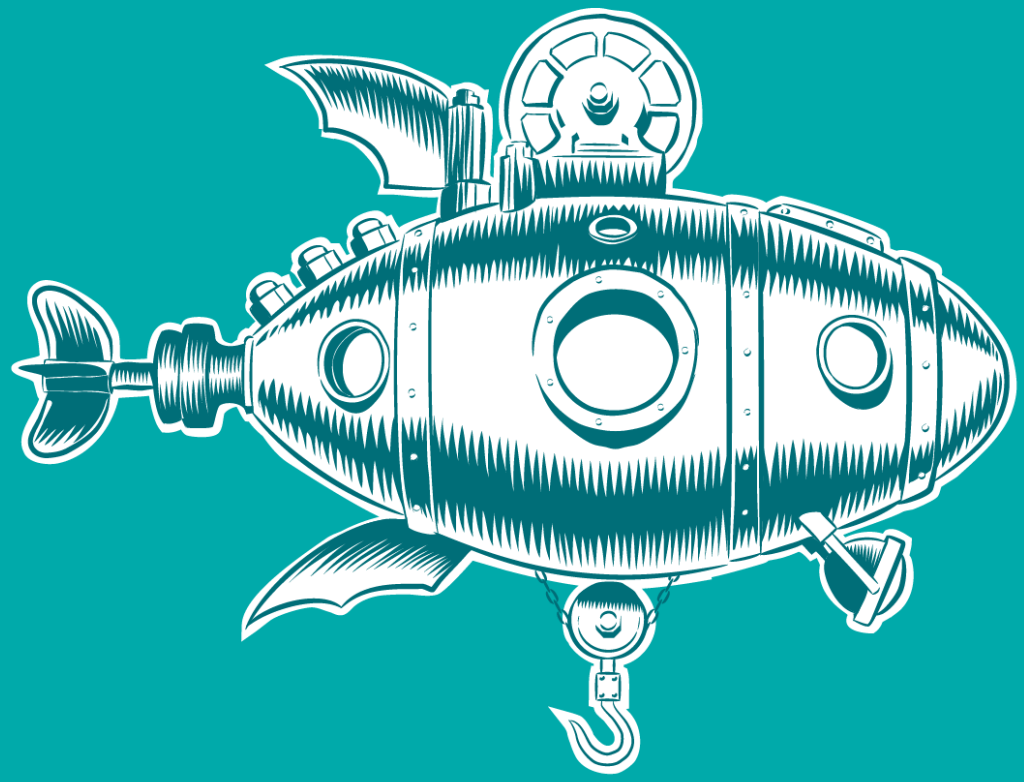
ALEF

Splunk a Cisco – spolu a silnější

Rok informatiky 2025



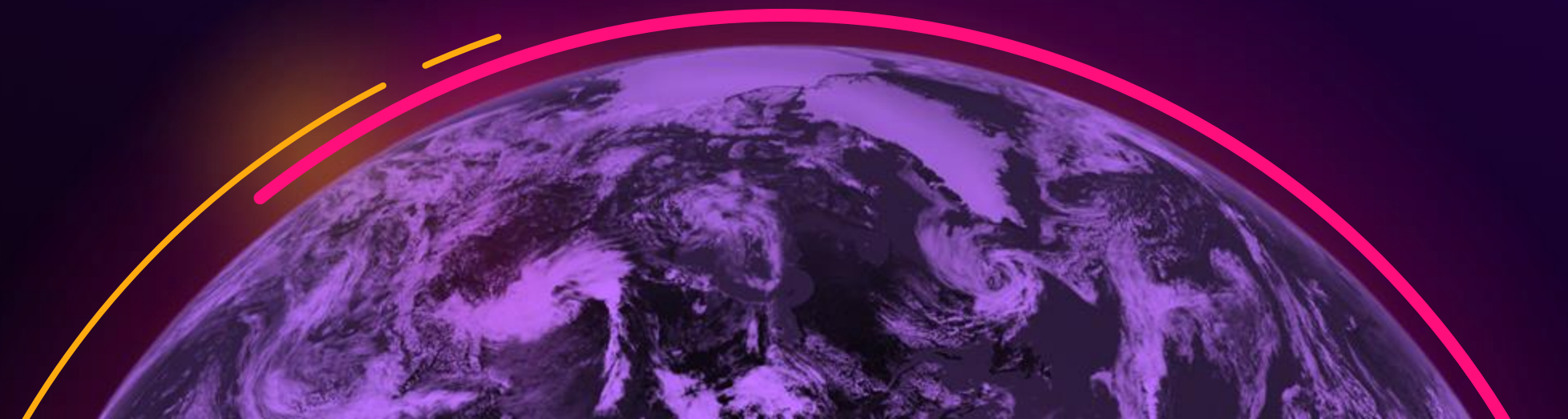
Lukáš Mečíř

Splunk/SIEM Specialist

lukas.mecir@alef.com

To power an inclusive future for all

To build a safer and more resilient digital world



THIS IS MORE THAN A VACATION UPGRADE

IT'S THE BEST FAMILY VACATION IN THE WORLD

NEIGHBORHOODS

1. Thrill Island
2. Surfside℠
3. The Hideaway
4. Central Park®
5. Chill Island℠
6. AquaDome℠
7. Royal Promenade
8. Suite Neighborhood

ICONIC THRILLS

9. Category 6 Waterpark
10. Crown's Edge
11. FlowRider®
12. Sports Court & Rock Wall
13. Lost Dunes Mini Golf

ICONIC STAYS

14. Ultimate Family Townhouse

ICONIC CHILLS

15. Hideaway Pool
16. Royal Bay℠ Pool
17. The Cove℠ Pool
18. Cloud 17℠
19. Swim & Tonic℠
20. Water's Edge & Splashaway Bay
21. The Grove at Suite Sundeck
22. The Lime and Coconut®

ICONIC WOWS

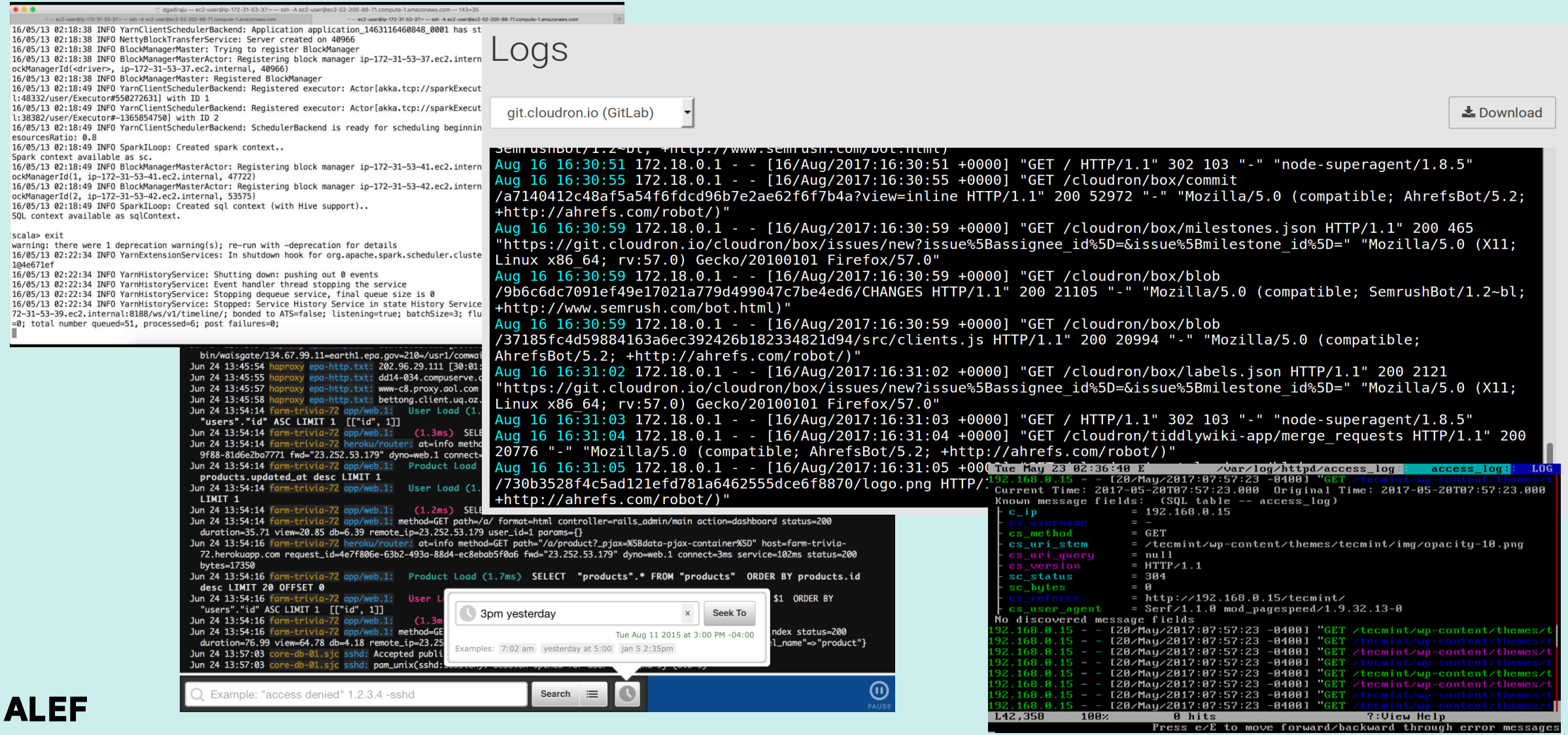
23. AquaDome℠ & AquaTheater
24. Absolute Zero℠
25. Royal Theater

DINING

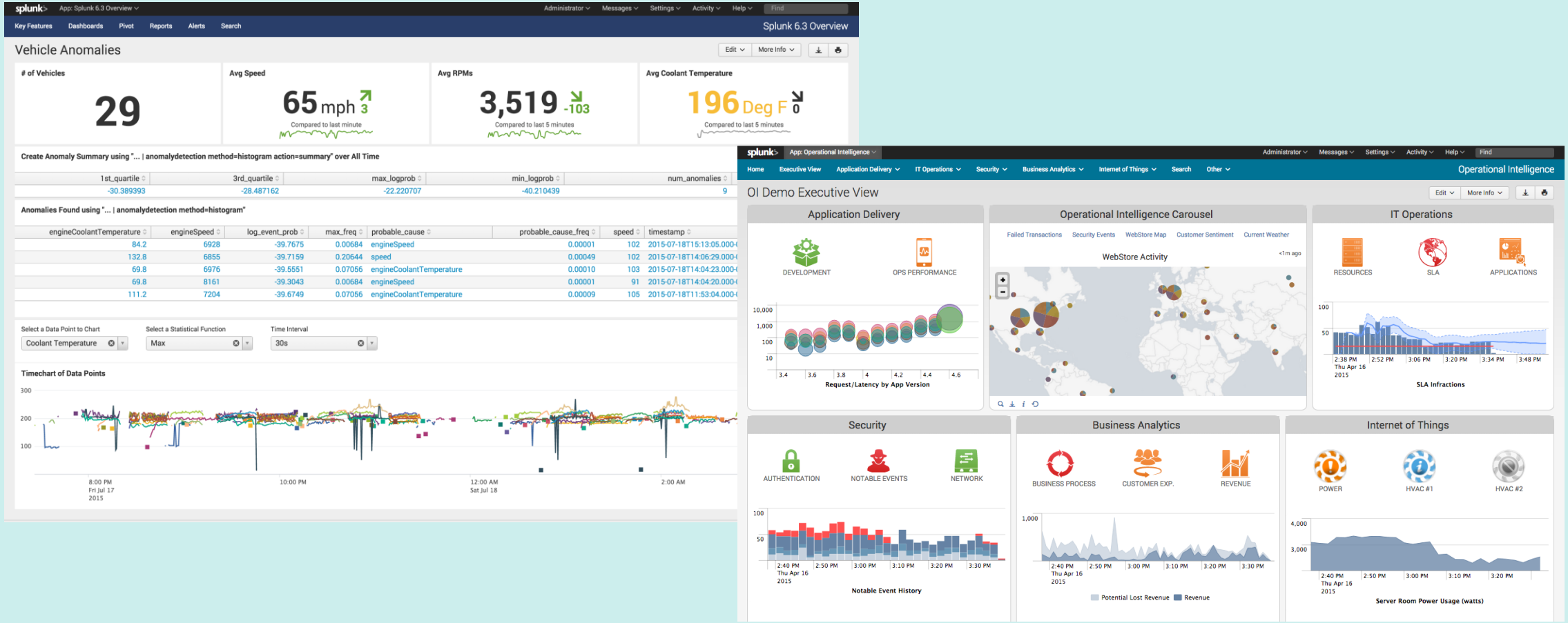
26. Dining Room
27. Windjammer Marketplace

*Images and messaging for *Icon of the Seas*℠ reflect current design concepts and may include artistic renderings and images of other class ships. Features, experiences and itineraries are subject to change without notice.

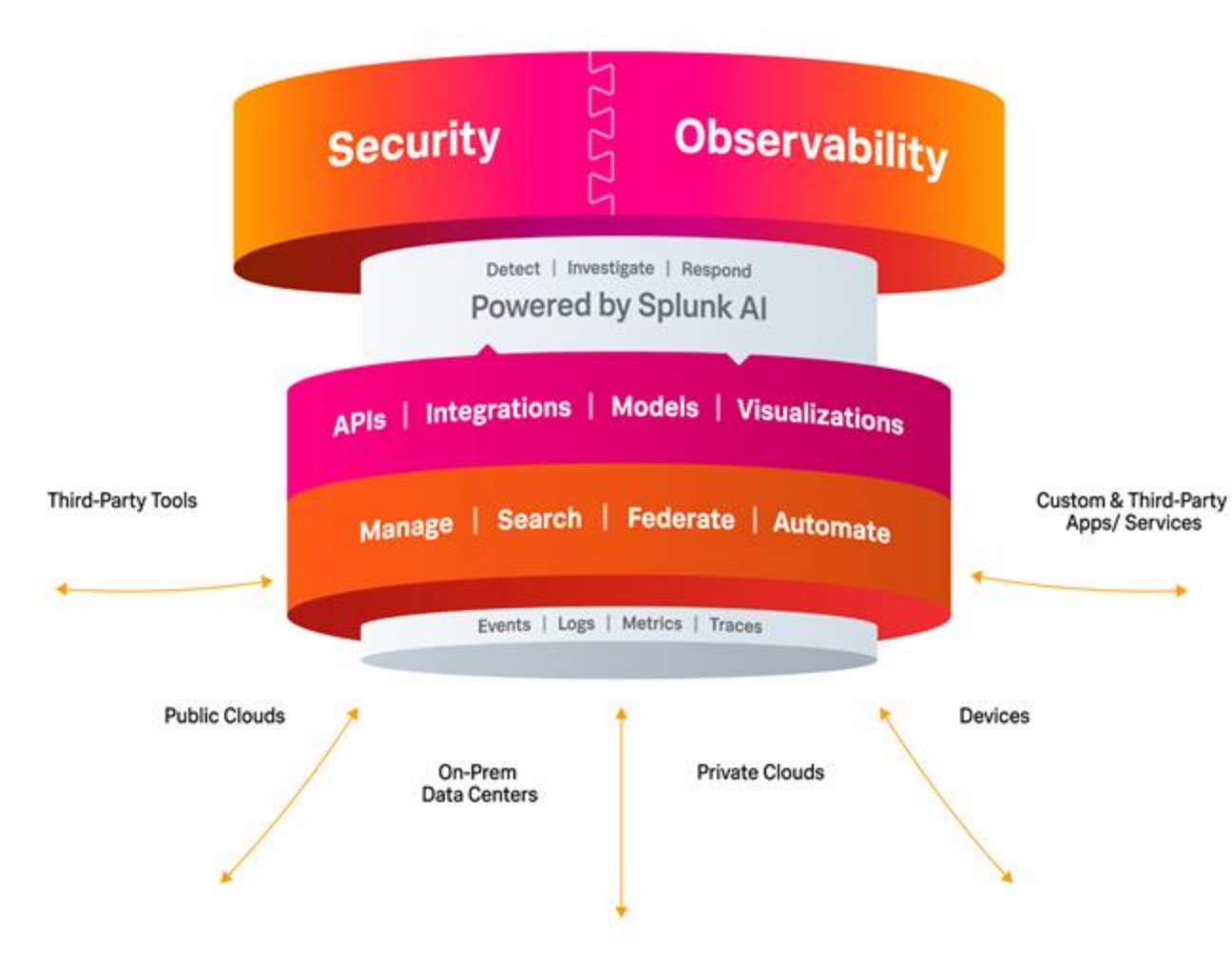
Splunk je způsob jak z tohoto...



...udělat tohle



Digital Resilience = Security + Observability



Cisco & Splunk & ALEF

- Více než 30 let zkušeností s Ciscem
- Téměř 10 let zkušeností se Splunkem
- Jeden z největších týmů Splunk v regionu CEE/SEE
- Nejvyšší (Elite) status v rámci SELL i MANAGE motions
- Nejlepší poměr ceny a hodnoty řešení
- Spolupráce s naším týmem bezpečnostních expertů (certifikováno NATO) a týmem pro Observabilitu (Cisco AppD)
- Vlastní produkty založené na Splunku (např. Alef SIEM Essential) zaměřené na malé a střední podniky

splunk> Partnerverse SELL ELITE

splunk> Partnerverse Manage ELITE

splunk> Partnerverse Security Solutions

splunk> Partnerverse Observability Solutions

splunk> Partnerverse Financial Services

Naši klienti

Moderní SOC založený na unifikované TDIR platformě

Flexible Deployment Models

Unified Worksurface
Workflows | Case Management | Dashboards

Threat Detection
Static | Dynamic (ML) | Pre-Built | Custom | Authoring

Investigation
Alert Driven | Risk Based | Hunting | Integrated Analysis

Response
Enrichment | Automation | Orchestration | Playbooks

GenAI for SecOps
Summarization | Natural Language Search | Investigation | Reporting

Common Services
Assets & Identities | Threat Intelligence | Risk

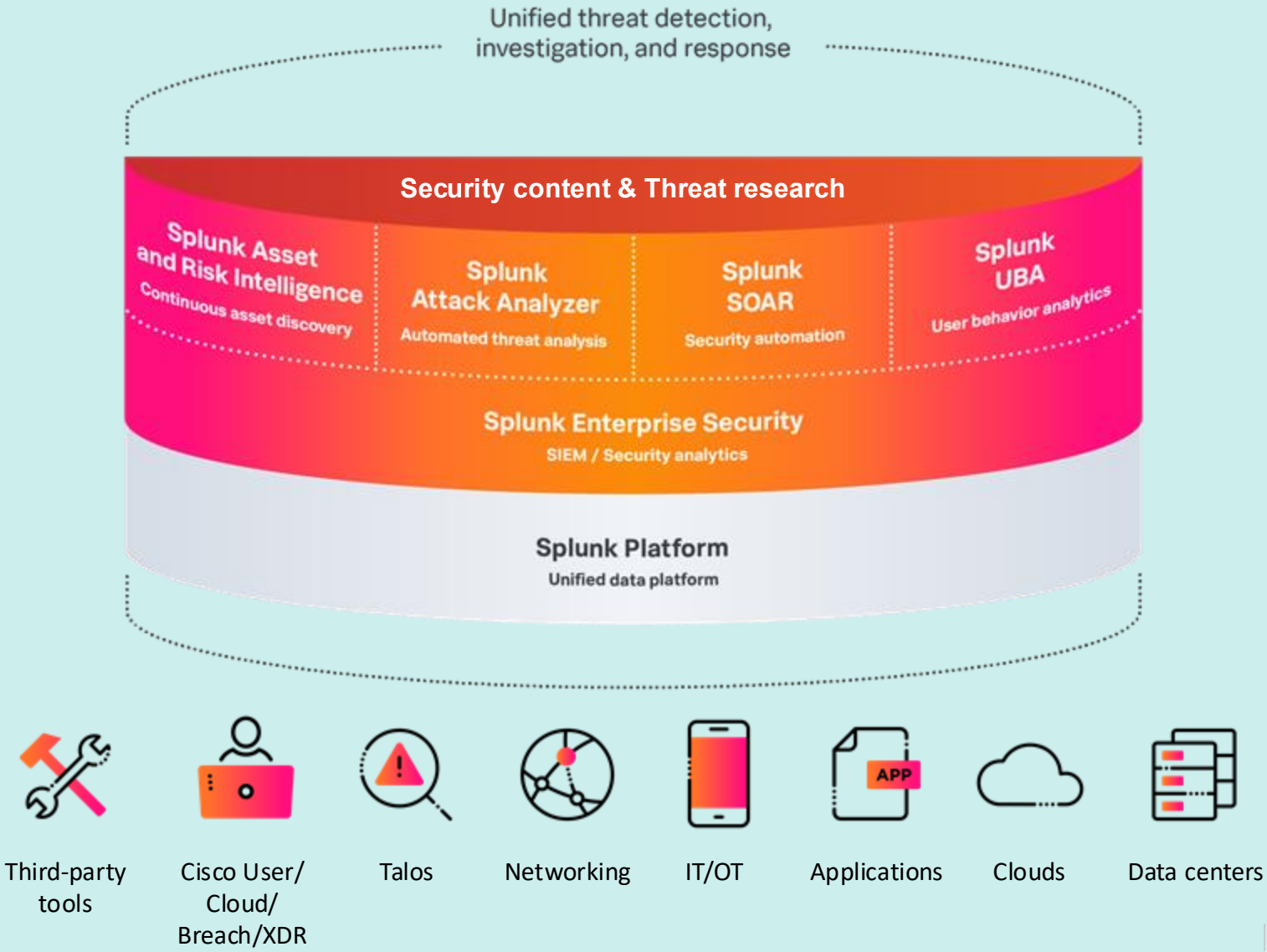
Data Access & Management
Filter | Mask | Route | Federation

True Multi-Vendor

Logs | **Events** | **Alerts** | **Telemetry**

ALEF

Splunk TDIR portfolio



Integrace v oblasti bezpečnosti

Splunk Enterprise Security + Cisco XDR

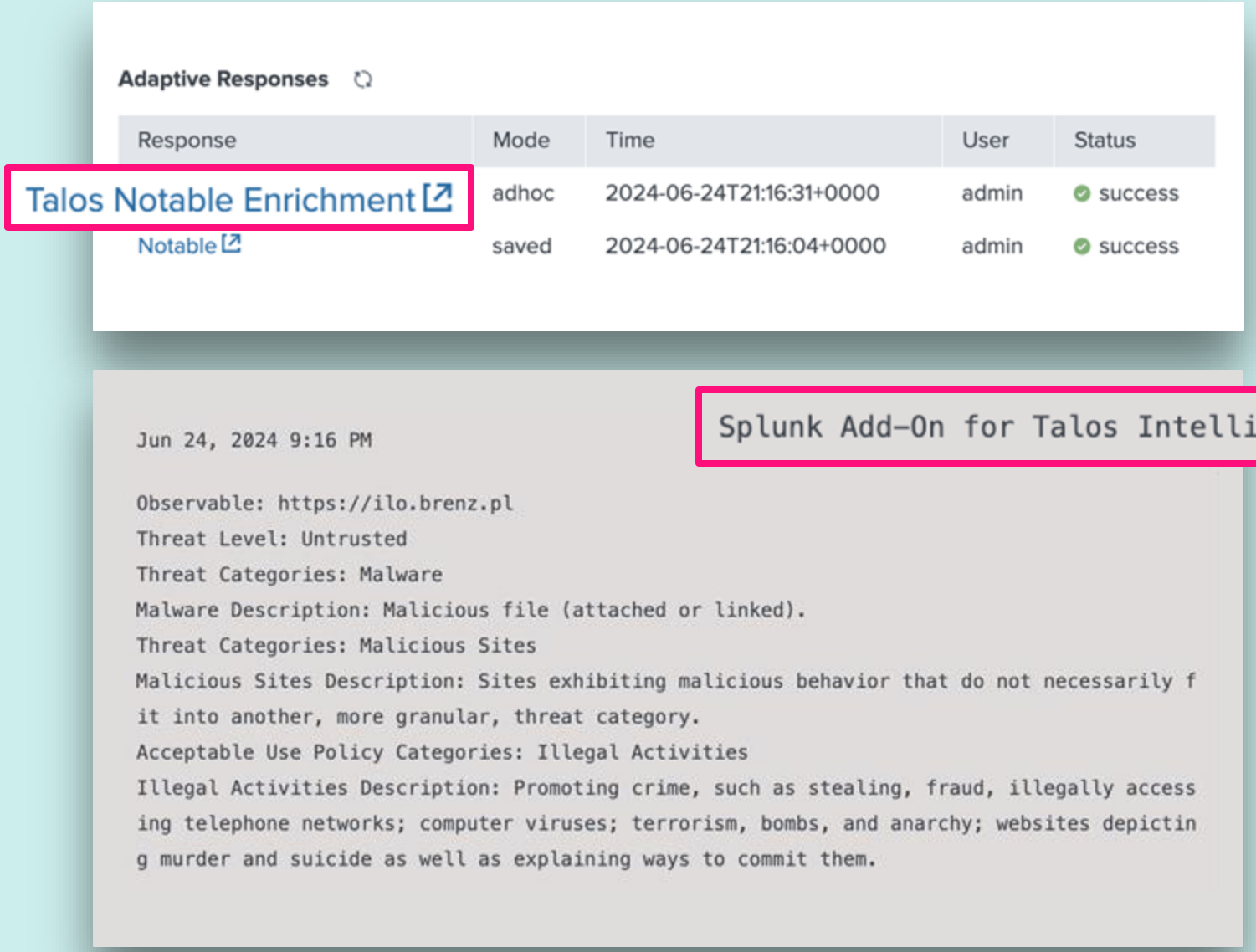
Urychlení vyšetřování a reakce

Splunk + Cisco Talos Threat Intelligence

Obohacení dat o Threat Intelligence informace

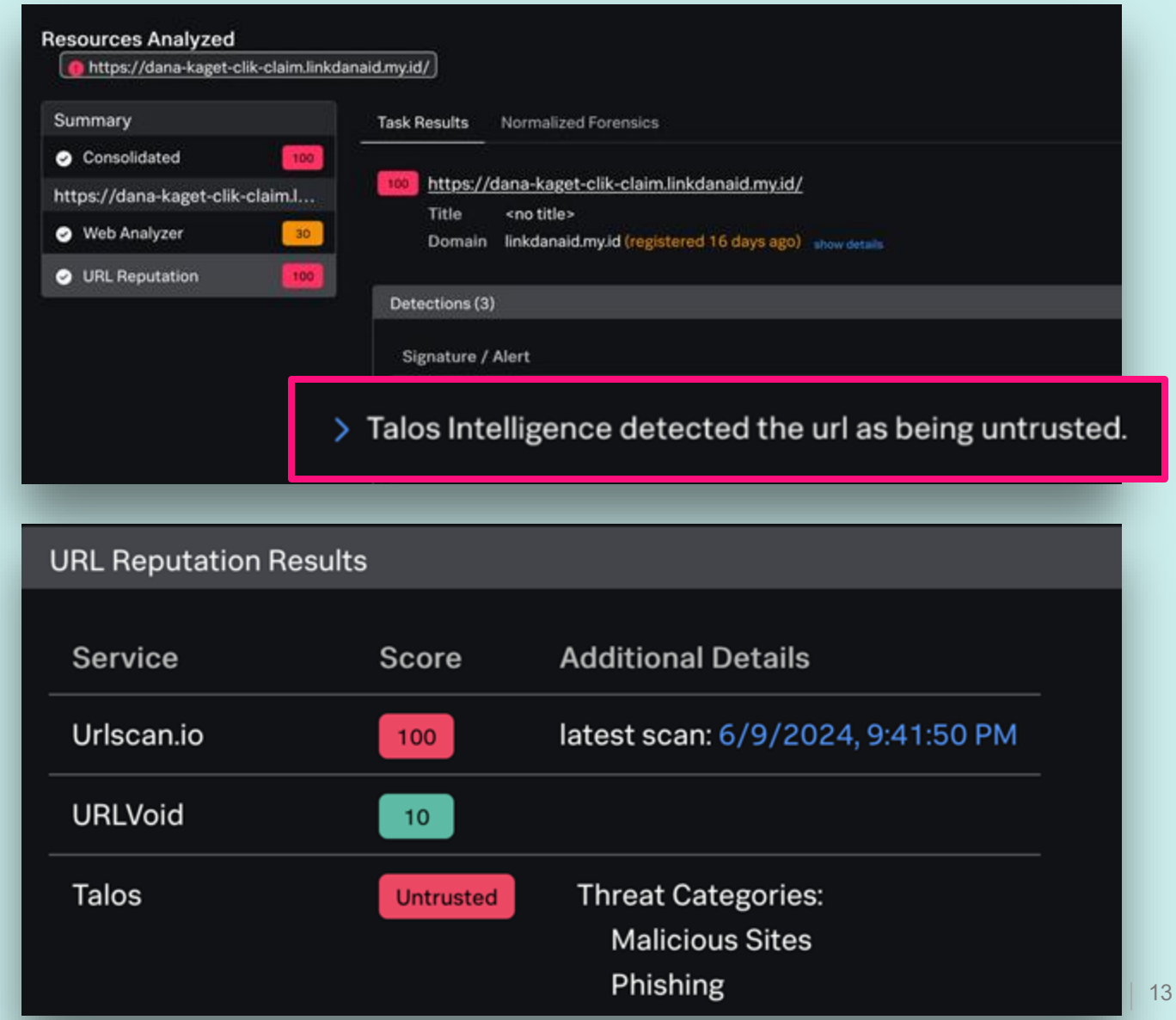
Splunk Add-on for Talos Intelligence

- **Out-of-the-box** adaptive response action
- **Dostupné zdarma** pro všechny uživatele Splunk SIEM
- **Bohatý zdroj informací** o množství IoC



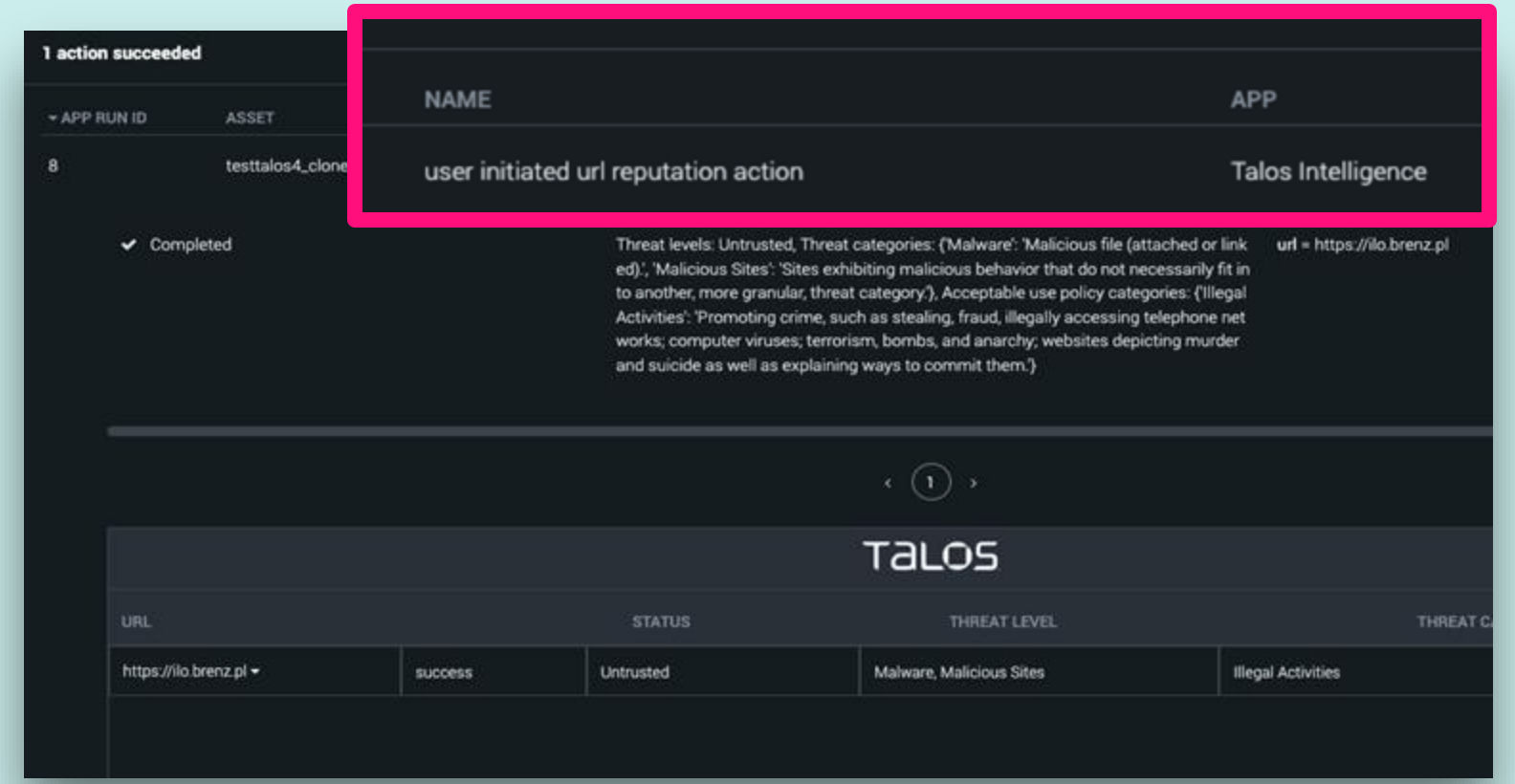
Talos Threat Intelligence for Splunk Attack Analyzer

- **Automatická integrace do Splunk Attack Analyzeru** – není nutná žádná uživatelská akce
- Obohacuje získaná data o reputační skóre (URL, soubory apod.)



Talos Intelligence Connector for SOAR

- **Out-of-the-box** konektor pro Splunk SOAR
- **Dostupné zdarma** pro všechny uživatele Splunk SOAR
- **Integruje Talos threat intelligence** přímo do incident response workflow



NIS2 požadavky

Detekce kybernetických bezpečnostních událostí

Hlášení kybernetických bezpečnostních událostí

- Do **24 hodin** (včasné varování)
- Do **72 hodin** (prvotní posouzení)
- Vyšší režim - **všechny** incidenty
- Nižší režim - pouze **významné** incidenty

Řešení kybernetických bezpečnostních událostí

NIS2 a Splunk

NIS2 požadavek	Splunk řešení
Detekce incidentů	Splunk Enterprise Security
	Splunk UBA
	Splunk Threat Research and Content Update
Vyšetřování, hlášení incidentů	Splunk Enterprise Security
	Splunk Attack Analyzer
	Splunk SOAR
Řešení incidentů	Splunk Enterprise Security
	Splunk SOAR

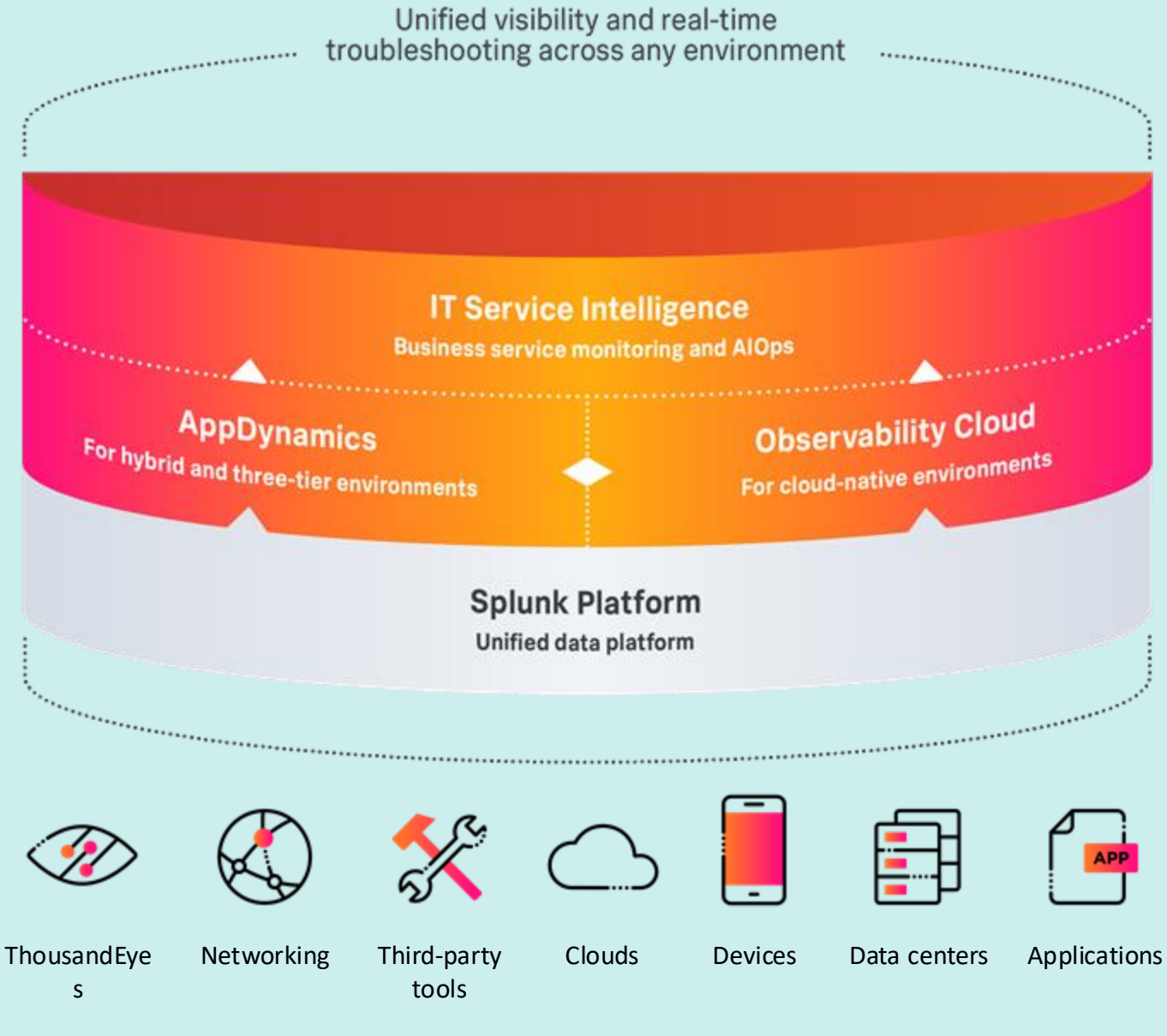
Splunk observabilita

Celkový přehled o funkčnosti infrastruktury
bez ohledu na prostředí a použité aplikace

Včasná detekce & rychlé vyšetřování
problémů, vedoucích k narušení funkčnosti

Efektivnější kontrola
dat a nákladů

Ucelený přehled o stavu celé infrastruktury



Cisco + Splunk integrace v observabilitě

AppDynamics + Splunk Platform

Rychlý a spolehlivý troubleshooting

Integrace logů ze Splunk Platform do AppDynamics pro získání kompletního přehledu o problému, urychlení jeho vyšetření a nalezení příčiny

AppDynamics + Observability Cloud

Integrovaný dohled nad heterogenním prostředím

Integrace AppDynamics & Splunk Observability Cloud pro integrovaný dohled nad heterogenním prostředím, které zahrnuje tradiční i cloudové aplikace

AppDynamics + IT Service Intelligence

End-to-end přehled o stavu IT infrastruktury

Integrace alertů & síťové telemetrie z AppDynamics do Splunk IT Service Intelligence - zvýšení relevance alertů & vazba mezi stavem IT a funkčností

ALEF

Děkuji za pozornost