

Technologický, aplikační a bezpečnostní dohled

Vlasta Šejvlová

Generální ředitelka

Představení společnosti



TOTALSERVICE

Open Apps Development



- Modulární platforma postavena na mikroservis architektuře
- Integrace aplikací přes integrační platformy
- Agregace, analýza a prezentace dat



- Sdružení různorodých dohledových systémů z oblasti aplikací, bezpečnosti a infrastruktury



- Business aplikace pro rozšíření a doplnění stávajících aplikačních řešení



TOTALSERVICE

- 25 let na trhu
- Více jak 90 techniků v týmu
- Více než 150 zákazníků veřejného i komerčního sektoru.
- Katalogové listy – definice služeb
- Plánování IT vývoje



SPRÁVA
VAŠEHO ICT



KYBERNETICKÁ
BEZPEČNOST



INTEGRACE
A CLOUD



PRODEJ ICT
TECHNOLOGIÍ



PROJEKTOVÉ
ŘÍZENÍ
A KONZULTACE



Bezpečnost informací nechte na nás

- ochrana osobních údajů, GDPR
- bezpečnostní testování
- bezpečnostní audit
- analýzy a hodnocení rizik
- kybernetická bezpečnost
- ISMS (ISO 27001)



Technologický a procesní monitoring

Dashboard

Technologický
dohled

Management a
vedení

Bezpečnostní
management

Uživatelé

Open Docs Data
(agregace, analýza a transformace dat)

Data

Monitoring
(Zabbix, Nagios)

SIEM
(Qradar, ELK)

Log
Management

Asset
Management

Analýza rizik

Bezpečnostní
testovací

Audit

ISMS

Zdroje

Sjednocené čtení dat z dohledových systémů

- Připravené datové konektory pro získání dat z běžně dostupných dohledových systémů
- Tvorba specializovaných datových konektorů pro ostatní systémy

Datová transformace a skladování vybraných ukazatelů pro pozdější analýzy

- Sběr dat
- Skladování dat
- Matematické operace
- Transformace dat
- Analytické vyhodnocení

Webová aplikace pro zobrazení

- Grafy
- Přehledy
- Alerty
- Notifikace
- Správa uživatelů a jejich oprávnění

- Sjednocená vizualizace, uživatel používá jednu aplikaci
- Jednotné ovládání
- Konfigurovatelné dashboardy dle monitorovaných oblastí
- Konfigurovatelná organizace dashboardů do složek dle zaměření
- Správa uživatelů a zobrazení dashboardů dle oprávnění uživatelů
- Pokročilá práce s vizuálními prvky a kombinace více zdrojů dat

Pohledy na jednotlivé dashboardy



Manage

Playlists

Snapshots

Library panels

New Dashboard

New Folder

Import

☐

Sort (Default A-Z)

☐

Filter by starred

Filter by tag

☐

Test folder

☐

General

☐

9123 - Elasticsearch

General

elasticsearchprometheus

☐

Course

General

☐

elastic log size

General

☐

JVM (Actuator) with application name

General

☐

JVM (Micrometer)

General

☐

Micrometer Spring Throughput

General

☐

Monitor Statistics

General

☐

Postgres Overview - 1

General

postgres

Pohledy na jednotlivé dashboardy



Pohledy na jednotlivé dashboardy



Response Time SLA

Monitor Name	SLA Name	Group Name	Status	
Example	SLA_6	2, testing_1, testing_2	100	View Report
Example	SLA_7	-	100	View Report
LoadBalancerTesting1	SLA_7	-	100	View Report
ApplicationLoadBalancerTest1	SLA_7	-	100	View Report
IntegrationDemoInstance	SLA_7	-	100	View Report
ReverseIntegration	SLA_7	-	100	View Report
ElbInstances	SLA_7	-	100	View Report
mydb	SLA_7	-	100	View Report
Music	SLA_6	3	100	View Report
Music	SLA_7	-	100	View Report
IPUpdates3	SLA_7	-	100	View Report
dynamodb	SLA_7	-	100	View Report
url-sep1	SLA_7	-	96.97	View Report

Next Generation Security Solutions

Bezpečnost informací nechte na nás

Oblasti

- kybernetická bezpečnost
- ISMS (ISO 27001)
- ochrana osobních údajů, GDPR
- TISAX – Informační bezpečnost pro automobilový průmysl
- bezpečnost IoT a průmyslu
- bezpečnostní architektura IS
- bezpečnost koncových zařízení
- správa privilegovaných účtů

Služby

- bezpečnostní testování
- NESTOR - Security Operations Center
- SIEM a Log management
- implementace bezpečnostních technologií
- bezpečnostní audity
- analýzy a hodnocení rizik
- školení kybernetické bezpečnosti
- SMC - Security Management Center
- outsourcing bezpečnostních rolí





System podpory správného bezpečnostního rozhodování

- Využívá informace z **technologií** (např. SIEM), ale i z **procesů** (např. analýza rizik)
- data analyzuje a vizualizuje srozumitelně **nejen pro odborníky na bezpečnost**, ale i pro bezpečnostní laiky
- plně uzpůsobeno potřebám konkrétního uživatele – zaměření na potřebu uživatele vědět, ne na vlastnosti a schopnosti nástroj
- poskytuje historické, současné a prediktivní zobrazení stavu bezpečnosti
- vizualizuje varianty přínosy nebo rizika plánovaných bezpečnostních změn (what-if dynamická analýza)
- vystačí si s minimem dostupných dat



Plně uzpůsobeno potřebám konkrétního uživatele

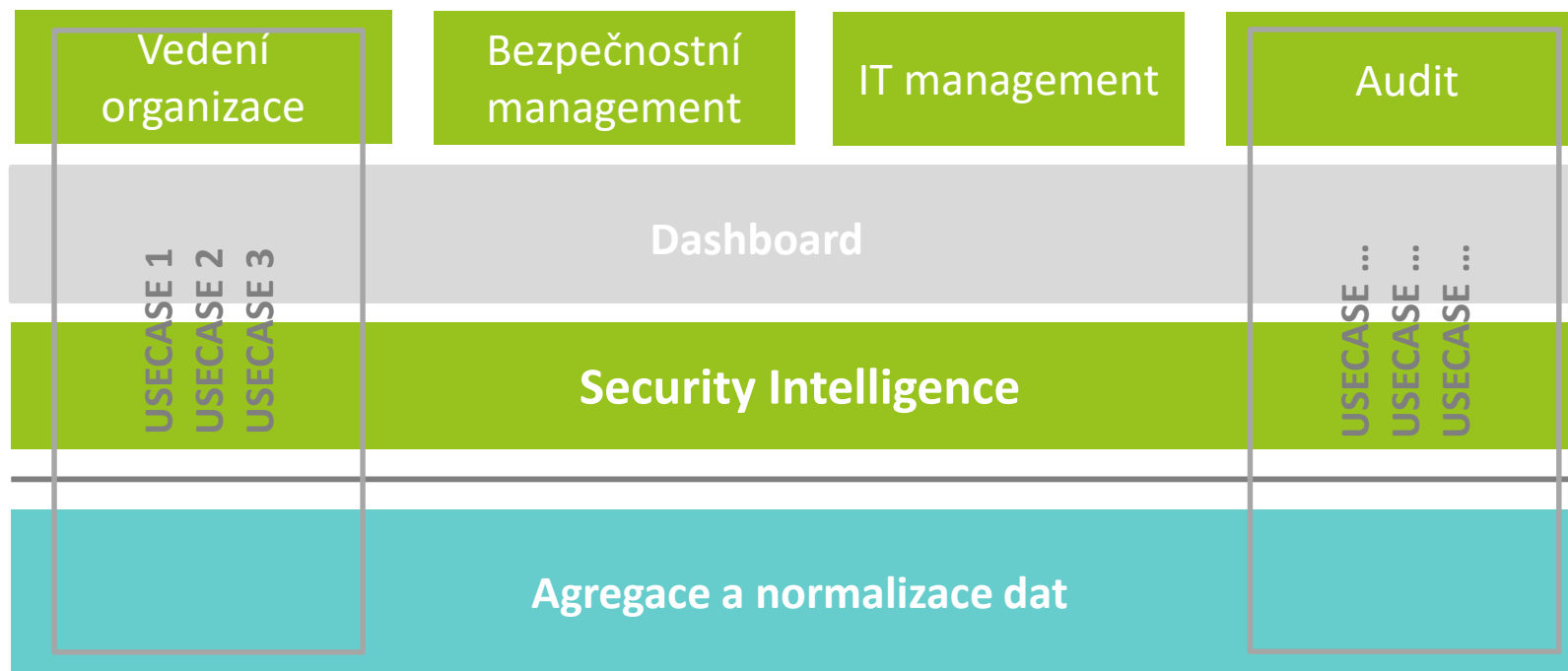


Provozováno jako SaaS



Škálovatelnost podle finančních možností klienta

System řízení bezpečnosti



Uživatelé

Reporting

Analýza

Data

Zdroje

System řízení bezpečnosti

- Lze provozovat zcela samostatně
- Lze integrovat s bezpečnostními dohledovými systémy a službami



↓
Událost
↓
Korelace
↓
Reportuji



↓
Událost
↓
Je to incident?
↓
Reportuji
↓
Řídím a zvládám incident



↓
Událost
↓
Je to incident?
↓
Jak velké riziko představuje?
↓
Jakou má prioritu? →
↓
Reportuji přiměřeným způsobem
↓
Řídím a zvládám incident

Má smysl budit třetí linii podpory, když nám hrozí riziko ve výši 3000 Kč? To počká do rána.

Správa výsledků v SMC



- PŘEHLED
- BEZPEČNOST
- RIZIKA
- EFEKTIVITA
- PROCESY
- TECHNOLOGIE
- SHODA
- UŽIVATELE
- ADMINISTRACE

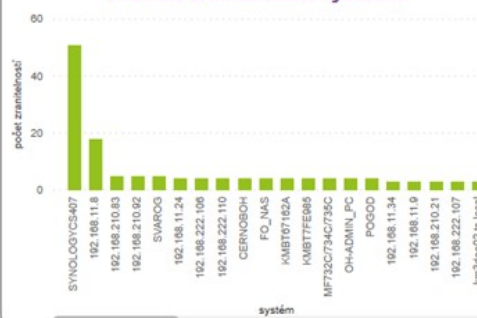
Technologie



Vysoce prioritní opatření k realizaci v IT



Přehled zranitelnosti systémů



Počet IT systémů se závažnou zranitelností

21

Top rizikové zranitelnosti

basescore	name	id_vulnerability
10.00	192.168.11.18	192
10.00	192.168.11.34	519
10.00	192.168.11.8	190
10.00	192.168.11.8	519
10.00	192.168.222.102	192
10.00	km3dear02.ts.local	256
10.00	km3dear02.ts.local	519
10.00	km3dear02.ts.local	256
10.00	km3dear02.ts.local	519
10.00	KMBT07162A	519
10.00	KMBT7FE985	519
10.00	MF833C/835C	519
10.00	MF732C/734C/735C	256
10.00	MF732C/734C/735C	519
10.00	SYNOLOGYCS407	192
10.00	SYNOLOGYCS407	213
10.00	SYNOLOGYCS407	9257
10.00	XR9C934E3B5D44	519
8.30	192.168.11.8	28691
7.80	SYNOLOGYCS407	49248
7.80	192.168.11.8	60319
7.50	192.168.11.8	64383
7.50	192.168.11.9	4268
7.50	192.168.210.84	615
7.50	FO_NAS	116109
7.50	SYNOLOGYCS407	58369
7.50	SYNOLOGYCS407	95530
7.50	SYNOLOGYCS407	95531
7.50	SYNOLOGYCS407	99439
7.50	SYNOLOGYCS407	99450
6.90	SYNOLOGYCS407	51825
6.80	192.168.11.24	62005
6.80	192.168.11.8	27451
6.80	SYNOLOGYCS407	62834
6.80	SYNOLOGYCS407	105429
6.40	192.168.11.8	28688
6.40	85.207.99.26	117195
6.40	SYNOLOGYCS407	83876
6.40	SYNOLOGYCS407	88553

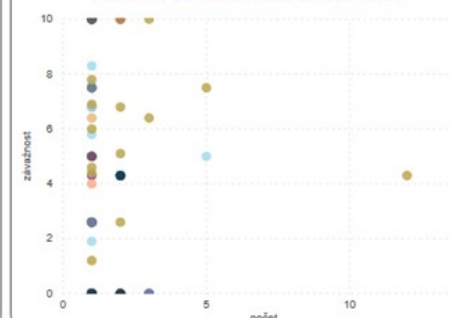
Počet zranitelností
209

Předpokládané náklady na technická opatření
490K Kč

Počet a trend zranitelnosti



Počet a závažnost zranitelnosti



Děkujeme za pozornost



Vlasta Šejvlová
Generální ředitelka
Vlasta.sejvlova@openapps.cz

Radovan Urban
Ředitel vývoje aplikací
radovan.urban@openapps.cz



Daniel Přívratský
Enterprise Security Architect
dprivratsky@ngss.cz

Stanislav Kollert
Information Security Architect
skollert@ngss.cz

TOTALSERVICE

Jan Navrátil
Obchodní ředitel
jnavratil@totalservice.cz