

Tech Club webinář

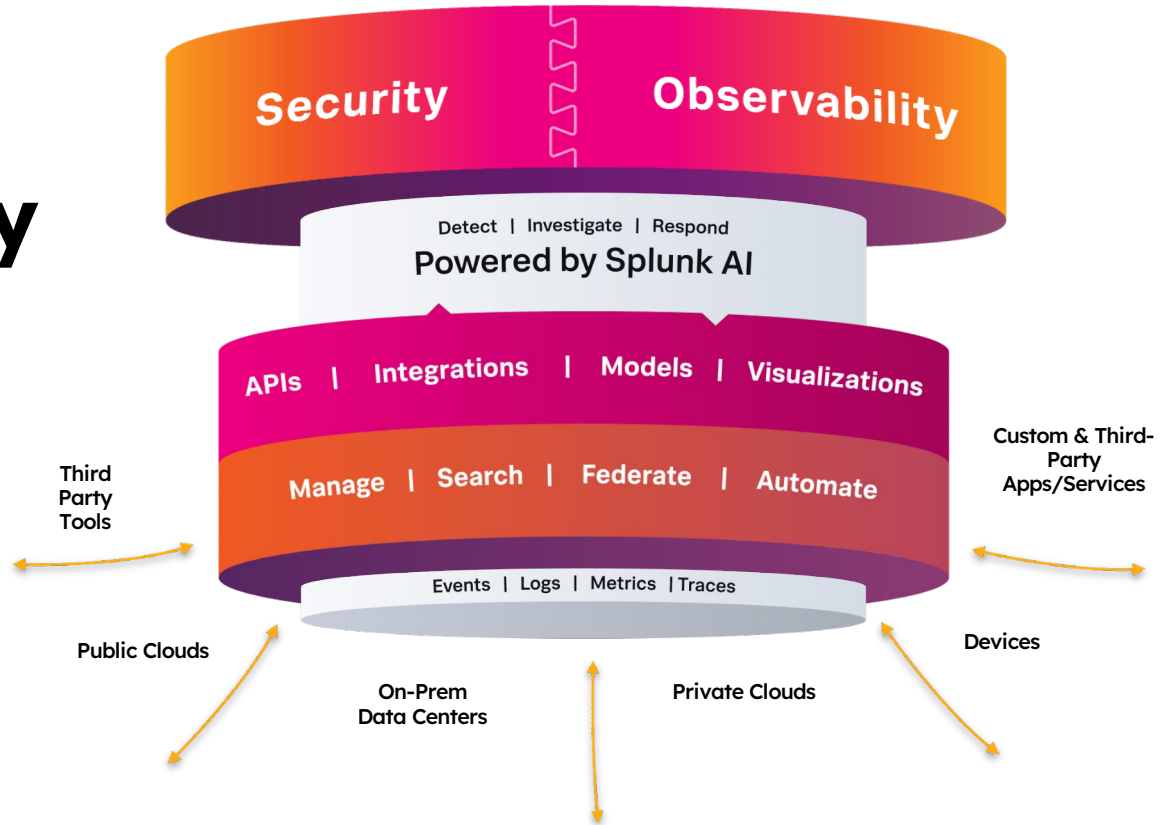
Bezpečnost a Splunk Přehled produktů a řešení

Artem Bryksa
Solutions Engineer

29. dubna 2025

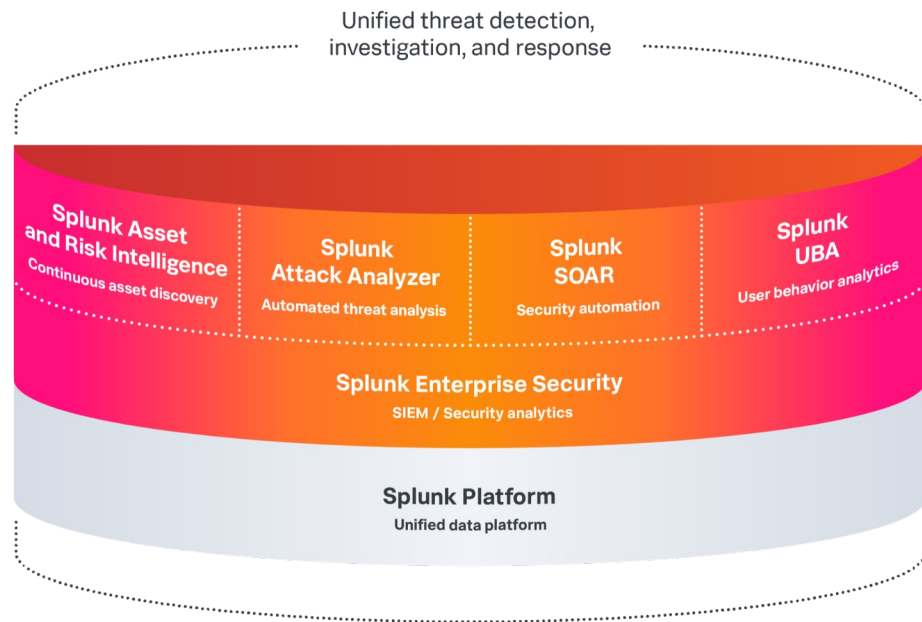


Sjednocená Security a Observability Platforma



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

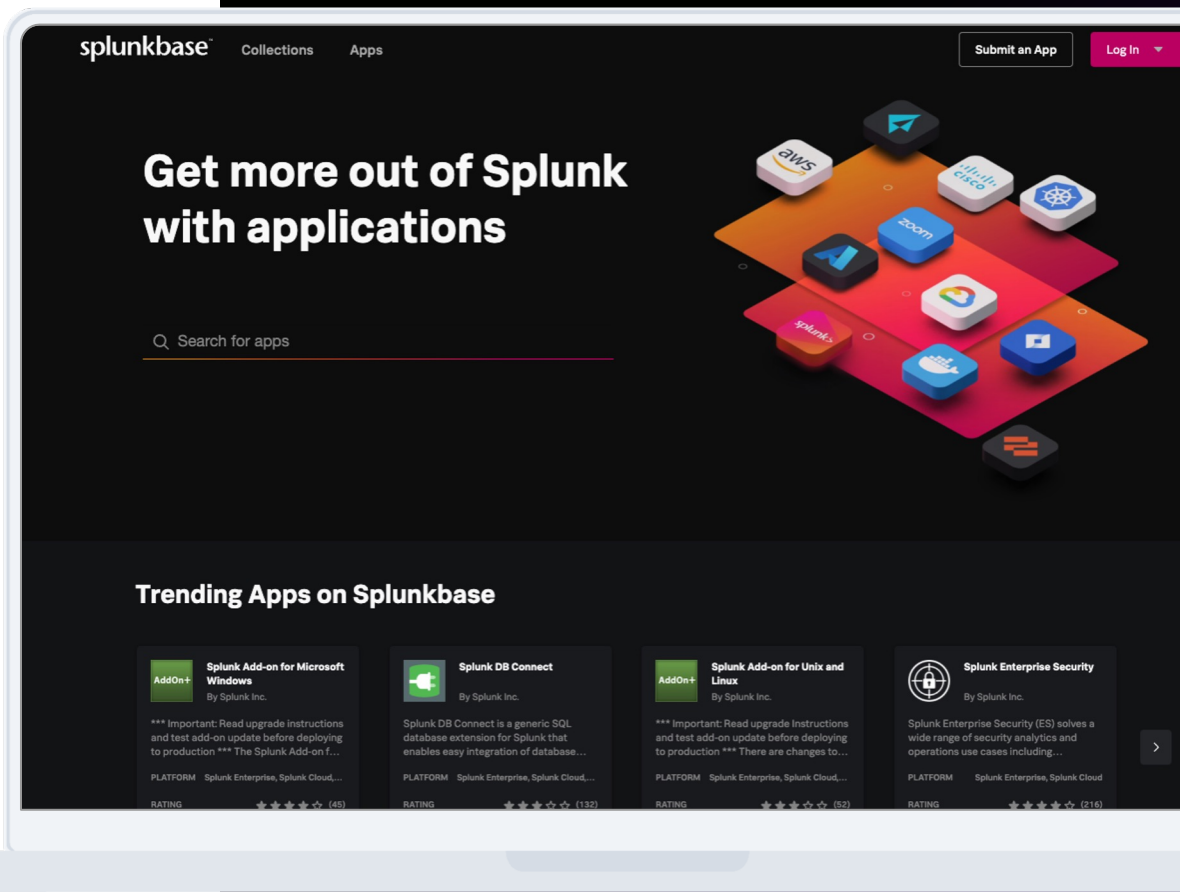
Získejte ochranu při budování, používání a inovacích pomocí umělé inteligence

Splunk +
AI Defense

Splunk aplikace a přídatky

<https://splunkbase.splunk.com>

- 2100+ aplikací a přídatků
- 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

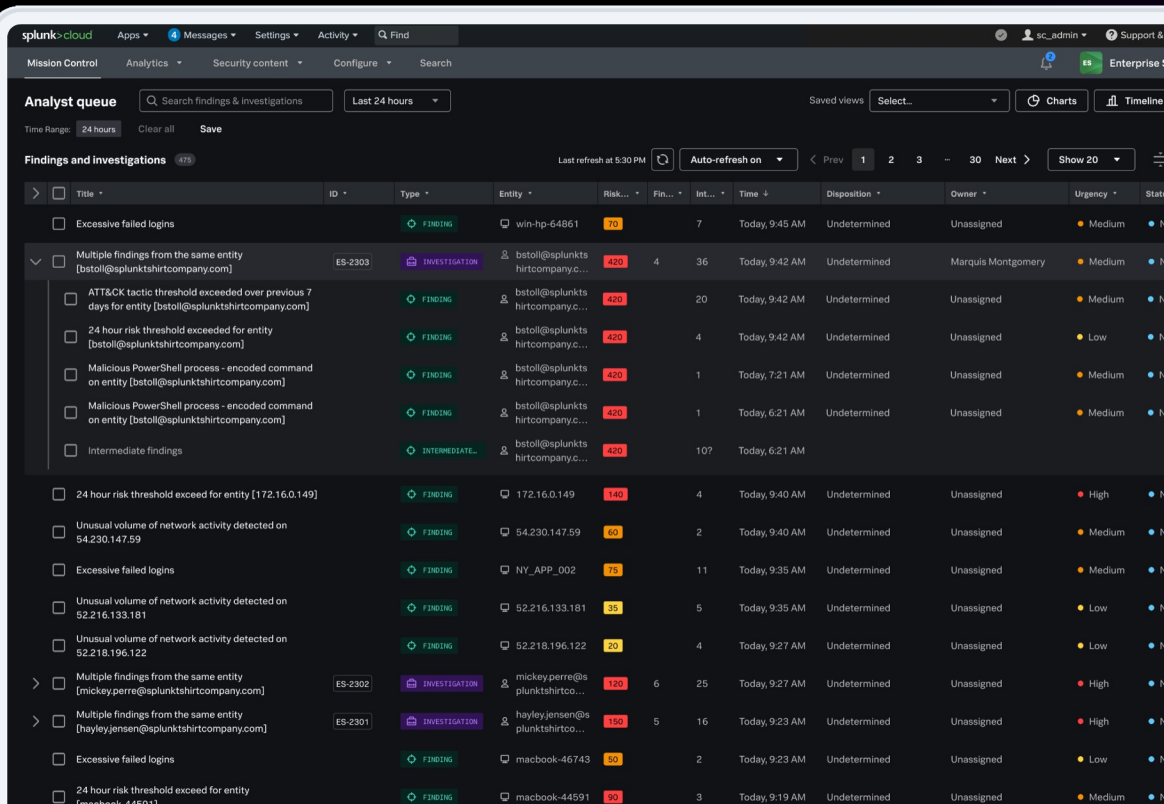
- Získejte komplexní přehled
- Podpořte přesné detekce
- Podpořte provozní efektivitu

The screenshot displays the Splunk Enterprise Security interface. The top navigation bar includes links for Mission Control, Analytics, Security content, Configure, and Search. The main content area is titled 'Investigation of findings from the same entity [bstoll@splunkshirtcompany.com]' and shows a 'Findings' section with a 'MITRE ATT&CK map'. The map includes categories like Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, and Defense Evasion. The 'Findings' section lists several findings, including 'Multiple findings from the same entity [bstoll@splu...]', 'ATT&CK tactic threshold exceeded over previous...', '24 hour risk threshold exceeded for entity [bsto...]', 'Malicious PowerShell process - encoded comm...', and 'Malicious PowerShell process - encoded comm...'. The right-hand sidebar contains sections for 'Info' (Owner: Marquis Montgomery, Status: New, Urgency: Medium, Severity: Unknown, Disposition: Undetermined), 'Notes' (Search notes, Sarah Dole Oct 23, 6:05 PM, Machine infected, Orville Esay Oct 23, 6:05 PM, Blocked outbound network access, Amanda Dyson Oct 23, 6:05 PM, Next steps), and 'Files'.

Získejte komplexní přehled

Získejte přehled nad datovým šumem

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

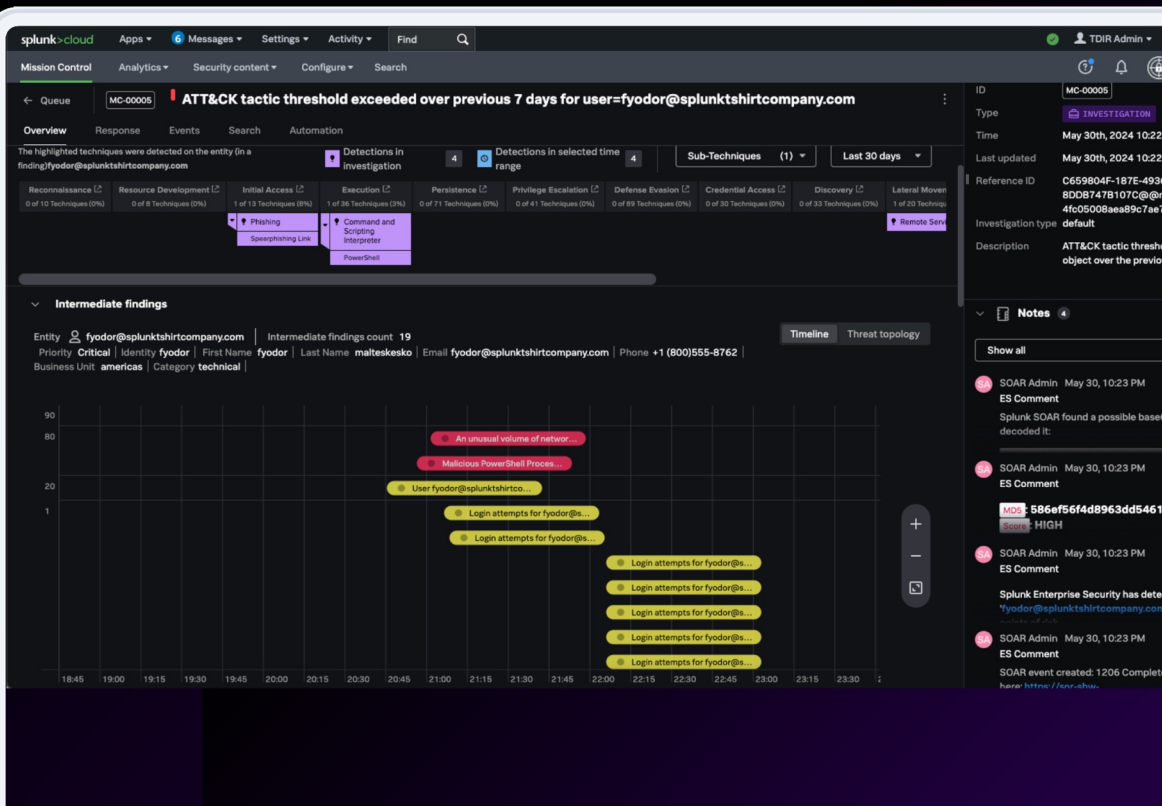


The screenshot displays the 'Analyst queue' in Splunk Cloud, showing a list of findings and investigations. The interface includes a search bar, filters, and a table of results. The table columns are: Title, ID, Type, Entity, Risk, Fin..., Int..., Time, Disposition, Owner, Urgency, and Status. The findings are categorized by type (FINDING, INVESTIGATION, INTERMEDIATE) and risk level (High, Medium, Low). The table shows various findings related to excessive failed logins, multiple findings from the same entity, and unusual volume of network activity detected on specific IP addresses.

Title	ID	Type	Entity	Risk	Fin...	Int...	Time	Disposition	Owner	Urgency	Status
Excessive failed logins		FINDING	win-hp-64861	70		7	Today, 9:45 AM	Undetermined	Unassigned	Medium	N
Multiple findings from the same entity [bstoll@splunkshirtcompany.com]	ES-2303	INVESTIGATION	bstoll@splunkshirtcompany.c...	420	4	36	Today, 9:42 AM	Undetermined	Marquis Montgomery	Medium	N
ATT&CK tactic threshold exceeded over previous 7 days for entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		20	Today, 9:42 AM	Undetermined	Unassigned	Medium	N
24 hour risk threshold exceeded for entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		4	Today, 9:42 AM	Undetermined	Unassigned	Low	N
Malicious PowerShell process - encoded command on entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		1	Today, 7:21 AM	Undetermined	Unassigned	Medium	N
Malicious PowerShell process - encoded command on entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		1	Today, 6:21 AM	Undetermined	Unassigned	Medium	N
Intermediate findings		INTERMEDIATE	bstoll@splunkshirtcompany.c...	420		107	Today, 6:21 AM				
24 hour risk threshold exceed for entity [172.16.0.149]		FINDING	172.16.0.149	340		4	Today, 9:40 AM	Undetermined	Unassigned	High	N
Unusual volume of network activity detected on 54.230.147.59		FINDING	54.230.147.59	60		2	Today, 9:40 AM	Undetermined	Unassigned	Medium	N
Excessive failed logins		FINDING	NY_APP_002	75		11	Today, 9:35 AM	Undetermined	Unassigned	Medium	N
Unusual volume of network activity detected on 52.216.133.181		FINDING	52.216.133.181	35		5	Today, 9:35 AM	Undetermined	Unassigned	Low	N
Unusual volume of network activity detected on 52.218.196.122		FINDING	52.218.196.122	20		4	Today, 9:27 AM	Undetermined	Unassigned	Low	N
Multiple findings from the same entity [mickey.perre@splunkshirtcompany.com]	ES-2302	INVESTIGATION	mickey.perre@splunkshirtco...	320	6	25	Today, 9:27 AM	Undetermined	Unassigned	High	N
Multiple findings from the same entity [hayley.jensen@splunkshirtcompany.com]	ES-2301	INVESTIGATION	hayley.jensen@splunkshirtco...	150	5	16	Today, 9:23 AM	Undetermined	Unassigned	High	N
Excessive failed logins		FINDING	macbook-46743	50		2	Today, 9:23 AM	Undetermined	Unassigned	Low	N
24 hour risk threshold exceed for entity [macbook-44591]		FINDING	macbook-44591	90		3	Today, 9:19 AM	Undetermined	Unassigned	Medium	N

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

The screenshot displays the Splunk SOAR interface for an automation workflow titled "Malicious PowerShell Process - Encoded Command On FYOD...". The workflow is in the "Automation" tab, showing a history of runs. The "Automation history" section lists several successful runs of the "user initiated geolocate ip action" and "user initiated quarantine device action". The "Automation" section shows the "user initiated geolocate ip action" with a status of "Success". Below this, a table lists the details of the automation run, including the RUN ID (21015), CONFIGURATION (maxmind), NAME (geolocate ip), CONNECTOR (MaxMind), and STATUS (success). The "INFO" section on the right provides details about the automation, including the Owner (splunker), Status (New), Urgency (High), Sensitivity (Green), Incident Type (encoded_ps), and Disposition (True Positive). The "Description" section explains that the search looks for PowerShell processes that have encoded the script within the line. The "Created" section shows the automation was created on Dec 9th, 2022 at 5:44 PM. The "Last updated" section shows it was last updated on Dec 9th, 2022 at 11:01 PM. The "Incident origin" section shows it is an ES Notable Event. The "SLA" section shows a duration of 18 hrs 44 mins. The "Contributing events" section shows a link to view contributing events. The "IP Geolocation" section shows a map of the location of the IP address 21015, which is Frankfurt am Main, Germany.

Automation history

Search: []

Show: [All] Sort: [Newest]

user initiated geolocate ip action by splunker Dec 09, 8:58 PM ✓

user initiated geolocate ip action by splunker Dec 09, 8:58 PM ✓
1 action failed for app MaxMind

user initiated geolocate ip action by splunker Dec 09, 8:57 PM ✓
1 action failed for app MaxMind

user initiated quarantine device action by splunker Dec 09, 8:56 PM ✓

user initiated disable user action by splunker Dec 09, 8:55 PM ✓

encoded_powershell_investigation by splunker Dec 09, 6:27 PM ✓
1 action ran
splunk_query ✓

Process Analysis by splunker Dec 09, 6:27 PM ✓
2 actions ran

user initiated geolocate ip action

Status: Success
Owner: SOS Admin
Started: Completed
Dec 09, 8:58 PM
Dec 09, 8:58 PM

Connector: MaxMind

ip = 45.77.53.176
City: Frankfurt am Main, State: HE, Country: Germany

RUN ID	CONFIGURATION	NAME	CONNECTOR	STATUS	
21015	maxmind	geolocate ip	MaxMind	success	

IP Geolocation: 21015

Map showing location of IP 21015 (Frankfurt am Main, Germany).

*Vyžadovaná Splunk SOAR license

Splunk SOAR

Pracujte chytřeji

Reagujte rychleji

Posilte svůj SecOps



Vneste řád do chaotického SOC

Zefektivněte vyšetřování
a zvýšte produktivitu

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



Splunk User Behavior Analytics (UBA)

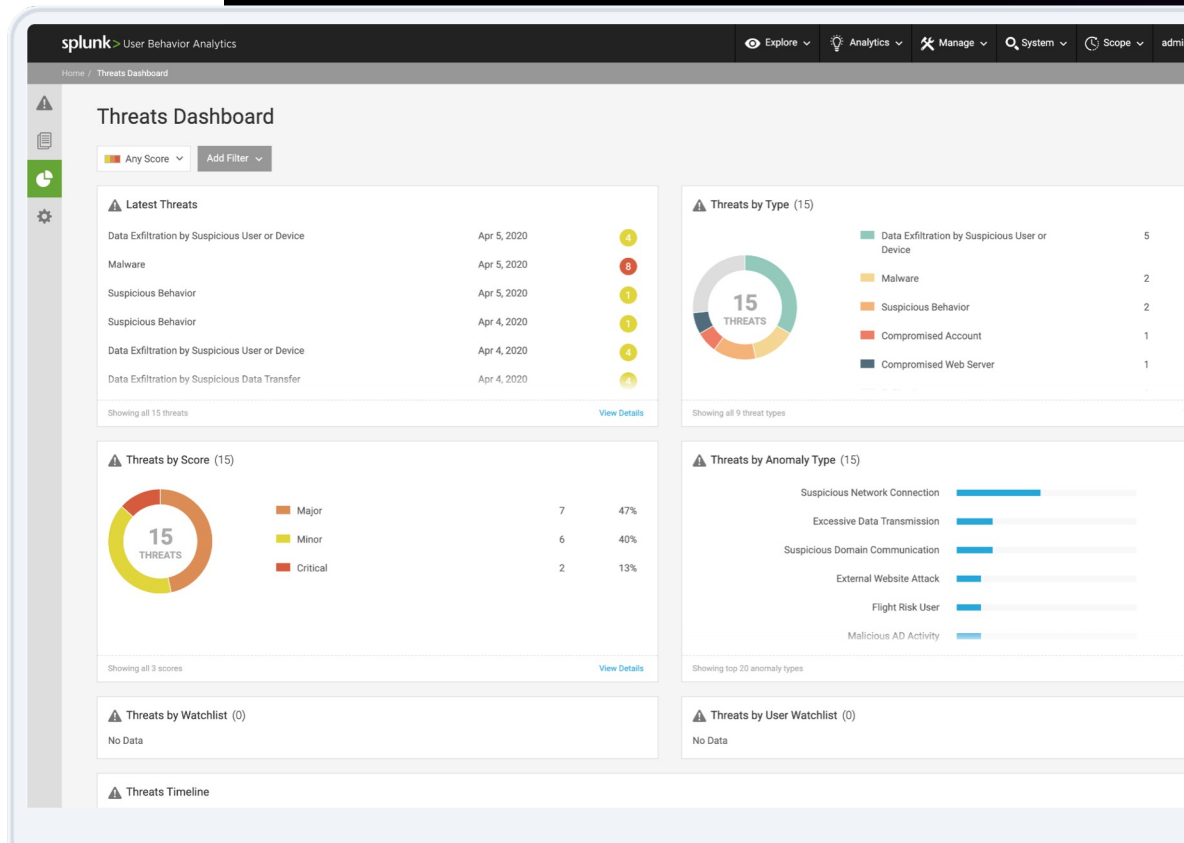
Detekujte neznámé hrozby
a anomální chování
pomocí strojového učení.



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)

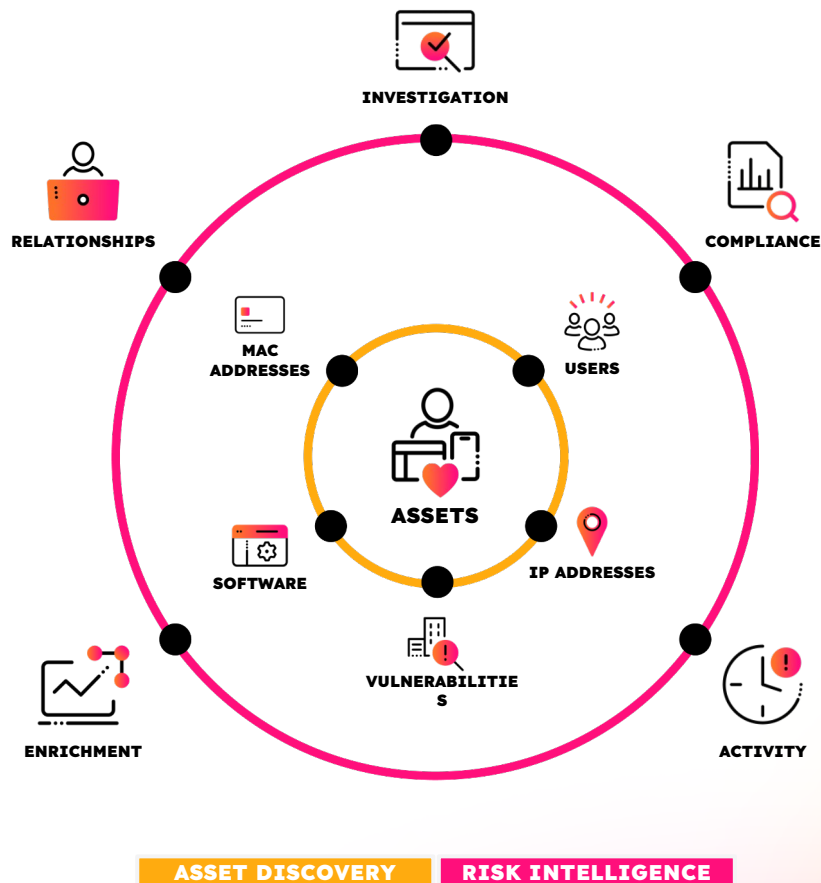


Splunk Asset and Risk Intelligence

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



Posílení SecOps pomocí Splunk Asset and Risk Intelligence



Získejte komplexní přehled o assetech pro snížení rizikového vystavení



Zrychlete bezpečnostní vyšetřování díky přesnému kontextu assetů



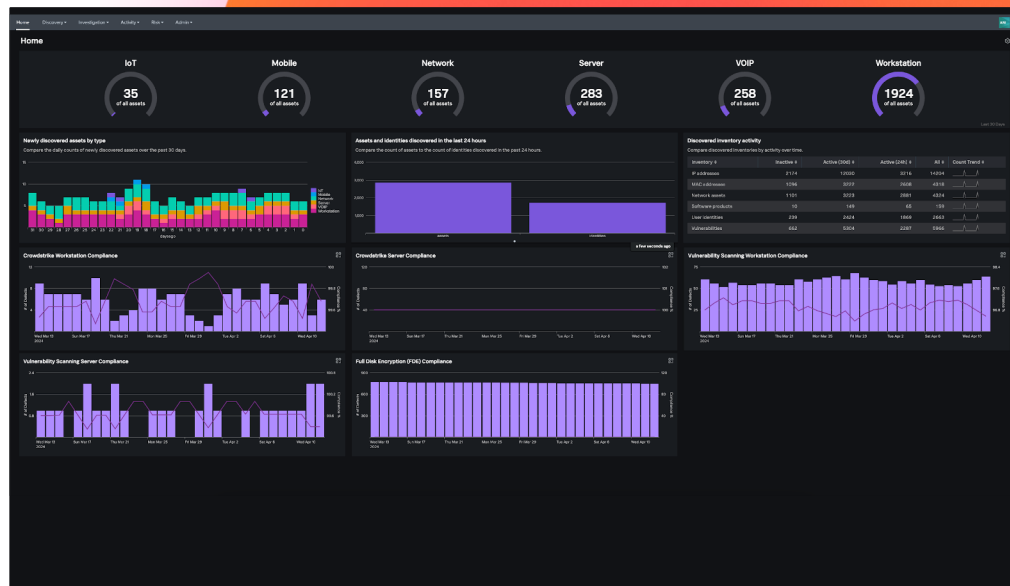
Identifikujte mezery v souladu s předpisy v bezpečnostních kontrolách



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

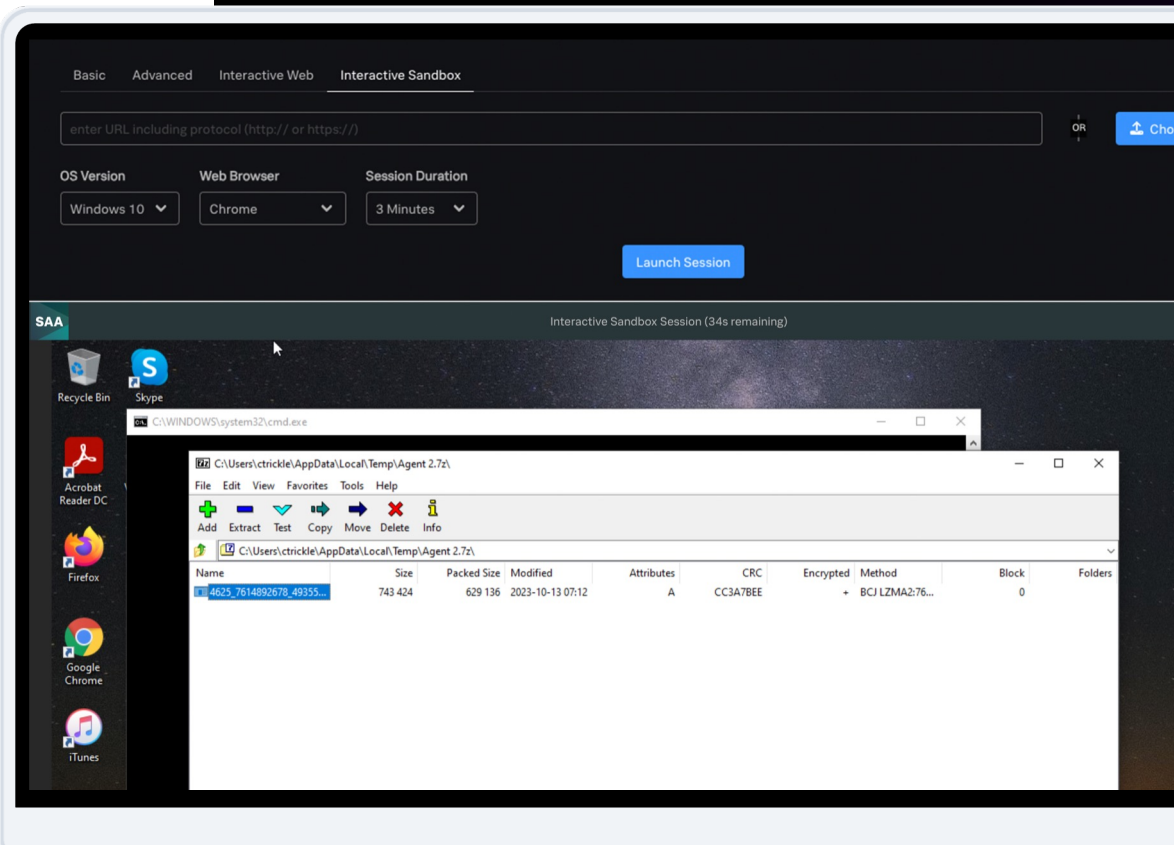


Intelligentní automatizace pro komplexní analýzu a reakci na hrozby



Bezpečně pracujte se škodlivým obsahem

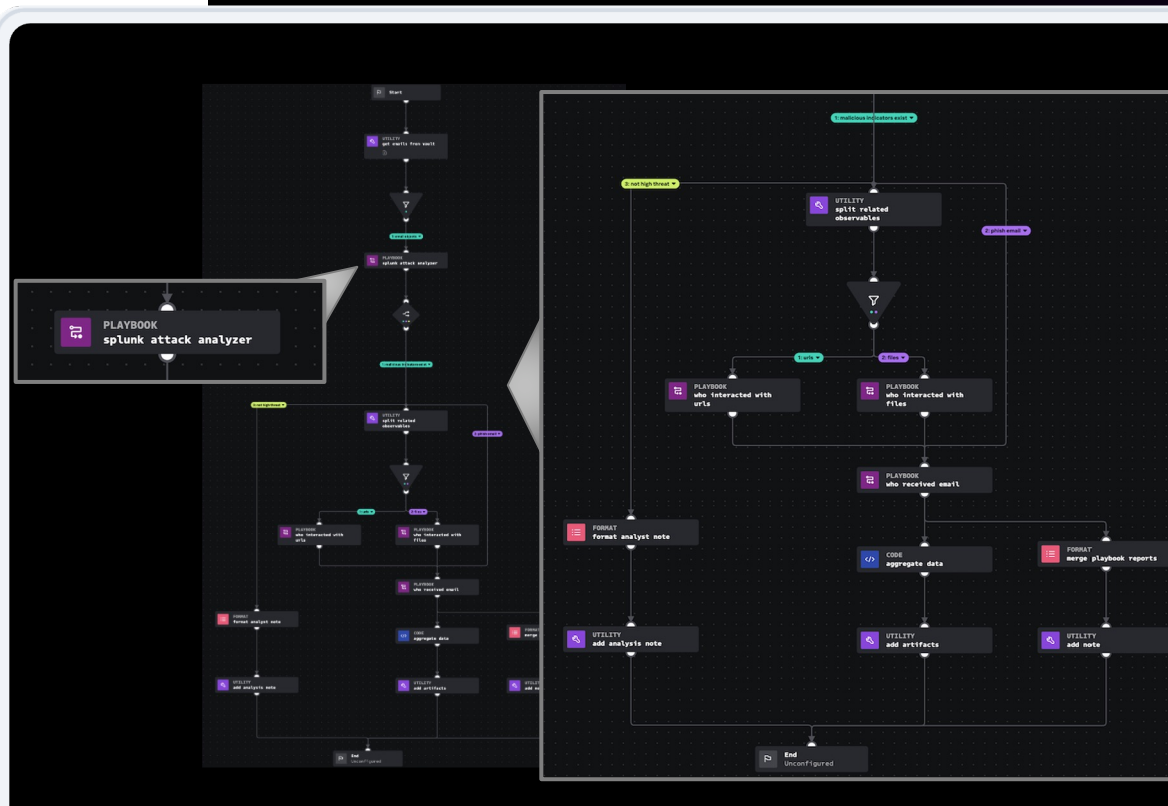
- Přistupujte ke škodlivému obsahu pocházejícímu z URL adres a souborů
- Provádějte důkladné vyšetřování a mějte jistotu, že identita analytika a společnosti zůstane skryta



Komplexní analýza a reakce

Integrujte se Splunk SOAR pro inteligentní automatizaci

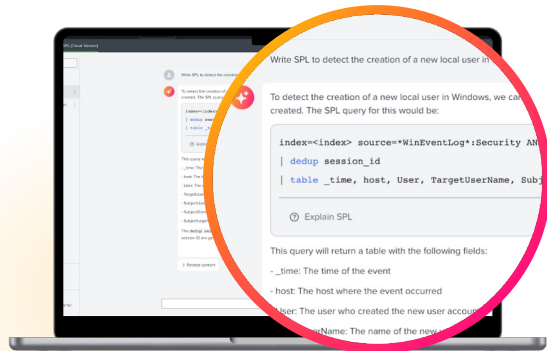
- **Provádějte automatizovanou analýzu identifikovaných indikátorů** bez nutnosti manuálních vyšetřovacích úkolů
- **Odstraňte potřebu složitých playbooků** využívajících více produktů pro analýzu hrozeb
- **Splunk SOAR spustí odpovídající playbook** poté, co Splunk Attack Analyzer potvrdí aktivní hrozbu



Splunk AI Asistenti

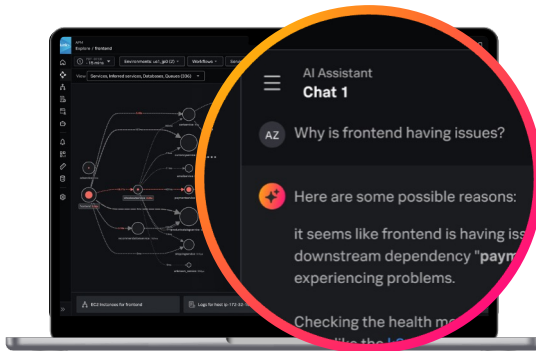
Zvyšte produktivitu, a umožněte rychlejší detekci a řešení

AI Assistant for SPL



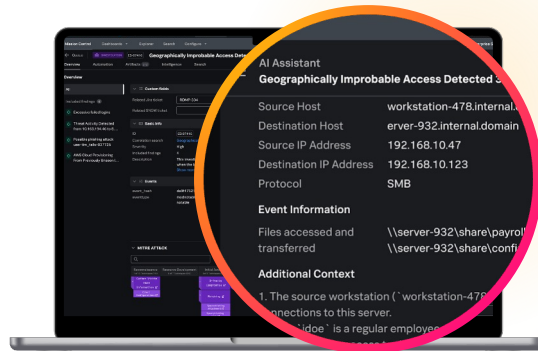
Generally Available

AI Assistant in Observability Cloud



Generally Available

AI Assistant in Enterprise Security

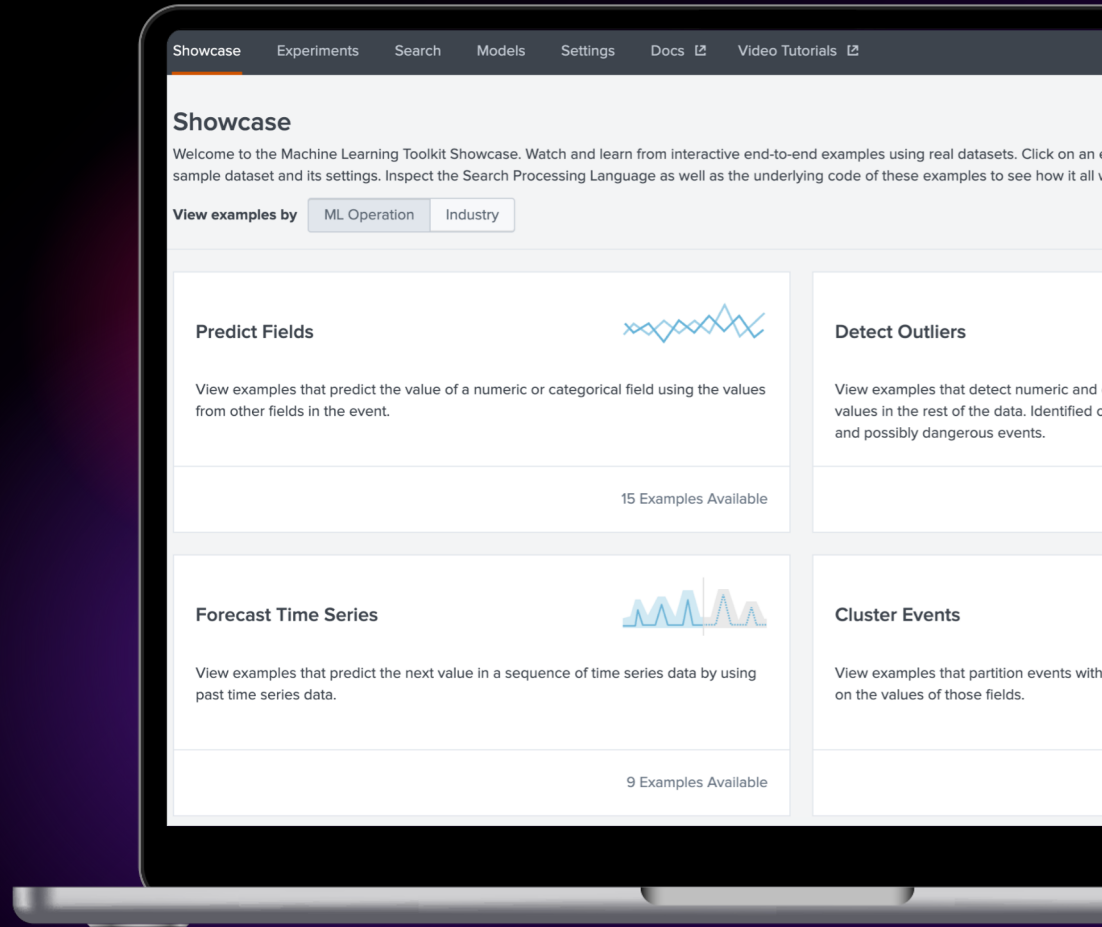


Preview

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.



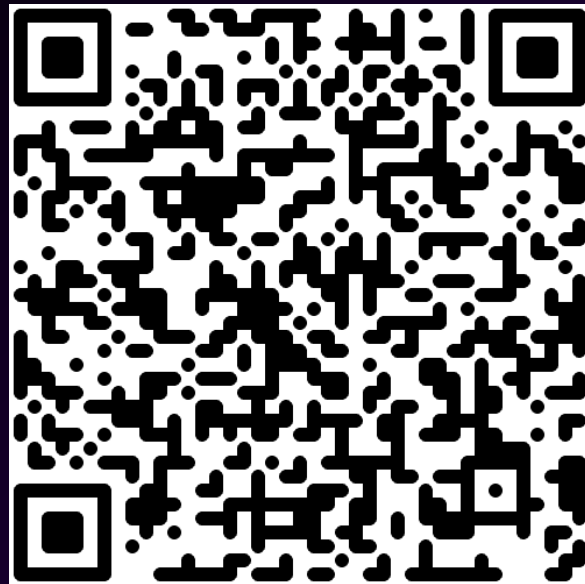
Staňte se EMEA BOTS šampionem!

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 sítí

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