splunk>

a cisco company

splunk> a CISCO company

Bezpečnost a observabilita od Cisca

Leoš Jeřábek, Sales Manager
ljerabek@cisco.com

Strojová data obsahují cenné informace

Data Sources

Order Processing

Error in middleware

Complain raised at Call Center

Post on Twitter

Customer ID

Order ID

Product ID

ORDER, 2016-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

MAY 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213.
Exception follows: weblogic.jdbc.extensions.(adSQLExcepti
weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The
DBMS driver exception was: [BEA][Oracle JDBC Driver] Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused

Order ID

Customer ID

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type
0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-
51.16

Time waiting on hold

05/21 16:33:11:242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
CUSTID 10098213

Customer ID

05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName: “Go Cowboys!!”,followersCount:1366,friendsCount:789,link:
http://dallascowboys.com/,location:{ jectType:“place”},
objectType:“person”,preferredUsername:“Cowb0ysF@n80”,statusesCount:6072},body: “Can’t buy
this device from @ACME. Site doesn’t work! Called, gave up on waiting for them to answer! RT if
you hate @ACME!!” objectType:“activity”,postedTime:“2016-05-21T16:39:40.647-0600”}

Customer’s Twitter ID

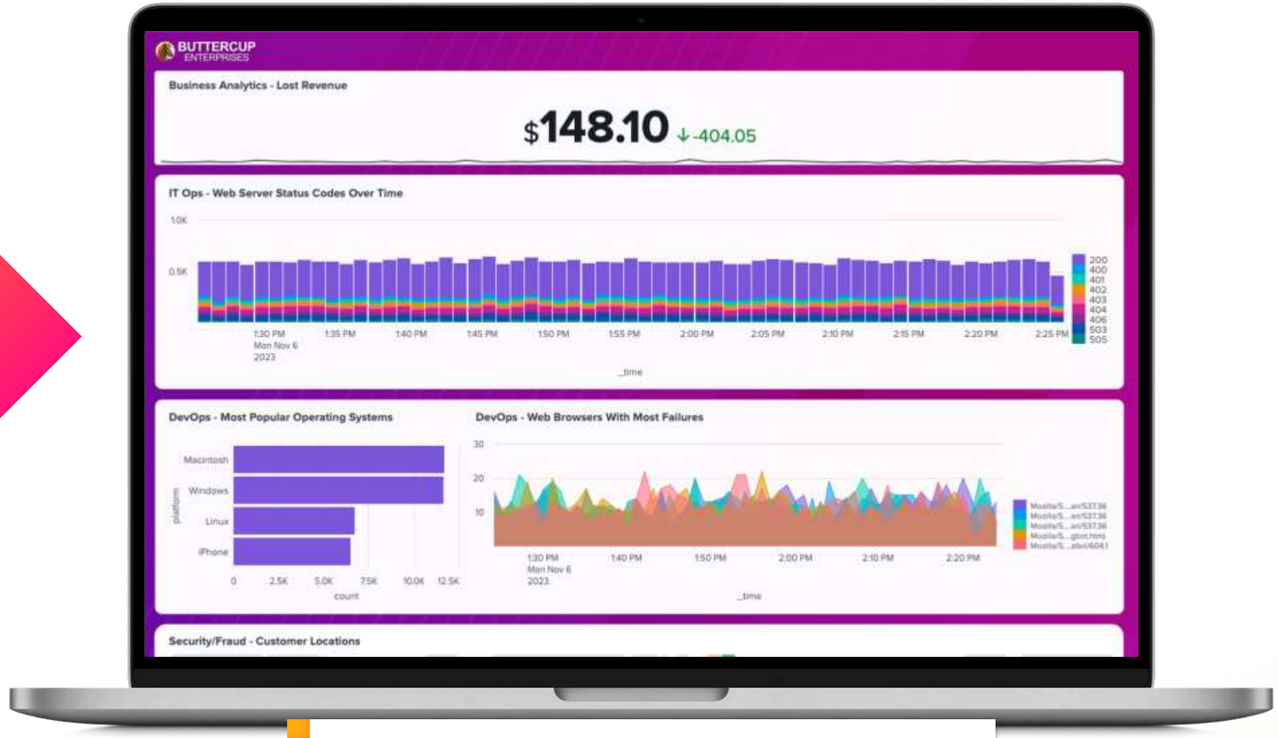
Customer’s Tweet

Company’s Twitter ID

Co umí Splunk?

splunk> a cisco company

Od chaotických strojových dat…



…k dynamickému, interaktivnímu dashboardu!

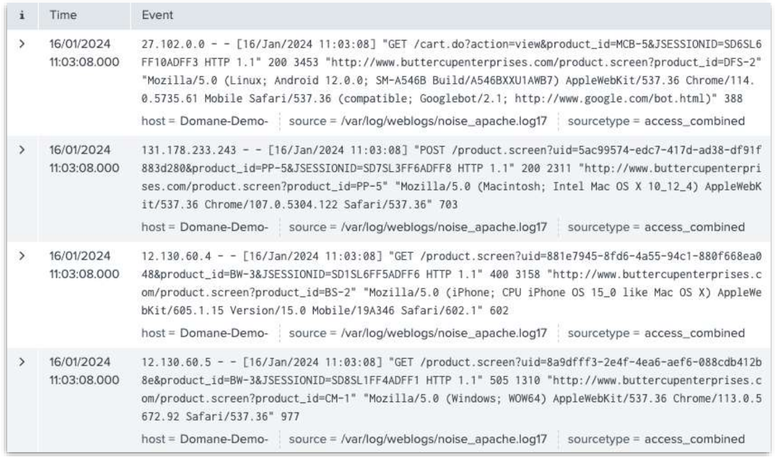
Search Processing Language (SPL)

Vyhledávací termíny | **Příkazy**

```
index=main action=purchase | stats count by status | rename count as "number of events"
```

Pipe character: Výstup zleva je vstupem doprava. | **Funkce**

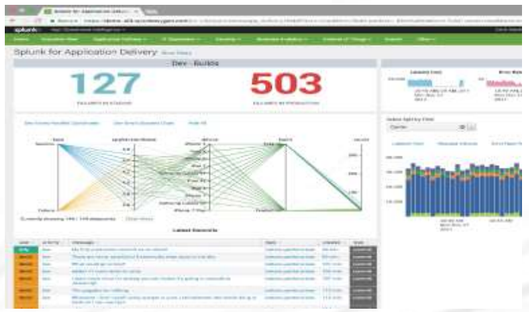
e.g. `index=main action=purchase` | `stats count by status` | `rename count as "number of events"`



i	Time	Event
>	16/01/2024 11:03:08.000	27.102.0.0 - - [16/Jan/2024 11:03:08] "GET /cart.do?action=view&product_id=MCB-5&JSESSIONID=SD6SL6FF10ADFF3 HTTP 1.1" 200 3453 "http://www.buttercupenterprises.com/product.screen?product_id=DFS-2" "Mozilla/5.0 (Linux; Android 12.0.0; SM-A546B Build/A546BXXU1AWB7) AppleWebKit/537.36 Chrome/114.0.5735.61 Mobile Safari/537.36 (compatible; Googlebot/2.1; http://www.google.com/bot.html)" 388 host = Domane-Demo- | source = /var/log/weblogs/noise_apache.log17 | sourcetype = access_combined
>	16/01/2024 11:03:08.000	131.178.233.243 - - [16/Jan/2024 11:03:08] "POST /product.screen?uid=5ac99574-edc7-417d-ad38-df91f883d280&product_id=PP-5&JSESSIONID=SD7SL3FF6ADFF8 HTTP 1.1" 200 2311 "http://www.buttercupenterprises.com/product.screen?product_id=PP-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 Chrome/107.0.5304.122 Safari/537.36" 703 host = Domane-Demo- | source = /var/log/weblogs/noise_apache.log17 | sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.130.60.4 - - [16/Jan/2024 11:03:08] "GET /product.screen?uid=881e7945-8fd6-4a55-94c1-880f668ea048&product_id=BW-3&JSESSIONID=SD1SL6FF5ADFF6 HTTP 1.1" 400 3158 "http://www.buttercupenterprises.com/product.screen?product_id=BS-2" "Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 Version/15.0 Mobile/19A346 Safari/602.1" 602 host = Domane-Demo- | source = /var/log/weblogs/noise_apache.log17 | sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.130.60.5 - - [16/Jan/2024 11:03:08] "GET /product.screen?uid=8a9dfff3-2e4f-4ea6-aef6-088cdb412b8e&product_id=BW-3&JSESSIONID=SD8SL1FF4ADFF1 HTTP 1.1" 505 1310 "http://www.buttercupenterprises.com/product.screen?product_id=CM-1" "Mozilla/5.0 (Windows; WOW64) AppleWebKit/537.36 Chrome/113.0.5672.92 Safari/537.36" 977 host = Domane-Demo- | source = /var/log/weblogs/noise_apache.log17 | sourcetype = access_combined

status	count
200	850
400	81
401	76
402	50
403	57

status	number of events
200	850
400	81
401	76
402	50
403	57



Security

IT/OT

AppDev

Biz Analytics

Streaming | Machine Learning | Scalable Index | Search and Visualization | Collaboration and Orchestration

APP

Management view – the so-called health score / KPI of a service, service, branch

Network

100	12 %	43 %	31 %
FEN Availability	VPN Utilization	Internet Circuit	Bandwidth Avail.

Operations

3 → 0%	1 ↗ 0%	100 →	32 ↘ hrs
Active Tickets	Outages	Server Health	RCA/Closure Reports

Security

6 → 0%	18 ↗	34 ↘	6 → 0%
Daily Incidents	ACAS Scan Results	HBSS & SCCM	Open Vulnerabilities

Service Requests | VIP Tickets | Scheduled Outages | Non-Compliant Systems | Systems Quarantined | Expired ATOs | DISC Equipment Status | Circuit Speeds

Management view – the so-called health score / KPI of a service, service, unit, branch, etc

Mission Critical Applications

mObywatel	e-Recepta	e-Prawo Jazdy	JPK Service	System Paszportowy	E-Toll
100 0%	100 0%	100 0%	100 0%	44 0%	100 0%
Future Health (in 20 - 30 min)	Future Health (in 20 - 30 min)	Future Health (in 20 - 30 min)	Future Health (in 20 - 30 min)	Future Health (in 20 - 30 min)	Future Health (in 20 - 30 min)






Compute

VMWare Health	VMs	ESXi	Datastore
100 0%	100	100	100

Network

NS Health	LAN	WAN	LB
100 0%	100	100	100

Access

Identity Health	2Factor	External Auth	Internal Auth
70	100	100	69

Cloud

Cloud Health	CloudVPN	Response Time	Configuration Changes
52 0%	100	5k ms	0

Security

Notable Events	Vulnerabilities	Firewall	VPN Health	Active P1-Tickets
3	6	100 0%	100 0%	0

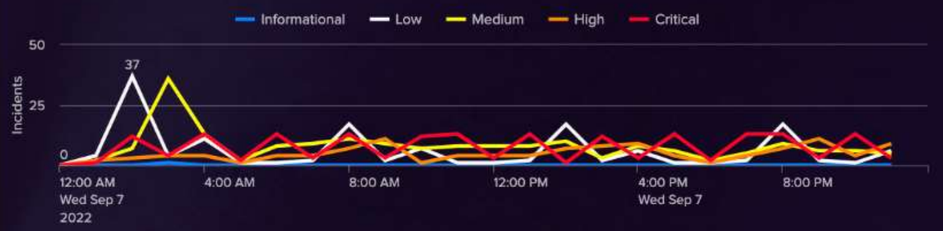
SOC Overview

splunk>

Incident Summary

Urgency	New	Unassigned	In Progress	Pending	Resolved	Closed	Total
Critical	154	0	26	0	1	0	181
High	86	0	30	1	0	0	117
Medium	145	0	42	0	1	0	188
Low	94	0	51	0	0	0	145
Informational	1	0	0	0	0	0	1
Total	480	0	149	1	2	0	632

Incident Timeline



Disposition

True Positive	Benign Positive	False Positive		Undetermined	Unassigned	Other
4	2	2	2	619	1	0
0.6%	0.3%	0.3%	0.3%	97.9%	0.2%	0.0%
Suspicious Activity	Suspicious but expected	Inaccurate data	Incorrect Analytic Logic			

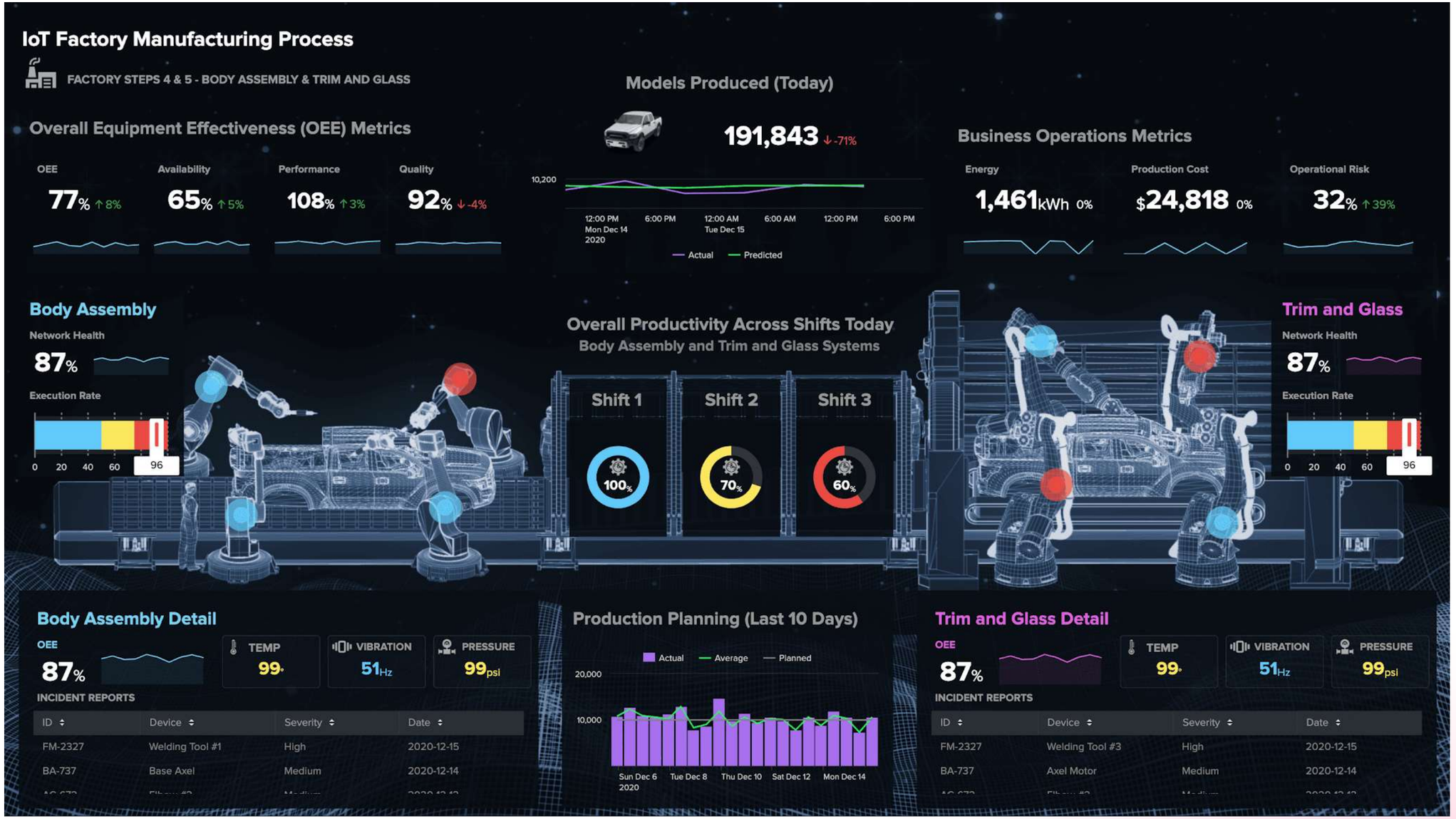
Incident Analysis

Incident Assignments

Owner	New	Unassigned	In Progress	Pending	Resolved	Closed	Total
lthomson	2	0	0	1	0	0	3
sc_admin	1	0	0	0	1	0	2
sgeetarfunk	2	0	0	0	0	0	2
soar_admin	1	0	1	0	0	0	2
splunker	1	0	0	0	1	0	2
unassigned	473	0	148	0	0	0	621

MITRE ATT&CK Techniques by Risk Object

Proces monitoring



Performance metriky a analytika

TimeRange
Last 60 minutes

Refresh Rate
1 Minute

MAERSK

Captain Peter for RCM

100 Health Score

Notifications

Temperature	15	
Humidity	22	
CO2 Level	5	

Sustainability

Environmental Performance	Extrapolated	Goal	%
Energy Consumption TJ	419,832	400,000	105
CO2 Emissions 1,000 t	31,516	30,000	104
SOx Emissions 1,000 t	514	520	99
NOx Emissions 1,000 t	810	830	97

Shipment App

95 Health Score

75 Predictive Health Score

Active Users	15,064	
Failed Logins	115 -5	
Response Time	1,418.5ms	

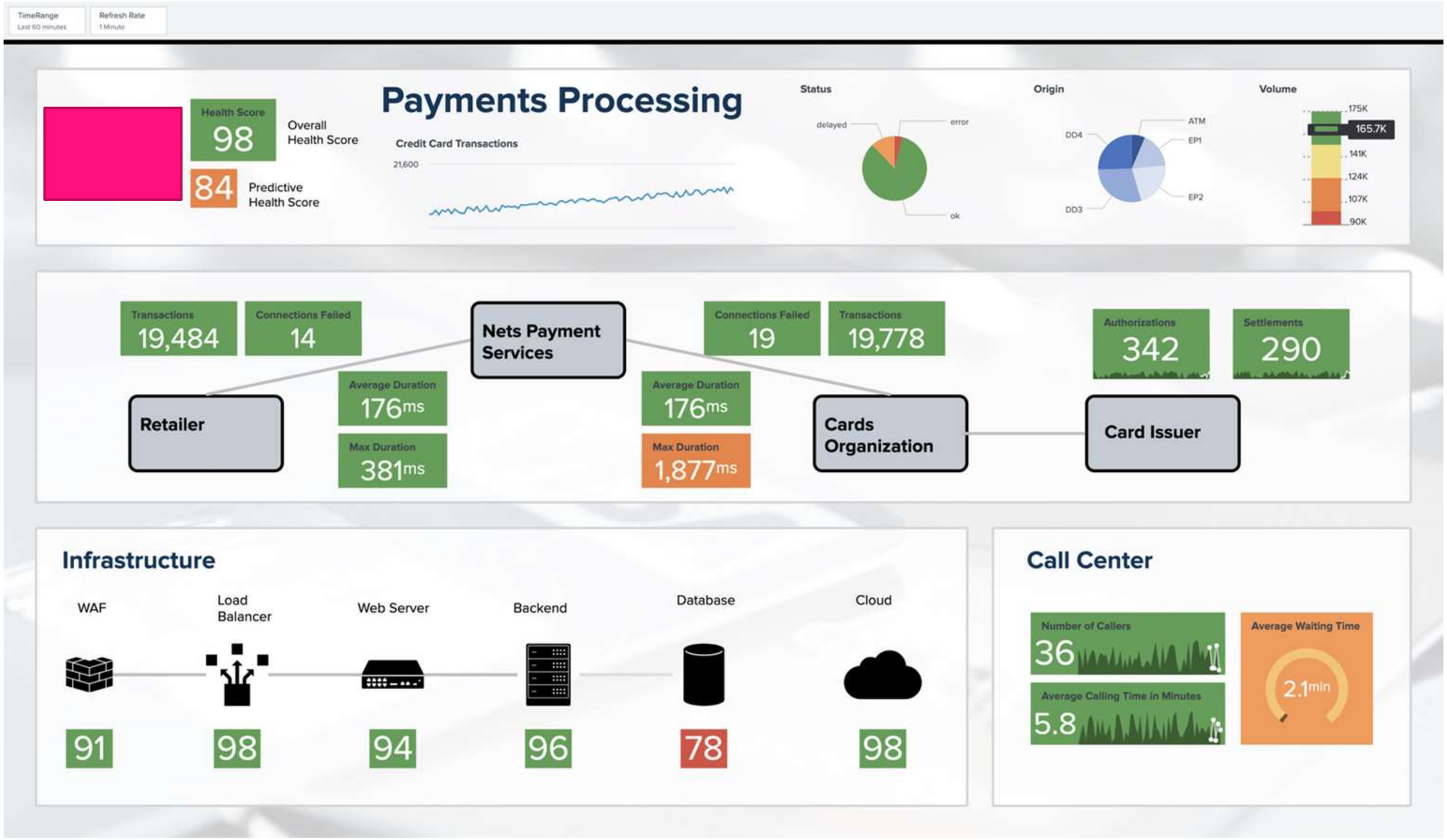
MyFinance

95 Health Score

97 Predictive Health Score

Active Users	8,851
Failed Logins	71 +8
Response Time	1,386.1ms

View your invoices	4,939
Raise you dispute	88
Check your balance	2,947
Pay online	2,904


TimeRange
Last 60 minutes
Refresh Rate
1 Minute
Payments Processing
Health Score
98
Overall Health Score
84
Predictive Health Score
Credit Card Transactions
21,600
Status
delayed
error
ok
Origin
DD4
ATM
EP1
DD3
EP2
Volume
175K
165.7K
141K
124K
107K
90K
Transactions
19,484
Connections Failed
14
Retailer
Average Duration
176ms
Max Duration
381ms
Nets Payment Services
Connections Failed
19
Transactions
19,778
Average Duration
176ms
Max Duration
1,877ms
Cards Organization
Authorizations
342
Settlements
290
Card Issuer
Infrastructure
WAF
Load Balancer
Web Server
Backend
Database
Cloud
91
98
94
96
78
98
Call Center
Number of Callers
36
Average Calling Time in Minutes
5.8
Average Waiting Time
2.1min

Reálné případy nasazení Splunku ve veřejné správě

Situational Awareness (Emergency Services): Sjednocení dat z dispečinků, senzorů a telemetrie vozidel pro rychlejší zásahy.
Monitoring kritické infrastruktury: Sjednocení IT a OT (operační technologie) pro zajištění odolnosti energetiky a dopravy.
Smart City: Propojení dat z dopravy, odpadového hospodářství a služeb občanům.
Zdravotnictví (Uptime): Zajištění dostupnosti elektronické zdravotní dokumentace a klinických systémů.
Kybernetická obrana: Sjednocená detekce hrozeb napříč vládními sítěmi.
Digitální služby: Sledování výkonu portálů pro občany a zajištění jejich spolehlivosti.
Detekce podvodů: Odhalování finančních nesrovnalostí v reálném čase.
Automatizace shody (Compliance): Automatický sběr důkazů pro audity a regulace.
Kybernetická odolnost ve vzdělávání: Ochrana výzkumných dat a univerzitních sítí.
Environmentální monitoring: Sledování emisí a udržitelnosti.
Prediktivní údržba: Předvídání poruch v dopravní a energetické infrastruktuře.
Krizové řízení: Dashboardy pro reakci na katastrofy.
Správa dat a politika: Data jako základ pro tvorbu vládní politiky.
Veřejné zdraví: Epidemiologický monitoring a včasná detekce hrozeb.
Plánování pracovní síly: Optimalizace nasazení zaměstnanců na základě dat.

Splunk – leader v securitě i observabilitě

Leader

11 years in a row

Gartner® SIEM Magic Quadrant™

No 1

SIEM i IT Operations market

Gartner

Leader Observability

Constellation, GigaOm and **Research in Action**

Gartner APM

splunk>
a CISCO company

Možnosti nasazení

Splunk Cloud

SaaS řešení

- Řešení bez starosti o svou vlastní infrastrukturu
- AWS, Azure, GCP

Splunk Enterprise

On-prem nasazení

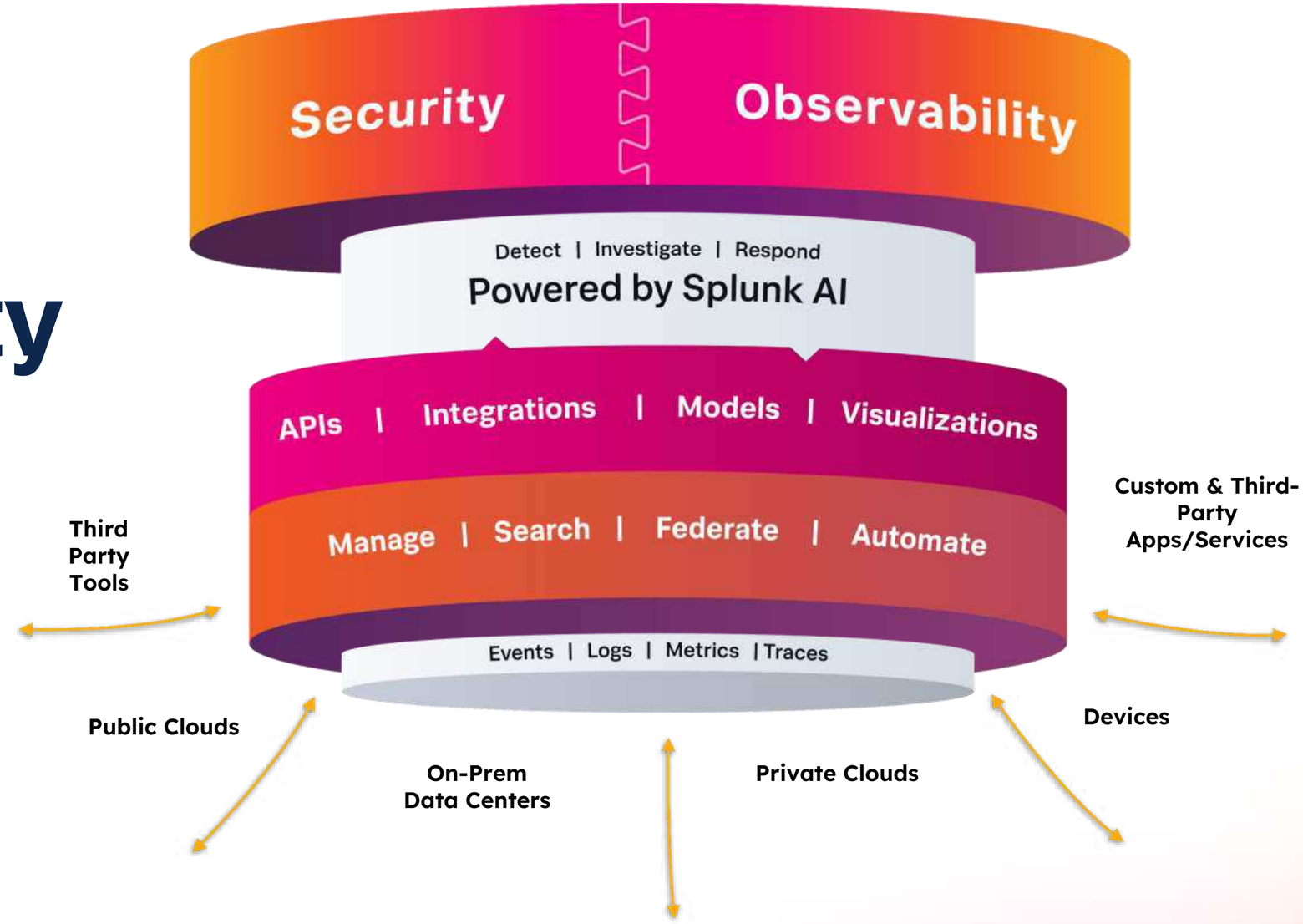
- Nasazení ve své infrastruktuře
- Absolutní kontrola svých dat
- Funguje i bez připojení k internetu (air-gapped)

Hybrid

Enterprise + Cloud

- Citlivá data on-prem, zbytek v Cloudu
- Přehled dat ve všech nasazeních díky Federated Search

Sjednocená Security a Observability Platforma



Splunk Security

Komplexní řešení pro Agentic SOC

Gartner®

11th consecutive time as a Leader

Gartner® Magic Quadrant™ for Security Information and Event Management

The expanding landscape of cyberthreats

Dopad dnešních bezpečnostních výzev

3+
hodiny strávené na vyšetřování upozornění

41%
upozornění je ignorováno

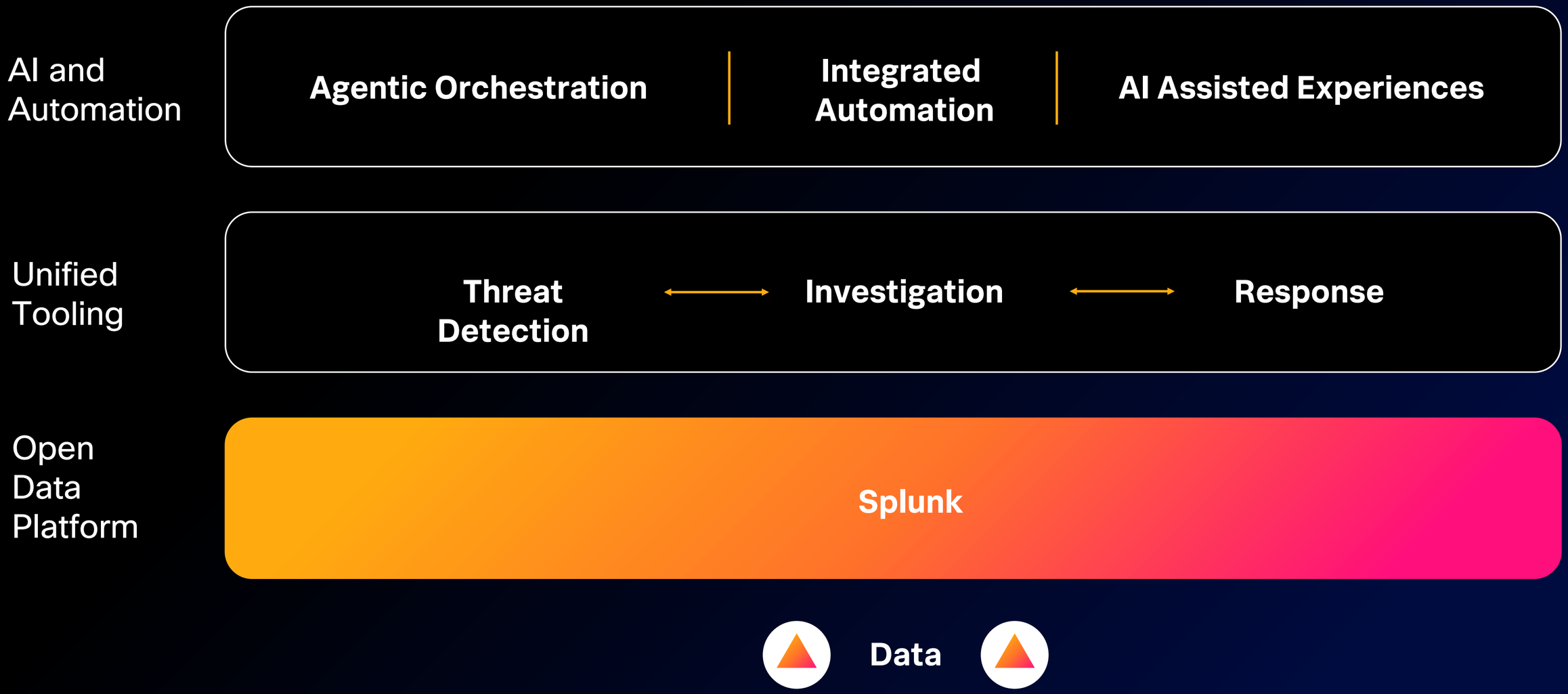
20+
různých bezpečnostních nástrojů je používáno v SOC

64%
týmů SOC má potíže s přechodem mezi nástroji, s malou integrací pro usnadnění

A strategic approach
Agentic SOC

splunk>
a CISCO company

Agentic SOC Architecture



Sjednocená SOC platforma

On-Prem | Cloud | Hybrid

Multi-cloud

True Multi Vendor

Aplikace

SIEM

UEBA

TIM

SOAR

Datová Platforma

Splunk

XDR

EDR

Firewall

IAM

Servery

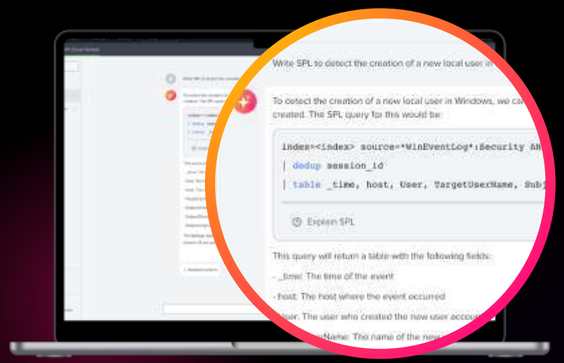
Cloud

Další zdroje

Splunk AI Asistenti

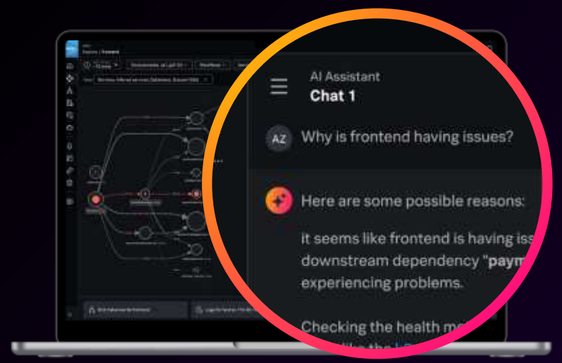
Zvyšte produktivitu, a umožněte rychlejší detekci a řešení

AI Assistant for SPL



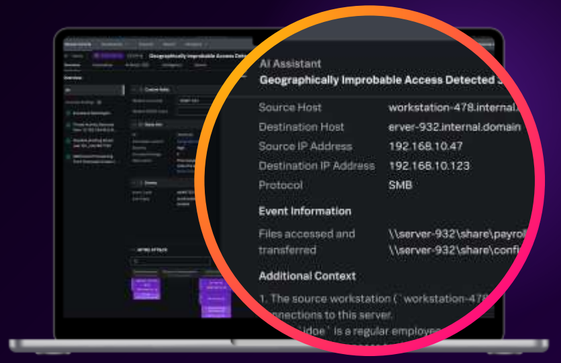
Generally Available

AI Assistant in Observability Cloud



Generally Available

AI Assistant in Enterprise Security

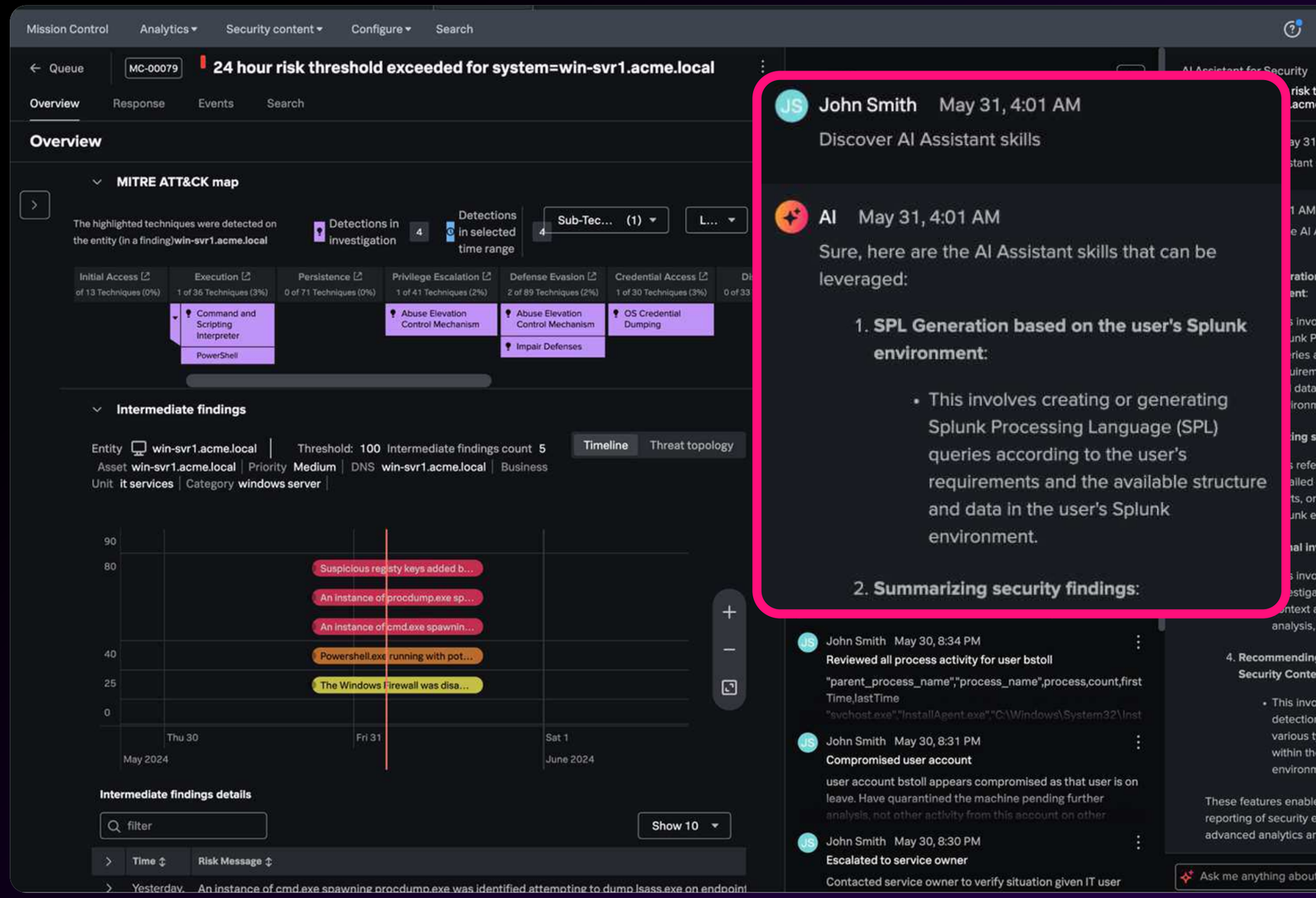


Generally Available

Agentic AI in Enterprise Security

- AI Toolkit
- Splunk MCP server
- Triage agent
- AI Malware reversing agent
- AI Assistant v Enterprise security

Vše v ceně produktu.....



Příklady nasazení on-prem

Single Server Deployment (S1)

- **Ideální pro:** Menší prostředí, PoC (Proof of Concept) nebo objemy dat zhruba do 300 GB/den.
- **Architektura (All-in-One):** Indexer a Search Head běží na jednom fyzickém nebo virtuálním serveru.
- **Výhody:** Velmi rychlé nasazení a nízké náklady na infrastrukturu.
- **Omezení:** Nemá High Availability. Pokud server spadne, nefunguje vyhledávání a nová data se musí bufferovat na Forwarderech.

Splunk Observability

Izolované týmy řeší izolované problémy

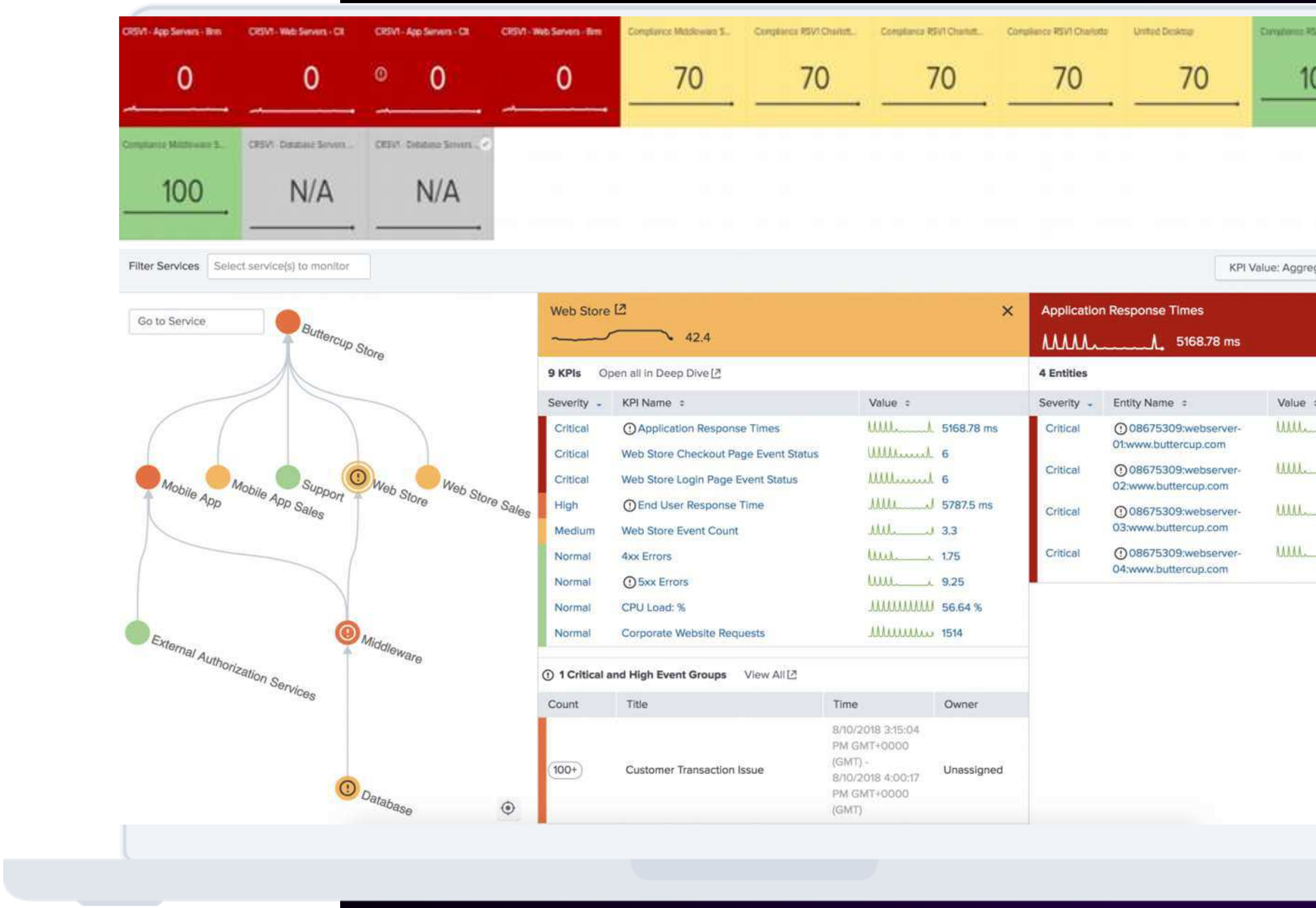
ITOps Tým

The War Room

Business linie

Skutečná end-to-end viditelnost

- Sledujte stav a výkonnost služeb (Service Analyzer)
- Získejte detailní pohled do infrastruktury – z jednoho dashboardu
- Root Cause analýza



Splunk IT Service Intelligence

Nejkomplexnější observability řešení na trhu

Získejte kompletní pokrytí

Plná viditelnost napříč sítí, infrastrukturou a aplikacemi

Snižte MTTD a MTTR

Rychlejší detekce a analýza incidentů

Priorita dopadu na business

Jak výkonnostní problémy ovlivňují klíčové KPI vašeho businessu

Mějte náklady pod kontrolou

Zvýšení provozní efektivity a snížení nákladů při řešení problémů

Proč spolupracovat se Splunkem?

Reálná byznysová hodnota podle ITOps týmů z různých oblastí

64%

▼ **Neplánované výpadky**

Optimalizace nákladů

Zvýšená dostupnost díky prevenci nákladných incidentů

90%

▼ **Méně výstrah**

Provozní efektivita

Týmy se mohou soustředit na to, co je skutečně důležité

97%

▼ **Zkrácení MTTR**

Dopad na byznys

Posílení reputace značky díky 360° přehledu o službách

75%

▼ **Chybovost vůči zákazníkům**

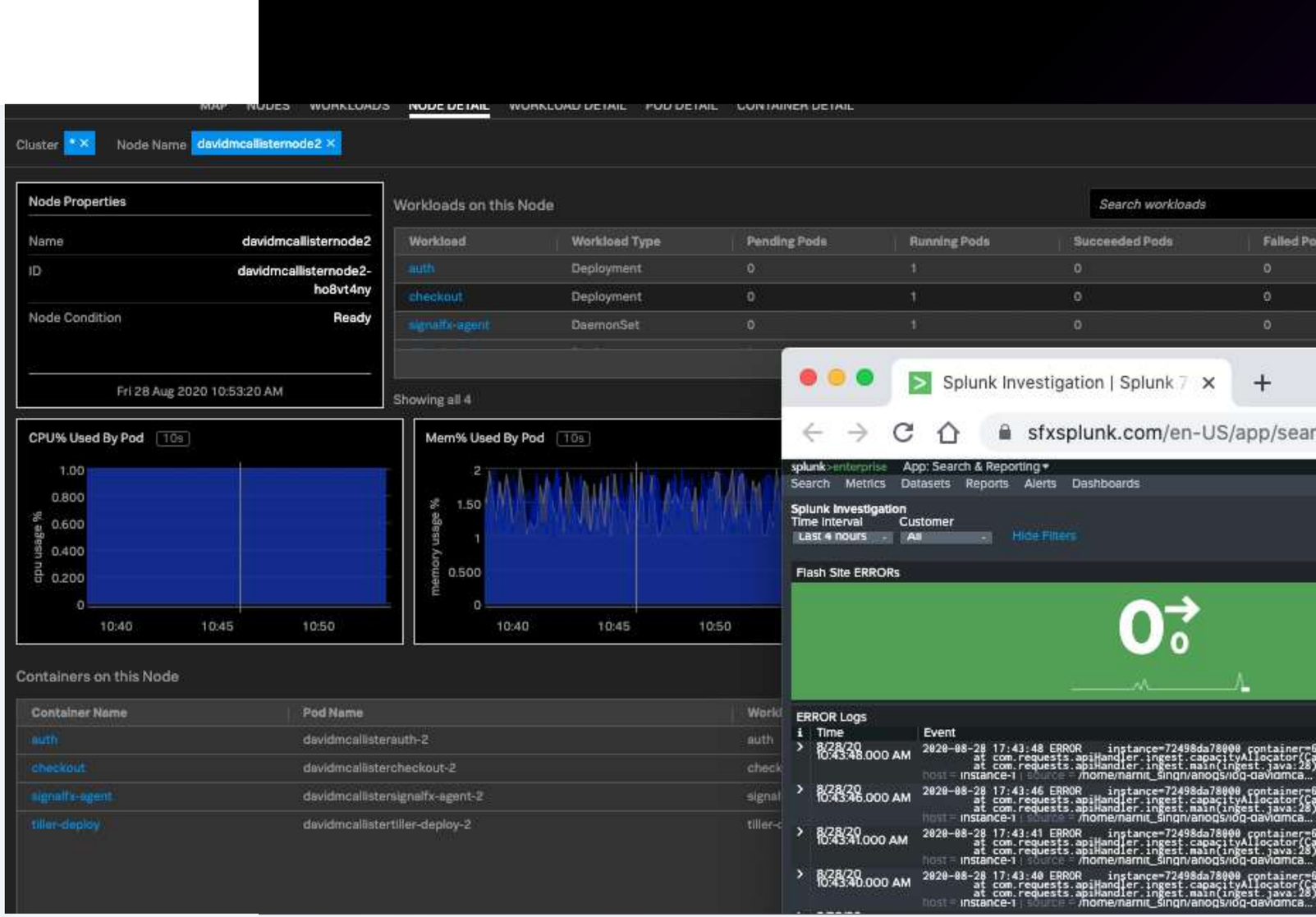
Inovace

Úspěšná transformace firmy pomocí moderních technologií

splunk> a CISCO company

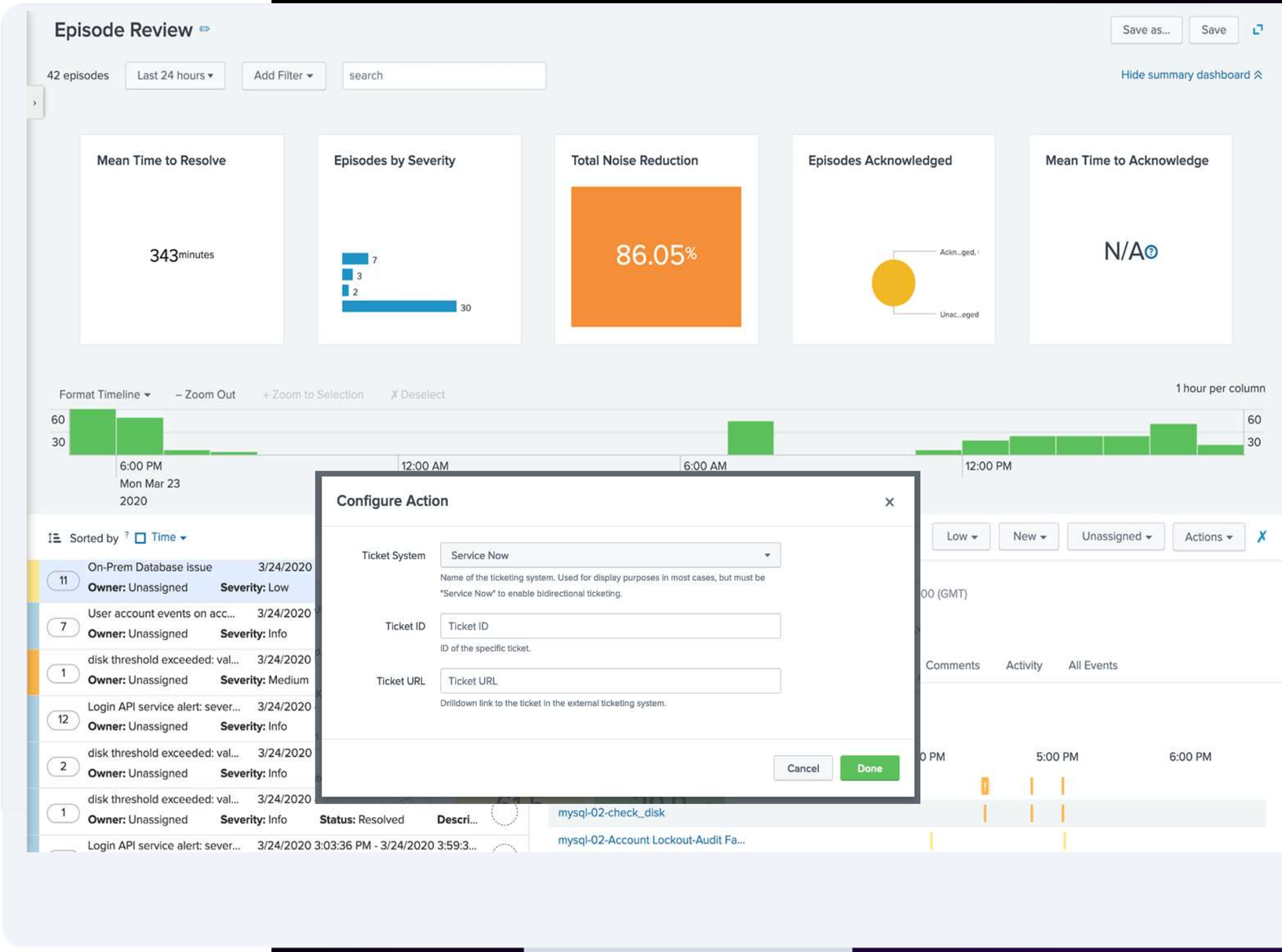
Monitoring infrastruktury

- **Konsolidujte dohledové a integrační nástroje**
- **Dohled virtualizačních platforem**
- **Monitoring kontejnerizace**



Inteligentní Incident Management

- **Zrychlete MTTR díky korelaci událostí v reálném čase**
- **Automatizovanému určování priorit incident**
- **Integraci s nástroji IT service managementu (ITSM)**



Glass Tables

- Vlastní a předpřipravené dashboard
- Ucelený pohled na celý IT/Bussines stack
- Dashboard Studio

Reference ve světě

Cloud & Online Services

Google · SONIFI · Zillow · mindtouch · PEXA · CONCUR · SurveyMonkey · slack

Education

Penn State · Duke University · University of Exeter · The George Washington University · Imperial College London · Illinois · Stanford University · USC University of Southern California · The University of Texas at Austin

Energy & Utilities

PG&E · Trane · ENERNOC · ENGIE · TransAlta

Financial Services

Aflac · TransUnion · FINRA · Nasdaq · AAA · Japan Net Bank · NCCoE · PSCU · PROGRESSIVE

Government

United States Census 2020 · NASA · City of Gold Coast

Healthcare

Pfizer · imprivata · Recursion · UCLA Health · myriad genetics · CardinalHealth · OhioHealth · AstraZeneca · NewYork-Presbyterian

Media & Entertainment

AIRBUS · ing · BMW · asics · MBDA · Honda · Shaw Floors · Bosch · P&G · Airbus · Jabil · Northrop Grumman · Yokogawa · Porsche · Discovery Communications · ESPN · CenturyLink · Ubisoft

Retail

amazon · Coca-Cola · Groupon · REI co-op · zulily · 7-Eleven · Tesco · Domino's

Technology

Adobe · hp · Zoom · Symantec · Autodesk · Rackspace · Intuit · TiVo · leidos · Viasat · Atlassian · intel · arlo

Telecommunications

Comcast · Telstra · NORLYS · verizon · telenor · Cisco · yelp · vodafone

Travel & Transportation

FedEx · lyft · eTravel · Dubai Airports · Expedia · Carnival · MTR · DKB · Hyatt · SNCF · YOUR LONDON AIRPORT Gatwick · McLaren

Hezký zbytek dne

splunk> a CISCO company

Splunk má největší lokální podporu v historii

Zkušení partneři a řada zákazníků v České republice

Cisco – jistá budoucnost a záruka inovace

Uvažujte Splunk s dalším projektem v bezpečnosti a observabilitě

Leoš Jeřábek, Cisco
ljerabek@cisco.com