



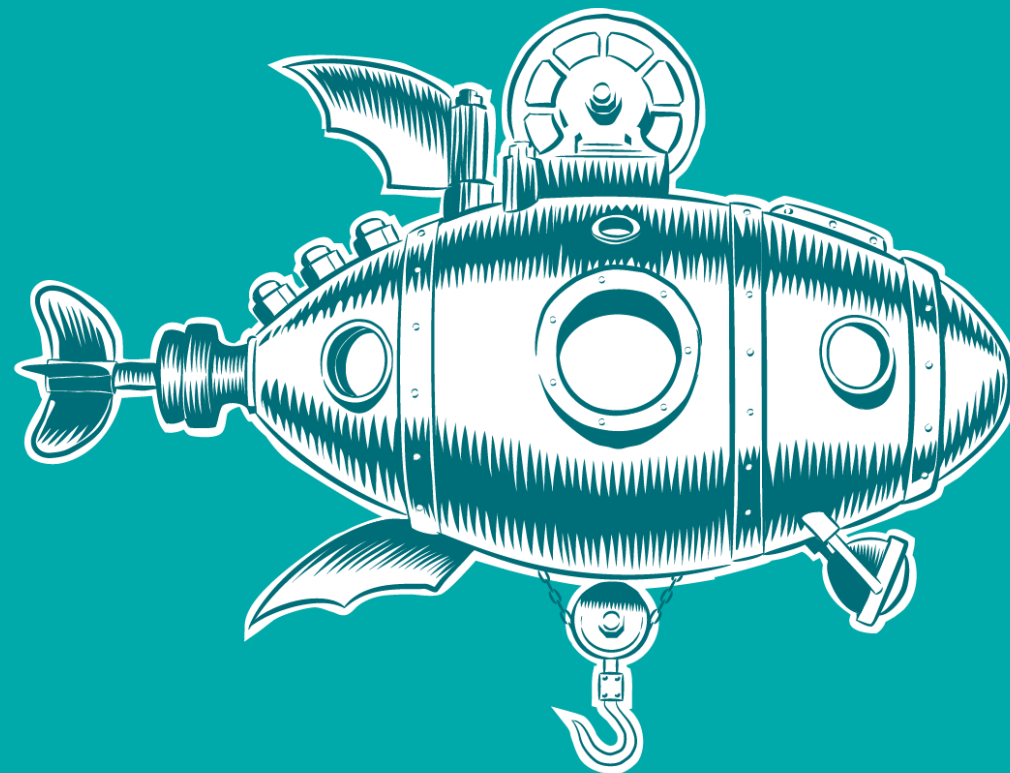
Splunk a Cisco – spolu a silnější

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. SurfsideSM
3. The Hideaway
4. Central Park[®]
5. Chill IslandSM
6. AquaDomeSM
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 BaySM Pool
17. The CoveSM Pool
18. Cloud 17SM
19. Swim & TonicSM
20. Water's Edge & Splashaway Bay
21. The Grove at Suite Sundek
22. The Lime and Coconut[®]

ICONIC WOWS

23. AquaDomeSM & AquaTheater
24. Absolute ZeroSM
25. Royal Theater

DINING

26. Dining Room
27. Windjammer Marketplace

*Images and messaging for Icon of the SeasSM 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...

Logs

git.cloudron.io (GitLab)

Download

```
Aug 16 16:30:51 172.18.0.1 - - [16/Aug/2017:16:30:51 +0000] "GET / HTTP/1.1" 302 103 "-" "node-superagent/1.8.5"
Aug 16 16:30:55 172.18.0.1 - - [16/Aug/2017:16:30:55 +0000] "GET /cloudron/box/commit/a7140412c48af5a54f6dcd96b7e2ae62f6f7b4a?view=inline HTTP/1.1" 200 52972 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)"
Aug 16 16:30:59 172.18.0.1 - - [16/Aug/2017:16:30:59 +0000] "GET /cloudron/box/milestones.json HTTP/1.1" 200 465
"https://git.cloudron.io/cloudron/box/issues/new?issue%5Bassignee_id%5D=&issue%5Bmilestone_id%5D=" "Mozilla/5.0 (X11; Linux x86_64; rv:57.0) Gecko/20100101 Firefox/57.0"
Aug 16 16:30:59 172.18.0.1 - - [16/Aug/2017:16:30:59 +0000] "GET /cloudron/box/blob/9b6c6dc7091ef49e17021a779d499047c7be4ed6/CHANGES HTTP/1.1" 200 21105 "-" "Mozilla/5.0 (compatible; SemrushBot/1.2-bl; +http://www.semrush.com/bot.html)"
Aug 16 16:30:59 172.18.0.1 - - [16/Aug/2017:16:30:59 +0000] "GET /cloudron/box/blob/37185fc4d59884163a6ec392426b182334821d94/src/clients.js HTTP/1.1" 200 20994 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)"
Aug 16 16:31:02 172.18.0.1 - - [16/Aug/2017:16:31:02 +0000] "GET /cloudron/box/labels.json HTTP/1.1" 200 2121
"https://git.cloudron.io/cloudron/box/issues/new?issue%5Bassignee_id%5D=&issue%5Bmilestone_id%5D=" "Mozilla/5.0 (X11; Linux x86_64; rv:57.0) Gecko/20100101 Firefox/57.0"
Aug 16 16:31:03 172.18.0.1 - - [16/Aug/2017:16:31:03 +0000] "GET / HTTP/1.1" 302 103 "-" "node-superagent/1.8.5"
Aug 16 16:31:04 172.18.0.1 - - [16/Aug/2017:16:31:04 +0000] "GET /cloudron/tiddlywiki-app/merge_requests HTTP/1.1" 200 20776 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)"
Aug 16 16:31:05 172.18.0.1 - - [16/Aug/2017:16:31:05 +0000] "GET /730b3528f4c5ad121efd781a6462555dce6f8870/logo.png HTTP/1.1" 200 1024 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)"
```

```
bin/waisgate/134.67.99.11=earth1.epa.gov=210=/usr1/comwa
Jun 24 13:45:54 haproxy epa-http.txt: 202.96.29.111 [30:01:
Jun 24 13:45:55 haproxy epa-http.txt: dd14-034.comuserve.d
Jun 24 13:45:57 haproxy epa-http.txt: www-c8.proxy.aol.com
Jun 24 13:45:58 haproxy epa-http.txt: bettong.client.uq.oz
Jun 24 13:54:14 farm-trivia-72 app/web.1: User Load (1.1
"users"."id" ASC LIMIT 1 ["id", 1]]
Jun 24 13:54:14 farm-trivia-72 app/web.1: (1.3ms) SEL
Jun 24 13:54:14 farm-trivia-72 heroku/router: at=info metho
9f88-81d6e2ba7771 fwd="23.252.53.179" dyno=web.1 connect=
Jun 24 13:54:14 farm-trivia-72 app/web.1: Product Load
products.updated_at desc LIMIT 1
Jun 24 13:54:14 farm-trivia-72 app/web.1: User Load (1.1
LIMIT 1
Jun 24 13:54:14 farm-trivia-72 app/web.1: (1.2ms) SEL
Jun 24 13:54:14 farm-trivia-72 app/web.1: method=GET path=/a/ format=html controller=rails.admin/main action=dashboard status=200
duration=35.71 view=20.85 db=6.39 remote_ip=23.252.53.179 user_id=1 params={}
Jun 24 13:54:16 farm-trivia-72 heroku/router: at=info method=GET path="/a/product?_pjax=%5Bdata-pjax-container%5D" host=farm-trivia-72.herokuapp.com request_id=4e7f806e-63b2-493a-88d4-ec8ebab5f0a6 fwd="23.252.53.179" dyno=web.1 connect=3ms service=102ms status=200 bytes=17350
Jun 24 13:54:16 farm-trivia-72 app/web.1: Product Load (1.7ms) SELECT "products".* FROM "products" ORDER BY products.id desc LIMIT 20 OFFSET 0
Jun 24 13:54:16 farm-trivia-72 app/web.1: User Load (1.1
"users"."id" ASC LIMIT 1 ["id", 1]]
Jun 24 13:54:16 farm-trivia-72 app/web.1: (1.3ms) SEL
Jun 24 13:54:16 farm-trivia-72 app/web.1: method=GET path=/a/ format=html controller=rails.admin/main action=dashboard status=200
duration=76.99 view=64.78 db=4.18 remote_ip=23.252.53.179 user_id=1 params={}
Jun 24 13:57:03 core-db-01.sjc sshd: Accepted publickey for root from 10.0.0.1 port 22 ssh2
Jun 24 13:57:03 core-db-01.sjc sshd: pam_unix(sshd:session) session opened for user root by root
```

3pm yesterday

Tue Aug 11 2015 at 3:00 PM -04:00

Examples: 7:02 am yesterday at 5:00 jan 5 2:35pm

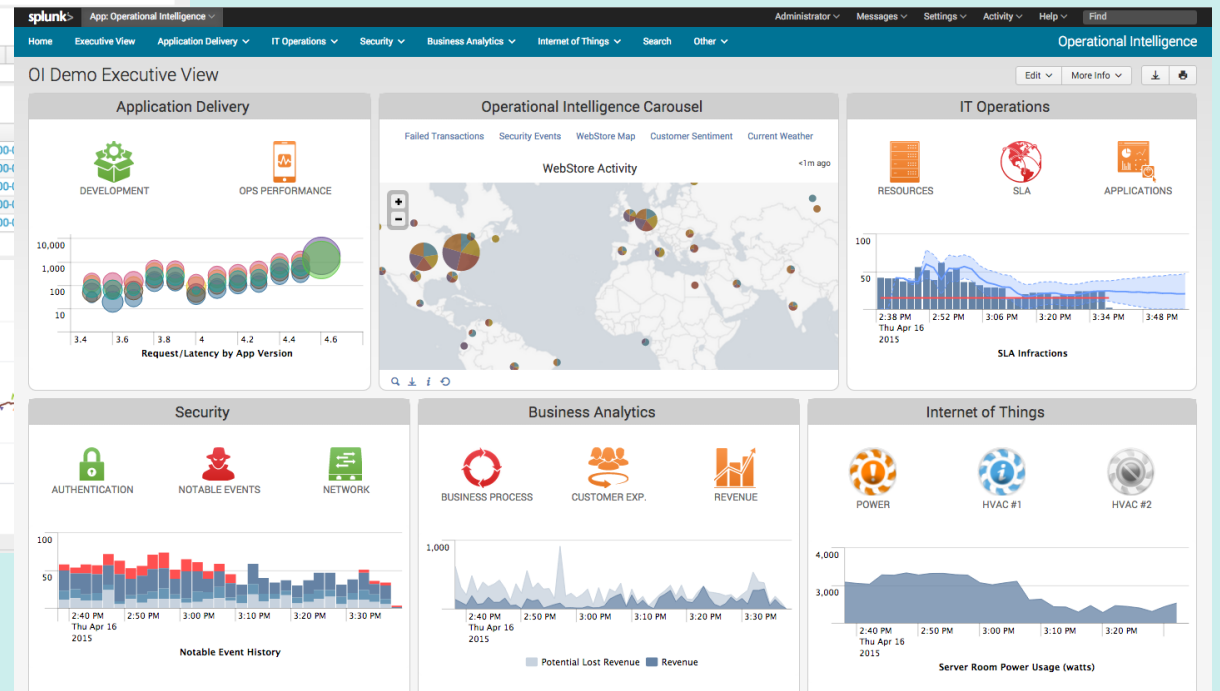
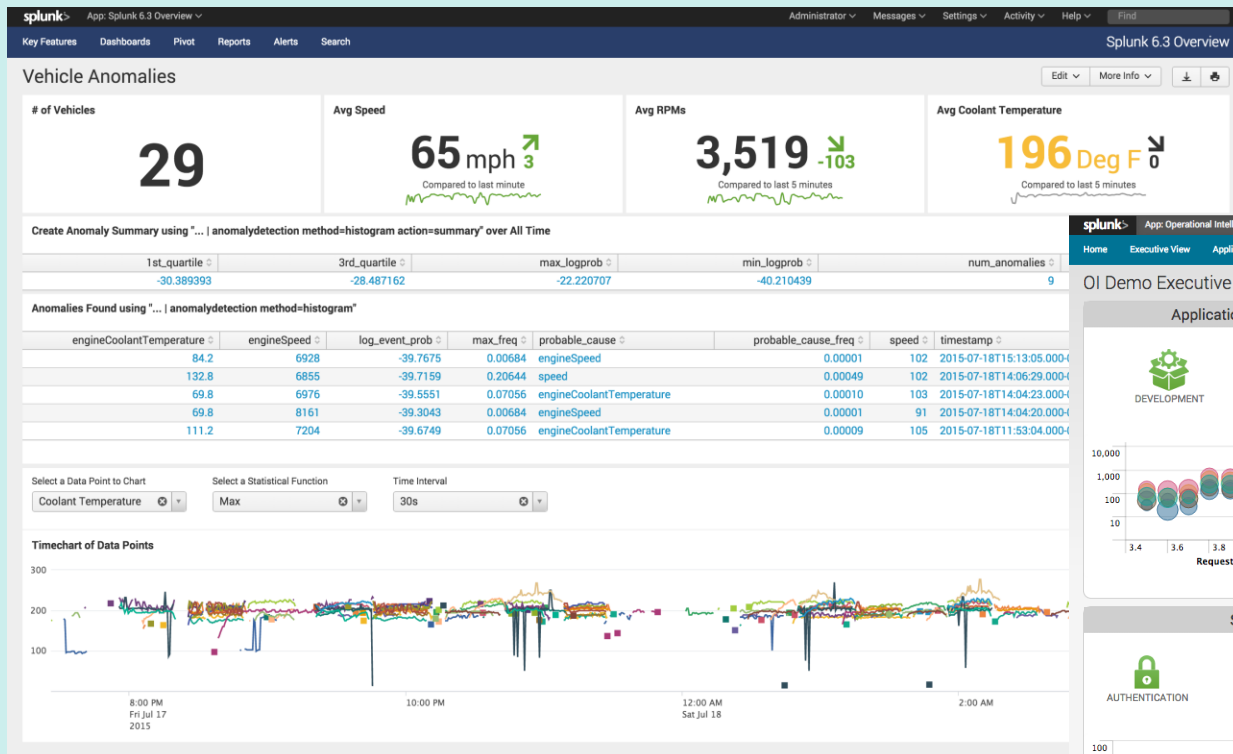
Example: "access denied" 1.2.3.4 -sshd

Search

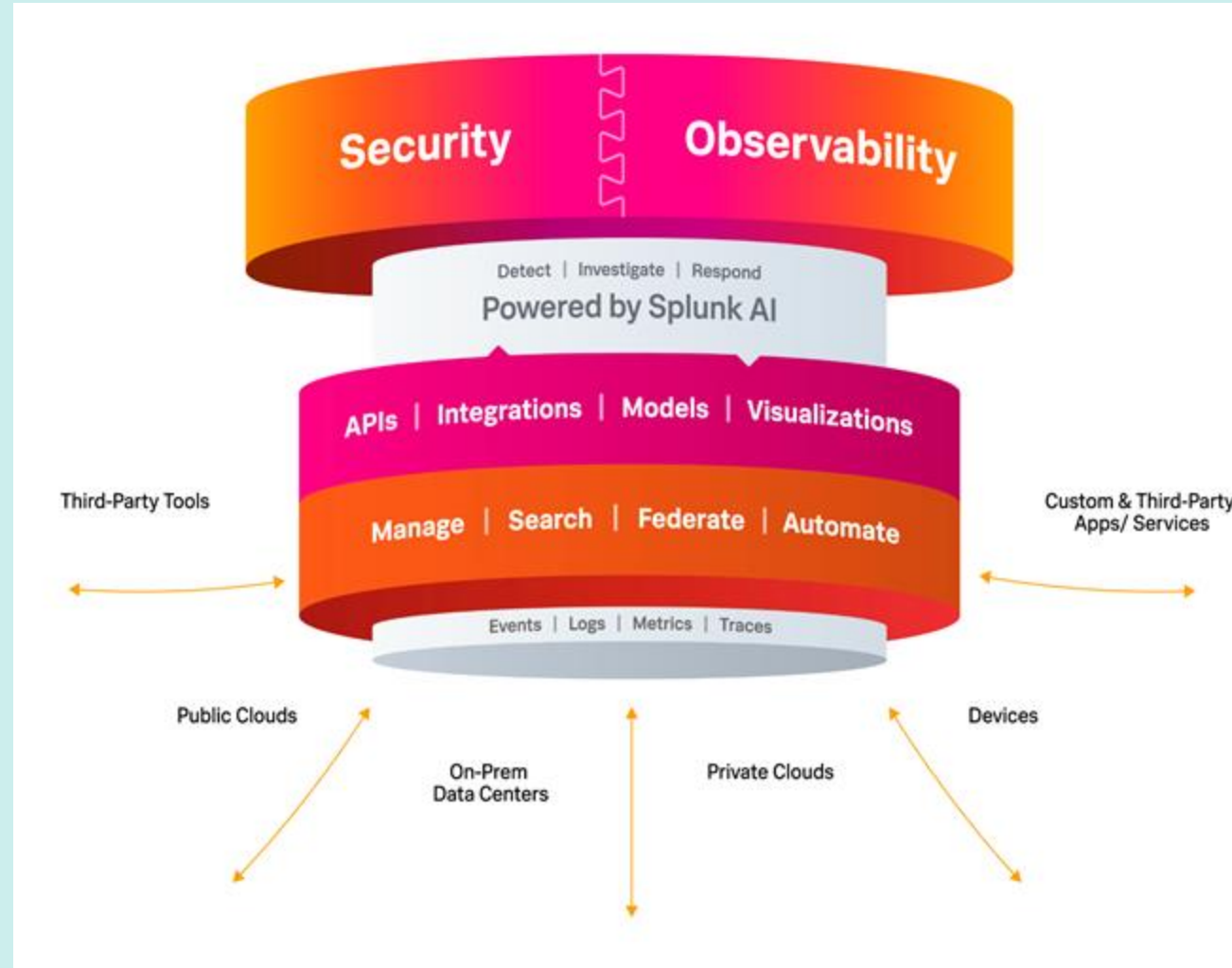


```
Tue May 23 02:36:40 E /var/log/httpd/access_log: access_log: LOG
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
Current Time: 2017-05-20T07:57:23.000 Original Time: 2017-05-20T07:57:23.000
Known message fields: (SQL table -- access_log)
c_ip = 192.168.0.15
cs_username =
cs_method = GET
cs_uri_stem = /tecmin/wp-content/themes/tecmin/img/opacity-10.png
cs_uri_query = null
cs_version = HTTP/1.1
sc_status = 304
sc_bytes = 0
cs_referer = http://192.168.0.15/tecmin/
cs_user_agent = Serf/1.1.0 mod_pagespeed/1.9.32.13-0
No discovered message fields
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
192.168.0.15 - - [20/May/2017:07:57:23 -0400] "GET /tecmin/wp-content/themes/t
142.358 100% 0 hits ?View Help
Press e/E to move forward/backward through error messages
```

...udělat tohle

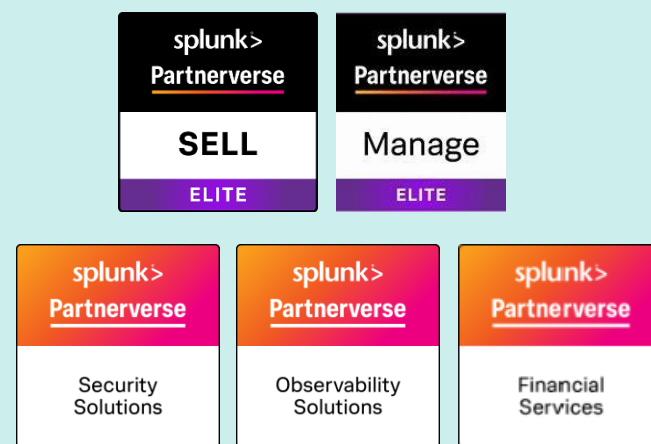


Digital Resilience = Security + Observability



Cisco & Splunk & ALEF

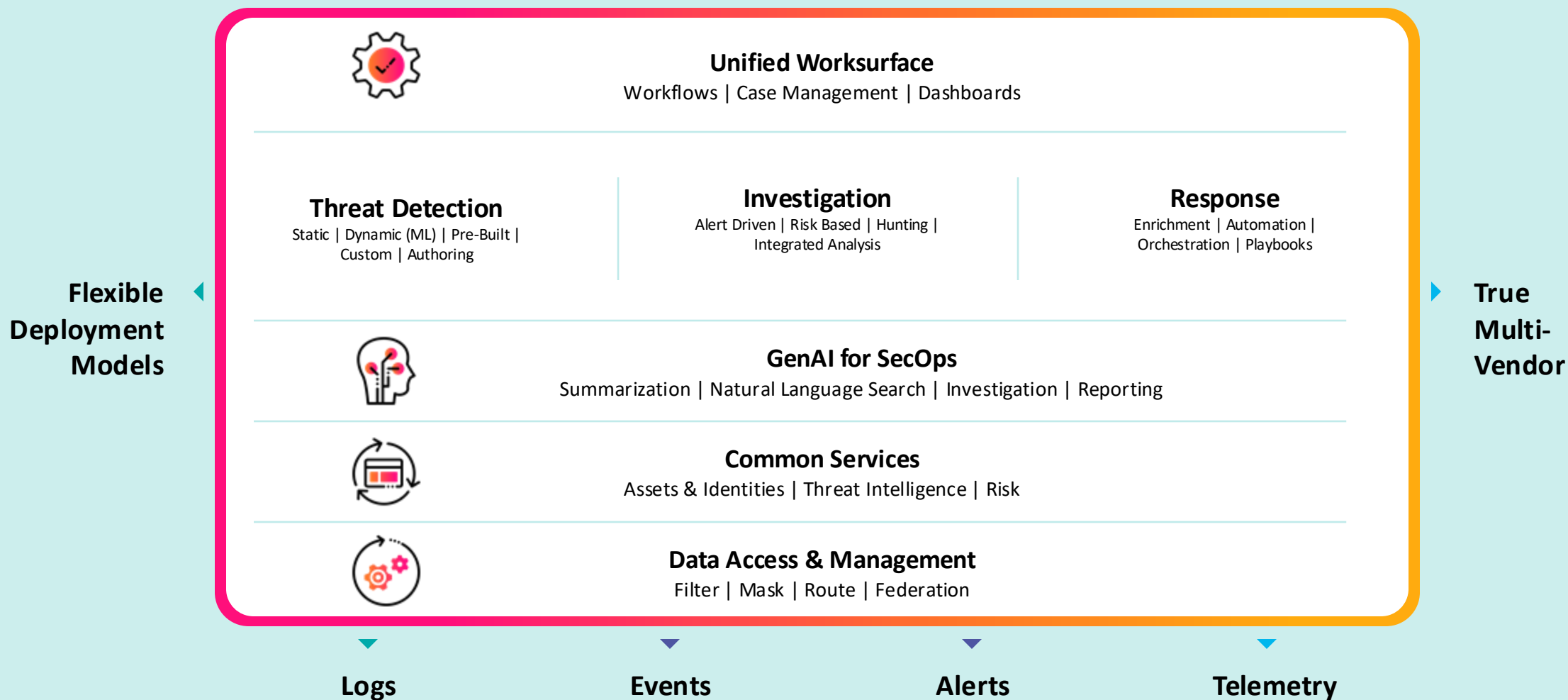
- Více než 30 let zkušeností s Ciscem
- Téměř 10 let zkušeností se Splunkem
- Jeden z největších týmů Splunk v regionu CEE/SEE
- Nejvyšší (Elite) status v rámci SELL i MANAGE motions
- Nejlepší poměr ceny a hodnoty řešení
- Spolupráce s naším týmem bezpečnostních expertů (certifikováno NATO) a týmem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



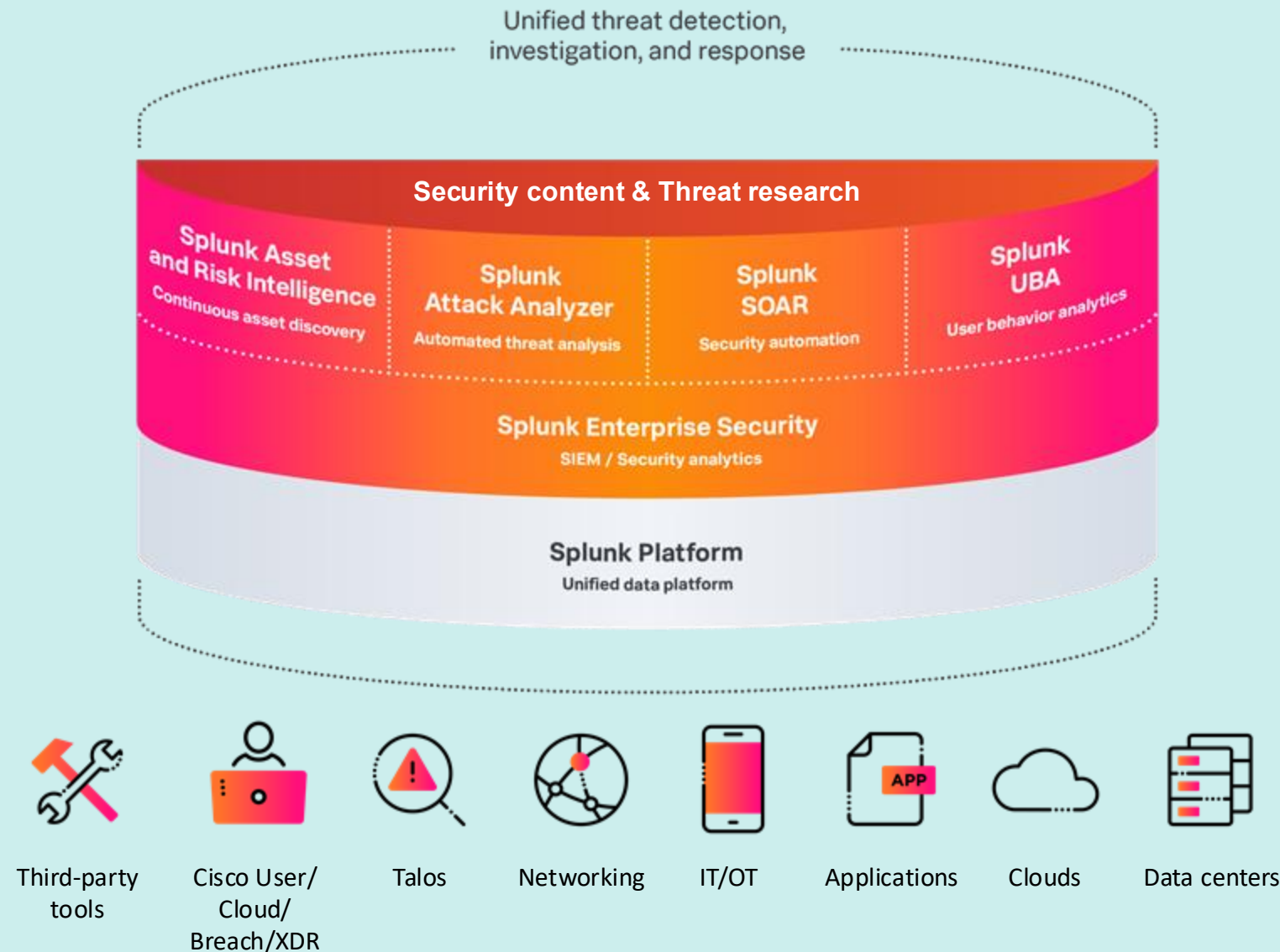
Naši klienti



Moderní SOC založený na unifikované TDIR platformě



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

Adaptive Responses

Response	Mode	Time	User	Status
Talos Notable Enrichment	adhoc	2024-06-24T21:16:31+0000	admin	✓ success
Notable	saved	2024-06-24T21:16:04+0000	admin	✓ success

Jun 24, 2024 9:16 PM

Splunk Add-On for Talos Intelligence

Observable: <https://ilo.brenz.pl>
Threat Level: Untrusted
Threat Categories: Malware
Malware Description: Malicious file (attached or linked).
Threat Categories: Malicious Sites
Malicious Sites Description: Sites exhibiting malicious behavior that do not necessarily fit into another, more granular, threat category.
Acceptable Use Policy Categories: Illegal Activities
Illegal Activities Description: Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.

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.)

Resources Analyzed

<https://dana-kaget-клик-claim.linkdanaid.my.id/>

Summary

- Consolidated 100
- Web Analyzer 30
- URL Reputation 100

Task Results

Normalized Forensics

100 <https://dana-kaget-клик-claim.linkdanaid.my.id/>

Title <no title>

Domain linkdanaid.my.id (registered 16 days ago) [show details](#)

Detections (3)

Signature / Alert

> Talos Intelligence detected the url as being untrusted.

URL Reputation Results		
Service	Score	Additional Details
Urlscan.io	100	latest scan: 6/9/2024, 9:41:50 PM
URLVoid	10	
Talos	Untrusted	Threat Categories: Malicious Sites Phishing

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

1 action succeeded

APP RUN ID	ASSET	NAME	APP
8	testtalos4_clone	user initiated url reputation action	Talos Intelligence

✓ Completed

Threat levels: Untrusted, Threat categories: {'Malware': 'Malicious file (attached or linked)', 'Malicious Sites': 'Sites exhibiting malicious behavior that do not necessarily fit in to another, more granular, threat category'}, Acceptable use policy categories: {'Illegal Activities': 'Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.'}

url = https://ilo.brenz.pl

TALOS

URL	STATUS	THREAT LEVEL	THREAT C
https://ilo.brenz.pl	success	Untrusted	Malware, Malicious Sites, Illegal Activities

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

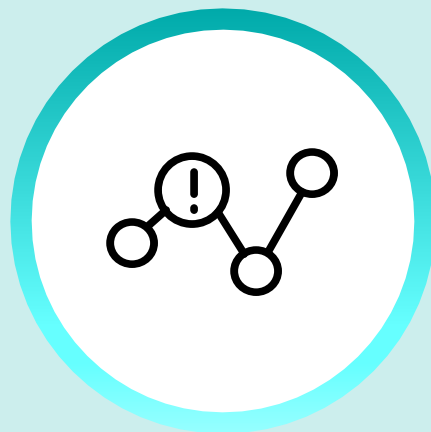
NIS2 a Splunk

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

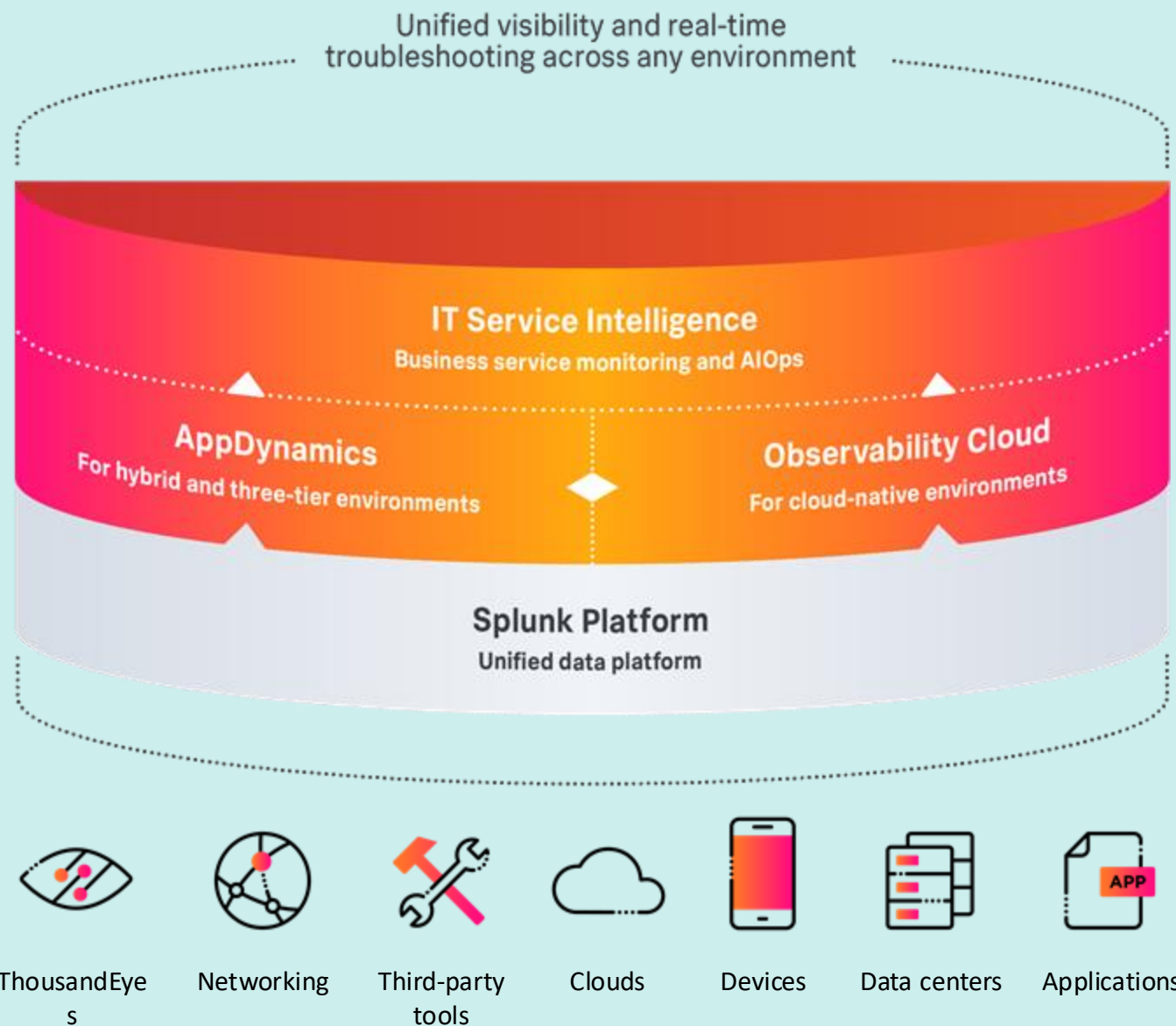


**Včasná detekce &
rychlé vyšetřování**
problémů, vedoucích k
narušení funkčnosti



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 funkcí

X ALEF

Děkuji za pozornost

