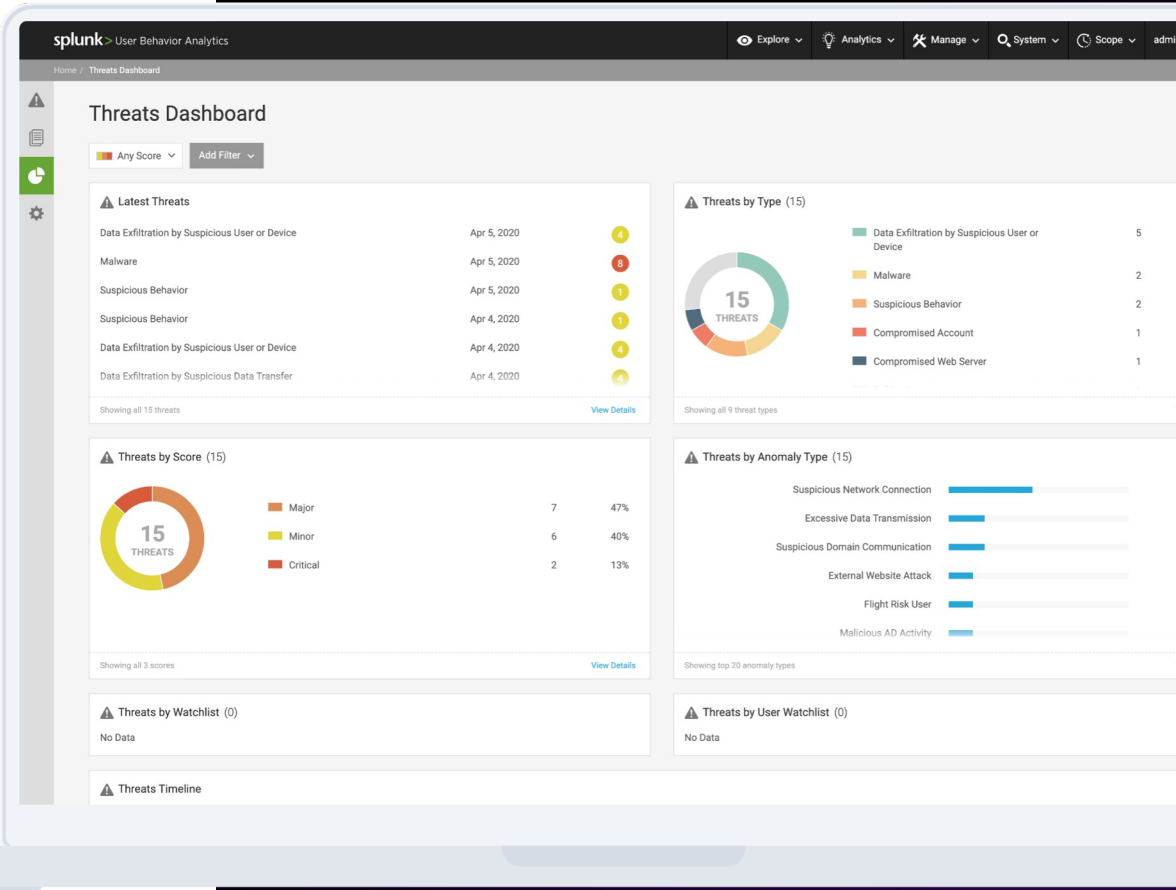
Splunk User Behavior Analytics (UBA)

Detekujte neznámé hrozby a anomální chování pomocí strojového učení.

Detekujte a eliminujte ty nejpokročilejší hrozby

Odhalte hrozby, které běžná pravidlová korelace obvykle přehlédne

- Objevte neobvyklé chování
- Rychle detekujte kompromitované uživatelské účty a stroje
- Využijte více než 250 pravidel a modelů strojového učení



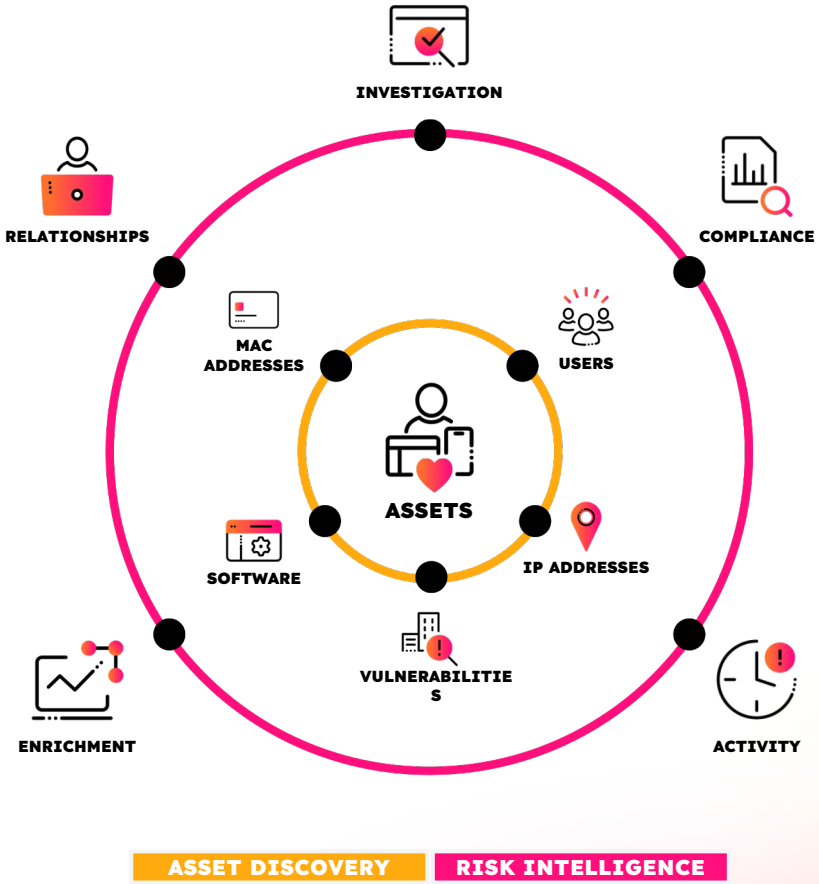
Splunk Asset and Risk Intelligence (ARI)

Splunk Asset and Risk Intelligence

Proaktivní snižování rizik prostřednictvím kontinuálního objevování assetů a monitorování souladu s předpisy

Nepřetržitě objevuje prostředky (včetně zařízení, uživatelů a aplikací) s využitím bohatých dat ve Splunku.

Asset and Risk Intelligence identifikuje porušení souladu s předpisy a mezery v bezpečnostních kontrolách pomocí předem připravených i vlastních frameworků, aby zrychlil vyšetřování a snížil rizikové vystavení.



Co ARI je a není

ARI je...

- Nástroj pro bezpečnostní vyšetřování, který poskytuje obohacení dat o assets a accounts
- SecOps řešení
- Součást kategorie produktů pro řízení IT rizik
- Schopnost vylepšit stávající nástroje pro ITOps

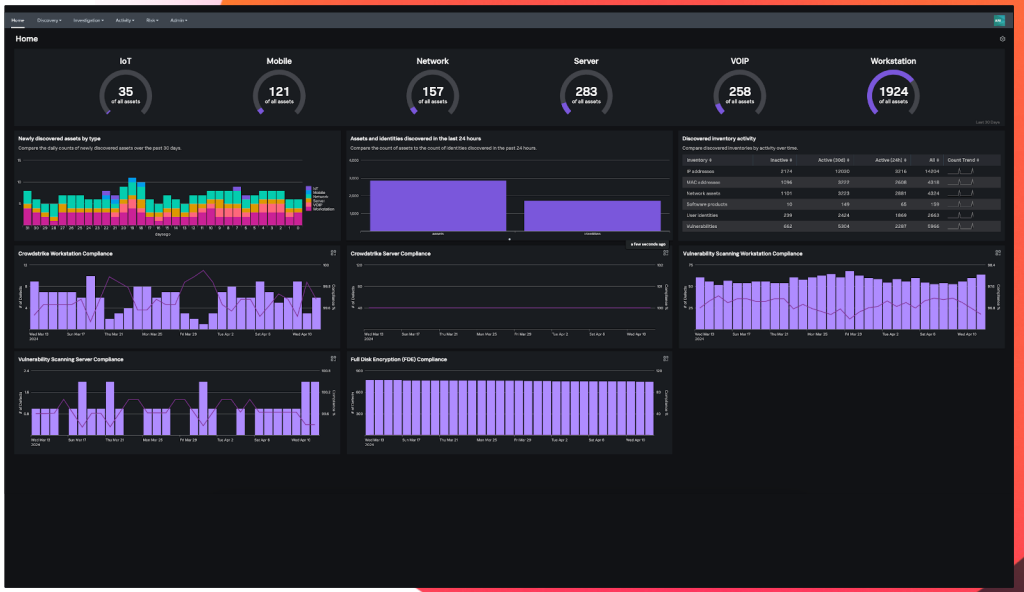
ARI NENÍ...

- Asset Management Tool
- CMDB nebo náhrada CMDB
- Náhrada nástrojů jako ServiceNow

splunk> a CISCO company

Posílení SecOps pomocí Splunk Asset and Risk Intelligence

- Získejte komplexní **přehled o assetech** pro snížení rizikového vystavení
- Zrychlete **bezpečnostní vyšetřování** díky přesnému kontextu assetů
- Identifikujte mezery v **souladu s předpisy** v bezpečnostních kontrolách
- Bezproblémová **integrace** a nasazení se Splunk **Enterprise Security**
- Propojte IT a bezpečnost pomocí integrace **ServiceNow CMDB**



Splunk Attack Analyzer

Splunk Attack Analyzer

Automatizujte analýzu hrozeb podezřelého malwaru a útoků typu phishing na přihlašovací údaje

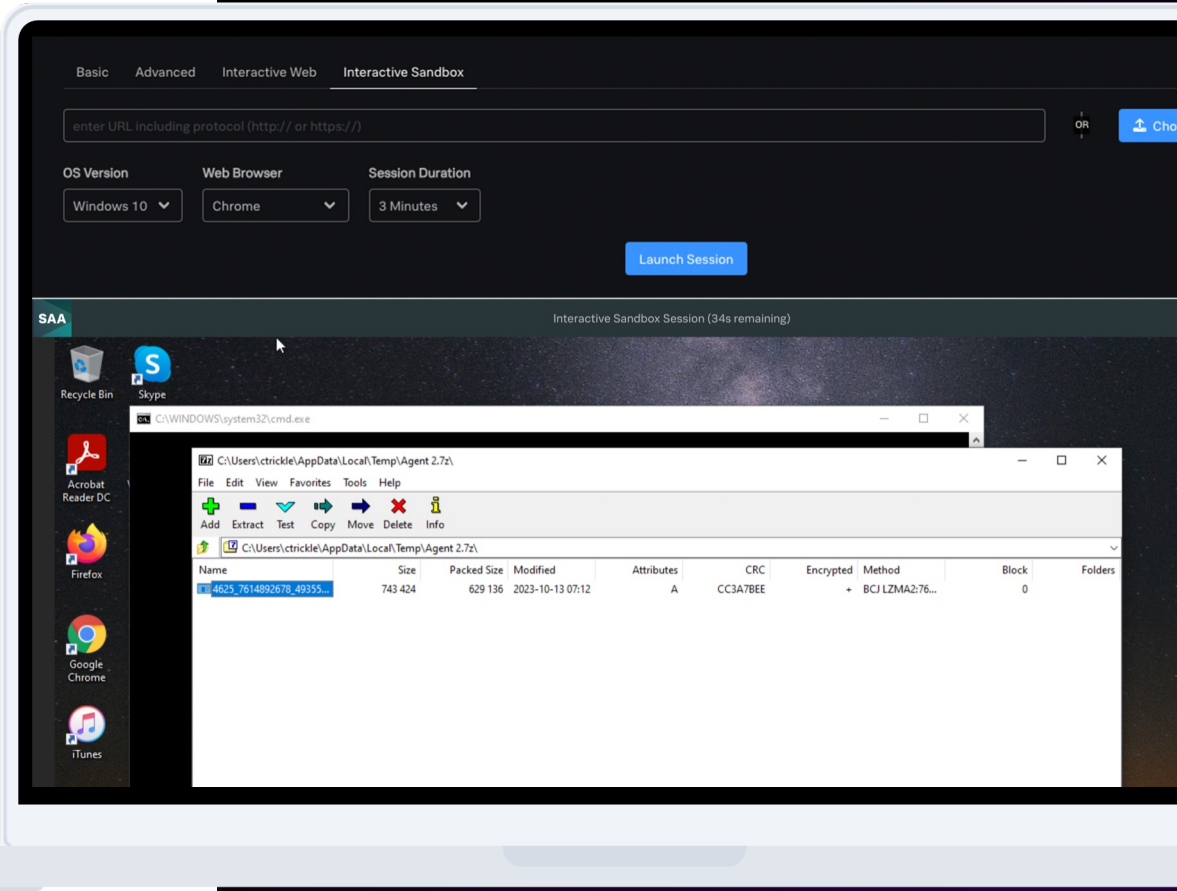
Odstraňte **manuální práci** z analýzy hrozeb

Získejte **konzistentní, komplexní** a vysoce kvalitní **analýzu hrozeb**

Inteligentní **automatizace** pro komplexní analýzu a reakci na hrozby

Bezpečně pracujte se škodlivým obsahem

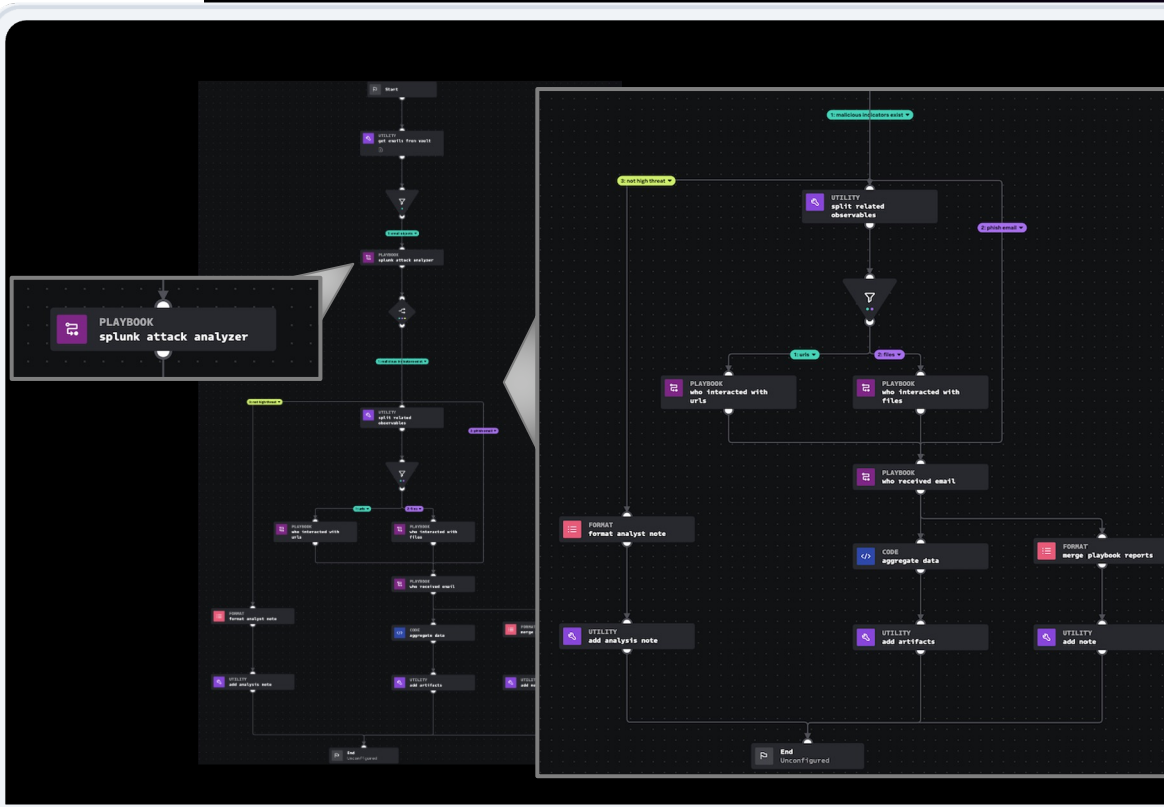
- **Přistupujte ke škodlivému obsahu** pocházejícímu z URL adres a souborů
- **Provádějte důkladné vyšetřování** a mějte jistotu, že identita analytika a společnosti zůstane skryta



Komplexní analýza a reakce

Integrujte se Splunk SOAR pro inteligentní automatizaci

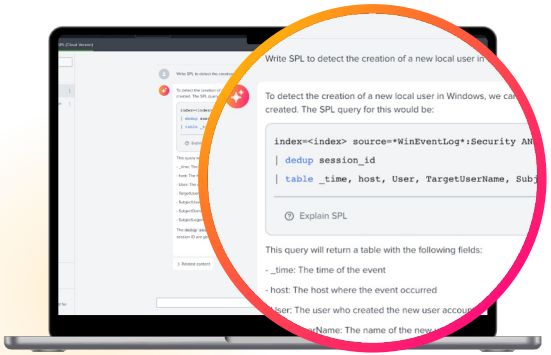
- **Provádějte automatizovanou analýzu identifikovaných indikátorů** bez nutnosti manuálních vyšetřovacích úkolů
- **Odstraňte potřebu složitých playbooků** využívajících více produktů pro analýzu hrozeb
- **Splunk SOAR spustí odpovídající playbook** poté, co Splunk Attack Analyzer potvrdí aktivní hrozbu



Splunk AI Asistenti

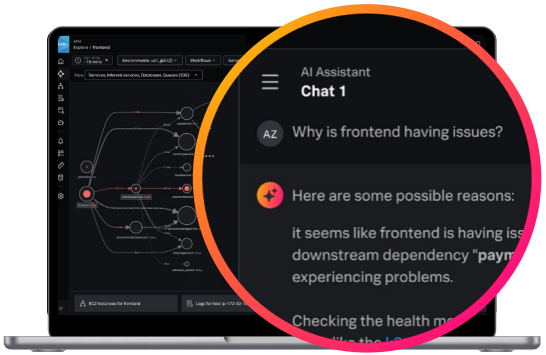
Zvyšte produktivitu, a umožněte rychlejší detekci a řešení

AI Assistant for SPL



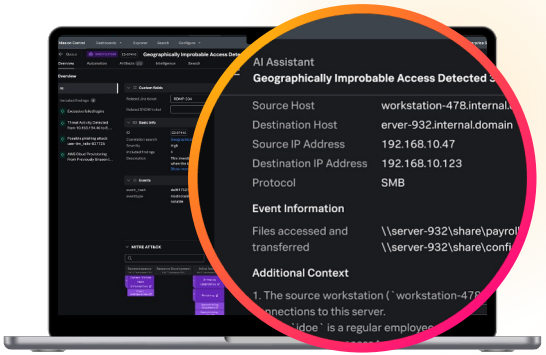
Generally Available

AI Assistant in Observability Cloud



Generally Available

AI Assistant in Enterprise Security

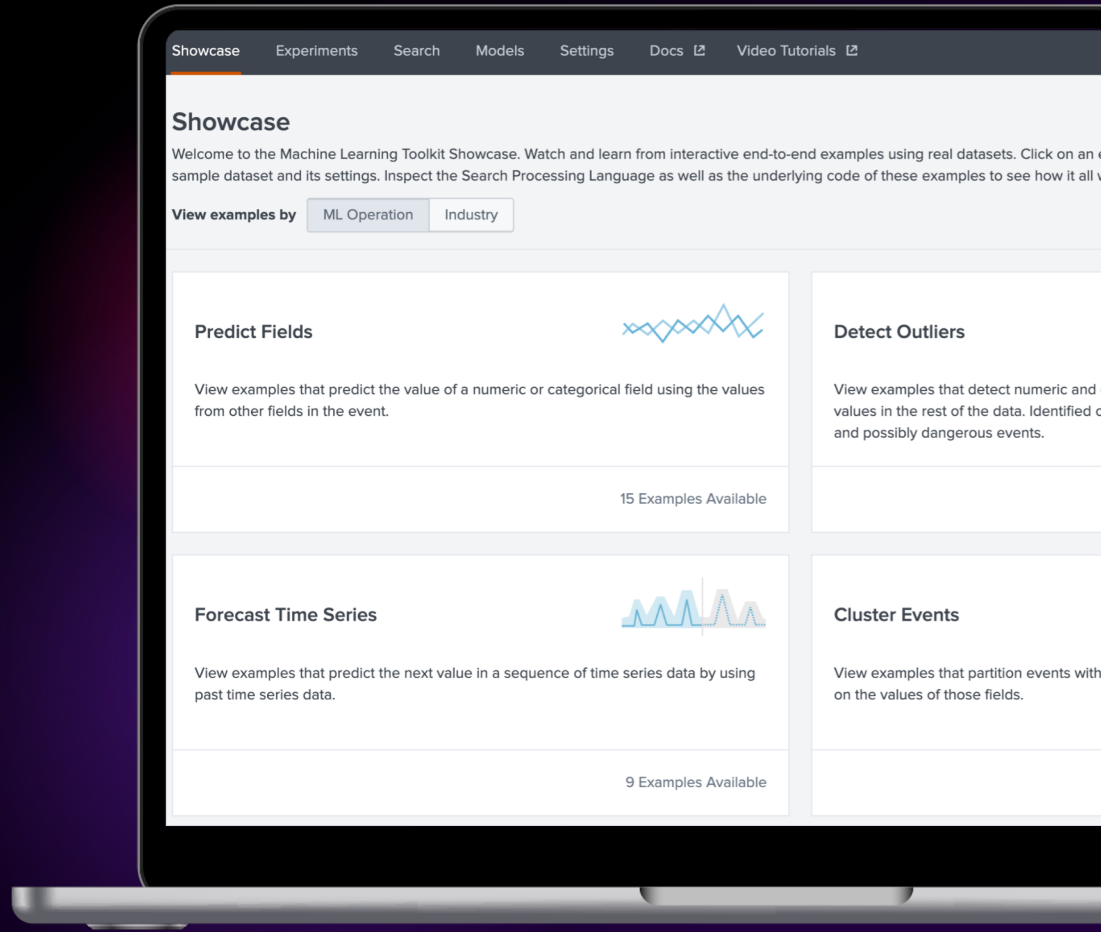


Preview

Machine Learning Toolkit (MLTK)

Ve Splunk Cloud and Enterprise

- Experimentujte a modelujte svá data ve Splunku s asistovaným průvodcem pro celý AI workflow.
- Více než 50 algoritmů na výběr nebo možnost přinést vlastní model.
- Trénujte a nasazujte pomocí vyhledávacích příkazů a operacionalizujte v reálném čase.



Staňte se EMEA BOTS šampionem!

Splunk Boss of the SOC

Praha – 7. května – 10:00 – 15:30
A taky online

Registrujte se nyní!

Děkujeme za Vaši pozornost

Následující Tech Club webinář:

13.5. **Stav a vývoj bezpečnosti počítačových sítích**

Hosté:

- Tomáš Čejka, Vedoucí oddělení pro síťovou bezpečnost a monitoring, CESNET
- Filip Dvořák, Architekt kybernetické bezpečnosti, Řízení letového provozu České republiky
- Stanislav Bárta, zástupce ředitele odboru Vládní CERT, NÚKIB
- Jiří Rott, Solutions Engineer, Cisco Systems

Registrovat se můžete na oficiálním webu **Cisco Tech Club webináře**