

Kybernetická bezpečnost jako služba

Tomáš Hlavsa

AtoS
CYBER
security

BULL -> ATOS



Atos

Bull

atos technologies

BULL se od 06/2015 stává součástí Atos IT Solutions and Services

Kterým zákazníkům jsme již pomohli

- ▶ Škoda Auto – Security + network monitoring , 20 000 EPS
- ▶ Pojišťovna české spořitelny - Security monitoring, 2 500 EPS
- ▶ Ministry of Environment - Security monitoring, 1 000 EPS
- ▶ Kooperativa - Security monitoring, 2 500 EPS
- ▶ Institute of Chemical Technology – Security + network monitoring
- ▶ Government institution – Security monitoring
- ▶ Finance institution- Security monitoring, 10 000 EPS

Kterým zákazníkům jsme již pomohli

- ▶ T-Mobile CZ – Network monitoring
- ▶ Vodafone CZ - Network monitoring
- ▶ University Hospital Ostrava – Security monitoring
- ▶ Czech Government – Network monitoring
- ▶ Allianz - Network analyses – Migration project
- ▶ Západočeská univerzita – ISMS audit 27001
- ▶ Vitana a.s. – Network audit
- ▶ Karlova univerzita - Network monitoring

Neustále se měnící bezpečnostní situace



Fraud (internal or external) will increase and require adapted detection within transaction conversation



Digital DNA (strong **identity verification**) including on mobile devices will go mainstream



Privacy legislation & cyber security standards will impact organizations



Threat Intelligence and contextual data feeds to detect Next Gen APTs with stealth capabilities

KYBERNETICKÁ BEZPEČNOST



Data discovery and monitoring key to protect “crown jewels” from theft or leakage



Malware expands to Mobile devices, Industrial Control Systems, and Internet of Things



DDoS Attacks will use adaptive and intelligent DoS techniques



Network behavior analysis to identify abnormal behavior and detect insider threats and/or advanced attackers moving laterally within the network



Security for/from the **Cloud** as Cloud data will be increasingly targeted

Agenda

Přístup ATOSu ke kybernetické bezpečnosti

S čím Vám ATOS může pomoci

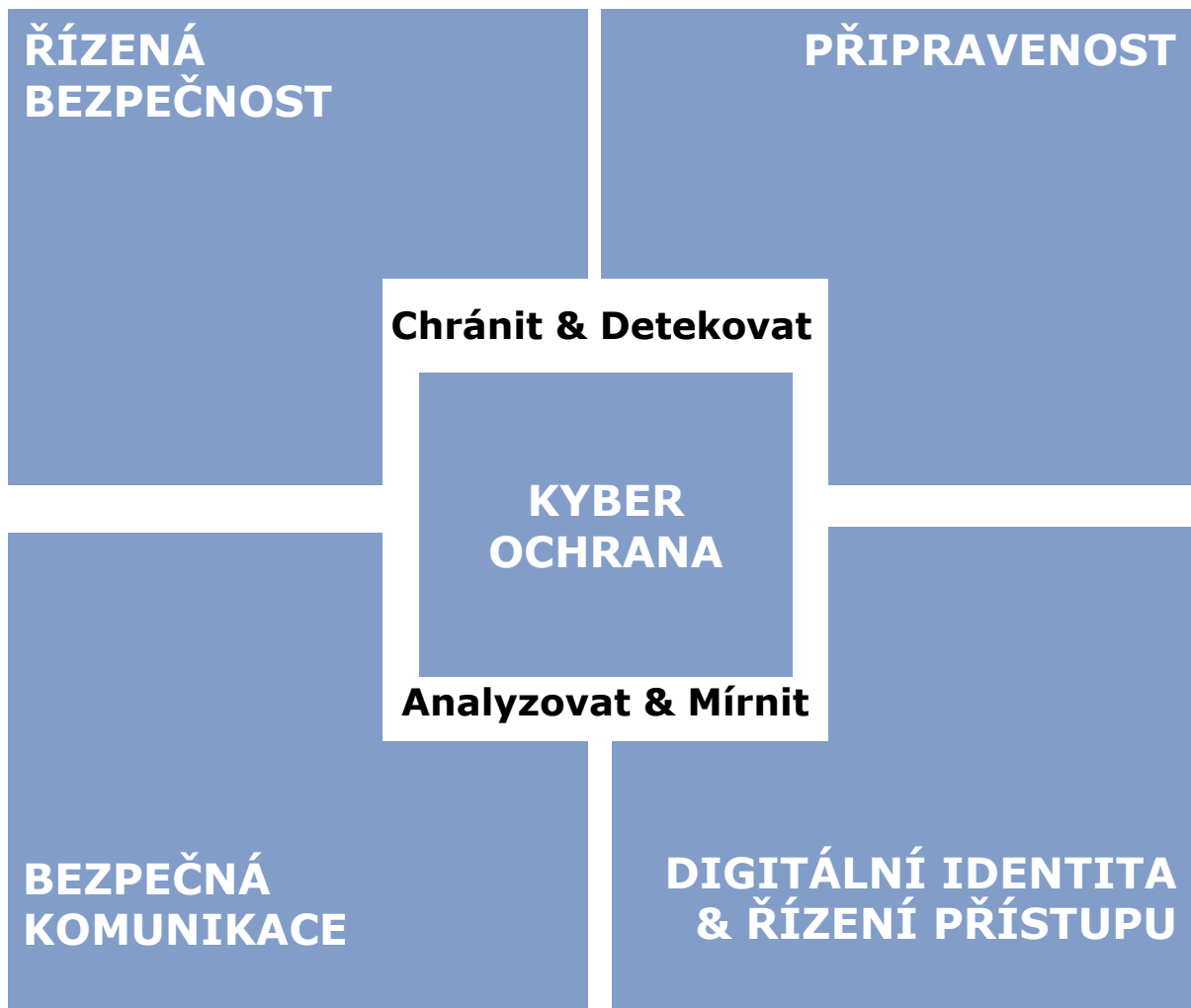
Co nás odlišuje?

Kontakty

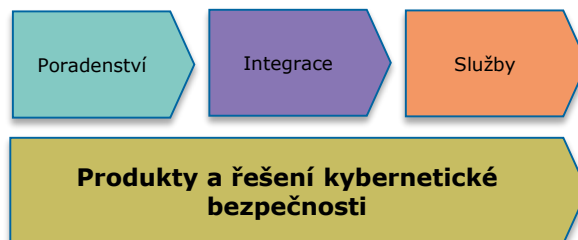
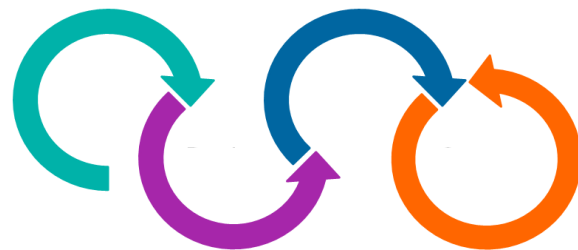


Kybernetická bezpečnost

Co Vám ATOS může nabídnout

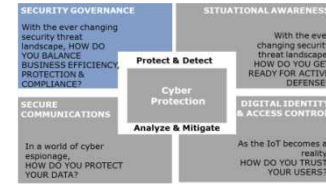


Atos poskytuje svým zákazníkům v oblasti kybernetické bezpečnosti **poradenství, návrh, implementaci & provoz** služeb

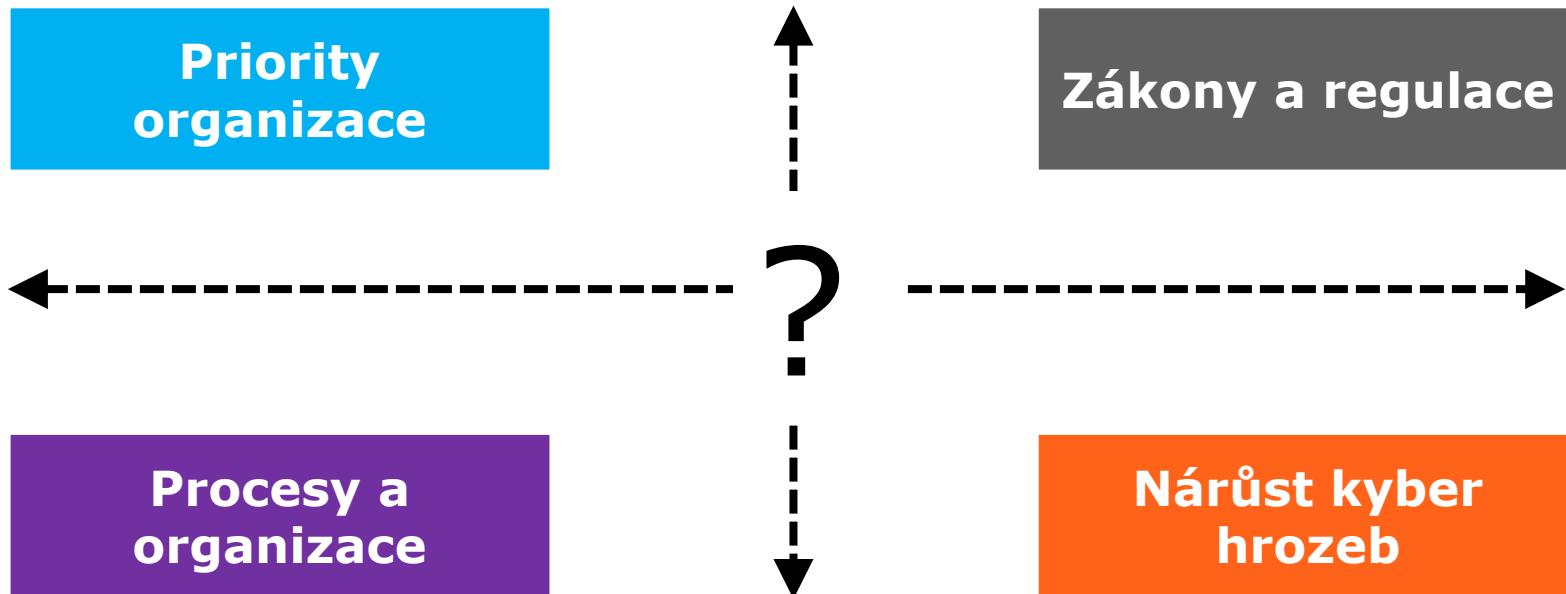


Řízení bezpečnosti

Prizpůsobení měnícím se regulacím i hrozbám



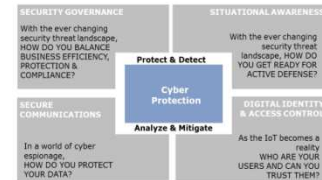
**HLEDÁME ROVNOVÁHU MEZI ÚČINNOSTÍ OPATŘENÍ,
STUPNĚM OCHRANY A ZÁJMY ORGANIZACE**



A co když něco nevyjde? Lze se vůči kybernetickým hrozbám pojistit? A jak? A za kolik?

OCHRANA kyber prostředí

End-to-End řešení



CHRÁNÍME CELÝ VÁŠ EKOSYSTÉM

Náš pohled: bezpečnost napříč organizací na všech úrovních

UŽIVATELÉ



KONCOVÁ ZAŘÍZENÍ

APLIKACE

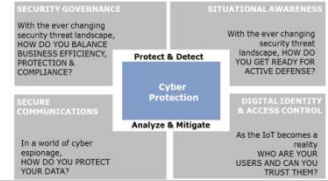
DATA

INFRASTRUKTURA

SÍTĚ



Atos zabezpečuje sběr a zpracování kritických dat INSEE



Francouzský národní institut pro statistiku a ekonomický výzkum
INSEE

Zadání

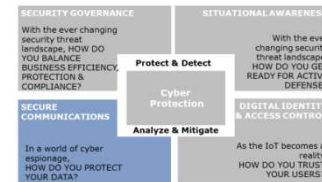
- IT institutu INSEE bylo silně decentralizované
- Nutnost nasazení nové aplikace pro sčítání obyvatel
- Návrh a dodání bezpečnostní architektury v nových datacentrech

Atos řešení

- Návrh architektury
- Podpora během konsolidace infrastruktury
- Následný bezpečnostní audit

Bezpečná komunikace

Atos řešení pro bezpečnou komunikaci



BEZPEČNOST TRANSAKČÍ

MetaPKI/ MetaSign

CardOS SmartCards

**BEZPEČNÉ MOBILNÍ
TERMINÁLY**

Hoox

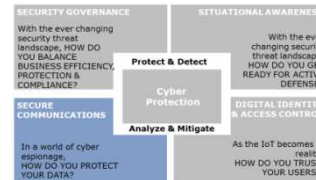
KRYPTOGRAFICKÁ ŘEŠENÍ

TRUSTWAY VPN

Hardware Security
Module

Realita: 95% Francouzských bank

Atos zabezpečuje jednu z největších „Homeland security“ sítí v Evropě



DEFENSE GRADE

Zadání

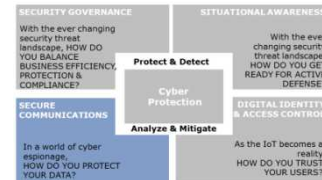
- Zabezpečit IP síť Francouzské národní gardy
- 4,600 + lokací po celém světě

Atos řešení

- Vysoce zabezpečená síť na úroveň “restricted use”
- 6000+ IP encryptors vč. správy a auditu

Secure Communication

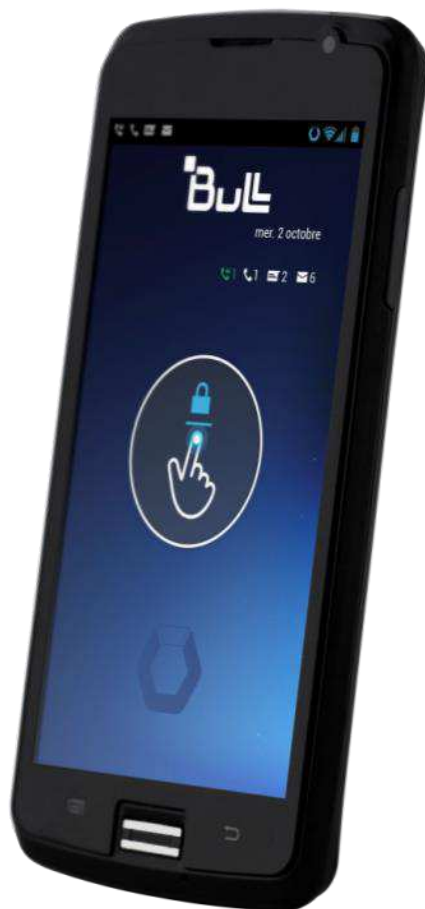
Hoox, smartphone pro bezpečnou komunikaci



Hlas, SMS a data
šifrovaná komunikace

Biometrická
autentizace

Vzdálená správa
(wipe...)



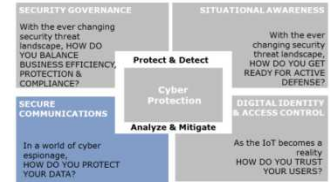
Data ve smarphonu
šifrována

Anti-intrusion fyzické
zabezpečení
Ruggedized secure OS

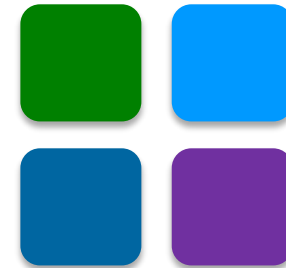
Audit a certifikace
Android aplikací

Secure Communication

Hoox, smartphone pro bezpečnou komunikaci



Komerční aplikace



Vaše aplikace

Audit – TrustRevealing™

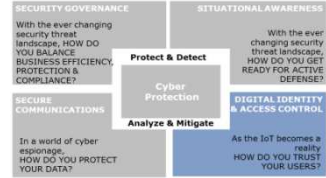
Vaše bezpečnostní politika

Váš firemní
"App store"



Digitální Identita & Řízení přístupu

Základní kámen bezpečnosti



ZABEZPEČENÝ PŘÍSTUP VE VŠECH SITUACÍCH

EVIDIAN



Řídit, spravovat, kontrolovat identitu a práva uživatelů

Identity & Access Management



Správa silné či firemně orientované autentikace

Authentication Management



On-line, vícefaktorová a silná autentikace pro publikování aplikací do webového prostředí

Web Access Management



Zabezpečený přístup k aplikacím z PC, tabletů, smartphonů ...

Enterprise Single Sign-On



Overall Leader
IAM/IAG Suites
September 2014



Overall Leader
Enterprise Single Sign-On
January 2014

DirX



Identity Access Management – Single Sign On

Use cases



University Hospitals of Geneva – SSO

8 nemocnic, 40 lokalit, 50+ aplikací, 12 000+ uživatelů
Single Sign-On kombinovaný s biometrickou autentizací
Redukce nákladů a HelpDesk potřeb

Lékaři a nemocniční personál se může přihlašovat odkudkoliv svým účtem k jakémukoliv PC, Kiosku...

German Electronic Health Card - eGK

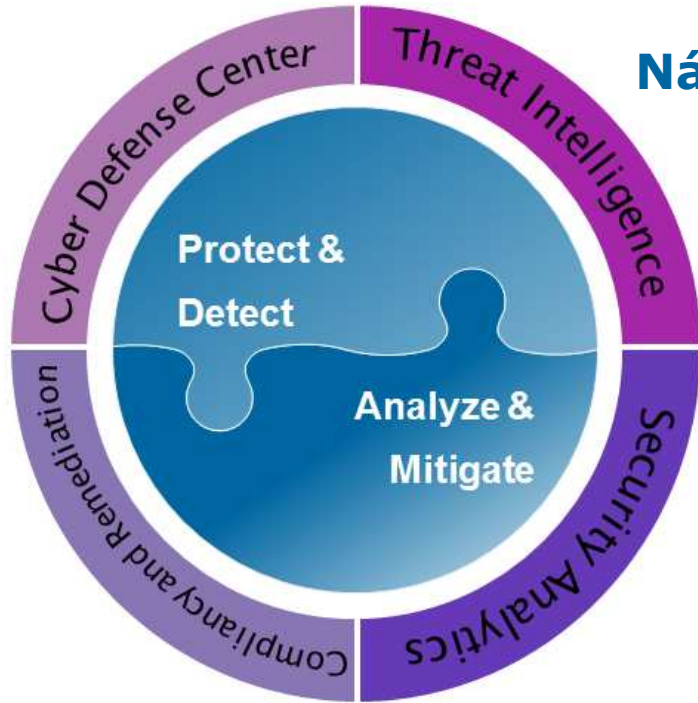
20 mil+ uživatelů , 50 000 certifikací hodinu
Online výměna dat s Card Application Management System (CAMS) zdravotních pojišťoven



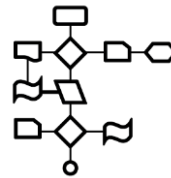
Jste připraveni na kyber hrozby?

Jste připraveni v režimu 24/7/365

SECURITY GOVERNANCE With the ever changing security threat landscape, HOW DO YOU BALANCE BUSINESS EFFICIENCY, PROTECTION & COMPLIANCE?	SITUATIONAL AWARENESS With the ever changing security threat landscape, HOW DO YOU GET READY FOR ACTIVE DEFENSE?
SECURE COMMUNICATIONS In a world of cyber espionage, HOW DO YOU PROTECT YOUR DATA?	DIGITAL IDENTITY & ACCESS CONTROL As the IoT becomes a reality, HOW DO YOU TRUST YOUR USERS?



Náš přístup: aktivní kontrola v reálném čase

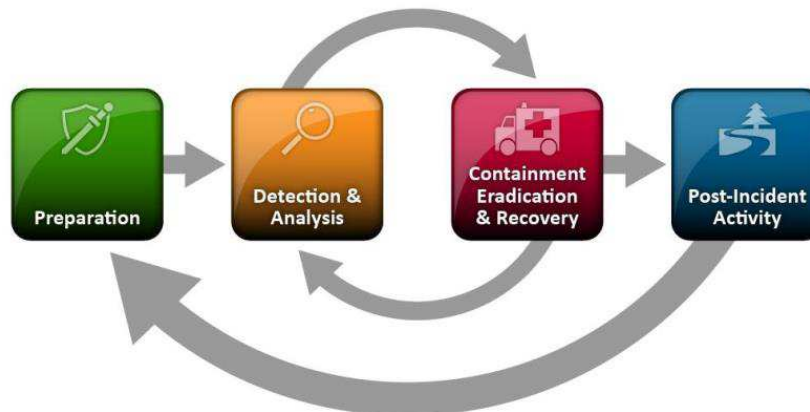


Dynamická rekonfigurace a izolace napadených prostředí

Profilování v reálném čase, analýza dat



3 Globální SOC & 3 Dedikované SOC
Globální CSIRT Team schopný řešit kyber hrozby

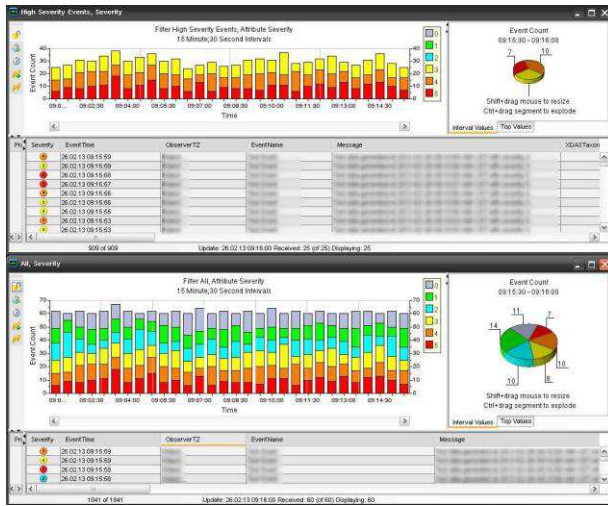
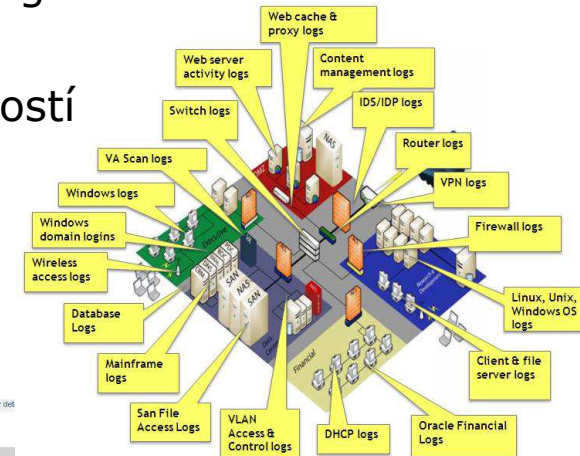


AHPS – ATOS High Performance Security

Správa kyber hrozeb v reálném čase

Služba Atos High Performance Security (AHPS) poskytuje organizacím:

- ▶ security log management
- ▶ součinnost naplňování zákonných a regulatorních povinností
- ▶ řízení rizik s ohledem na kontext organizace
- ▶ 24 x 7 inteligentní monitorovací služby
- ▶ schopnost zasahovat vůči urgentním hrozbám v reálném čase



SOC – Security Operations Center

Kybernetická bezpečnost jako služba

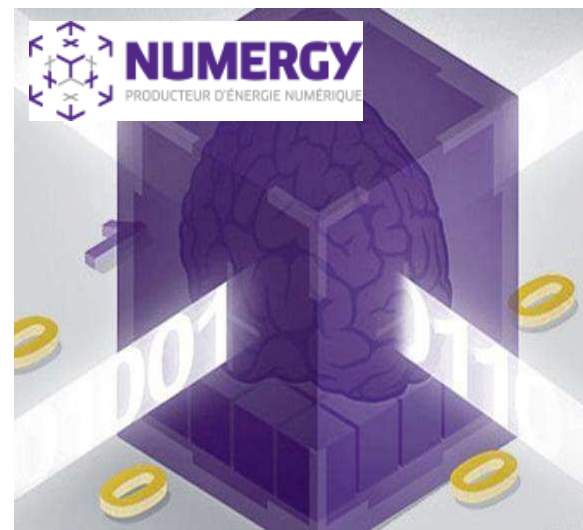


GasTerra - obchod se zemním plynem

- Monitoring a kontrola uživatelských přístupů nad více než 100 různými systémy a aplikacemi
- Založeno na integraci se SIEM službami
- SOC Analysts 24/7 připravený reagovat na kyber hrozby
- Měsíční reporting

NUMERGY – High-End cloud services

- Security Operations Center (SOC) dedikovaný pouze pro zákazníka a jeho potřeby
- Služby v režimu 24 x 7 x 365
- Výpočetní a Storage capacity



Agenda

Přístup ATOSu ke kybernetické bezpečnosti

S čím Vám ATOS může pomoci

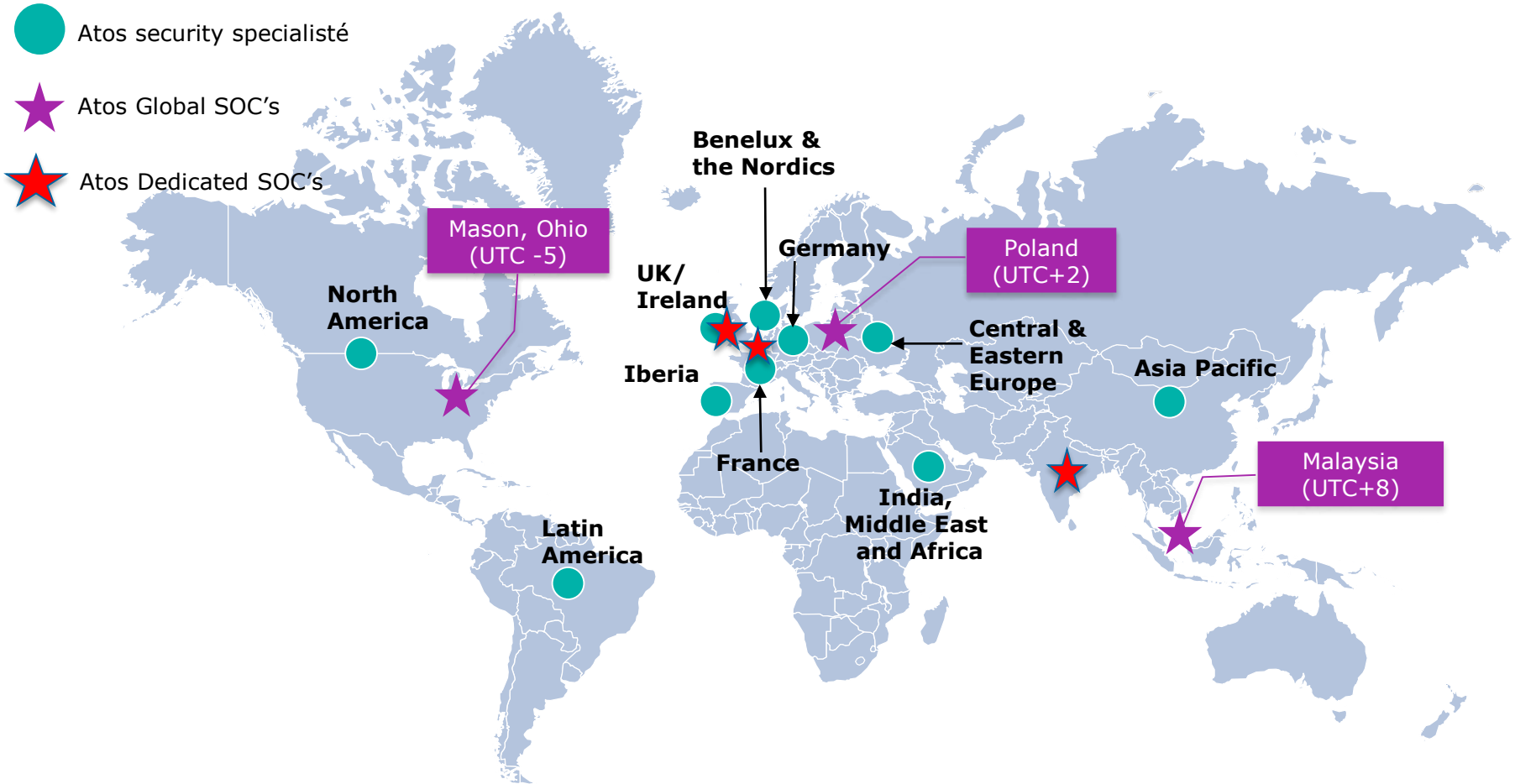
Co nás odlišuje?

Kontakty



Atos – Security Operations Centra

Poskytování SOC služby v režimu 24 x 7 x 365



**Atos SECURITY OPERATIONS CENTRA
jsou certifikována**

ISO 27001
MULTISITE
CERTIFICATE

ISO 20000
MULTISITE
CERTIFICATE

ISO 9001
MULTISITE
CERTIFICATE

Model kybernetické bezpečnosti

Jaké služby Vám jsme schopni poskytnout

Security Operations Center – L1, 7x24 onsite

- Communication
- Monitoring, alarms investigation & response
- CSIRT P3/P4 incident handling, communication, coordination, for all CSIRT incidents
- Vulnerability reporting
- 1st line activities cross all other GSS services

AHPS

L2/L3

Atos High Performance Security

5x10 business onsite
7x24 standby

Customer
onboarding
projects

Infrastructure
maintenance

CSIRT

L2/L3

Cyber Security Incident Response Team

5x10 business onsite
7x24 standby

Computer
Forensics

Cyber
Security
Incident
Management

Threat
Management

Endpoint and Perimeter Threat Management L2/L3

5x10 business onsite
7x24 standby

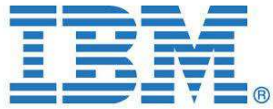
Vulnerability Management L2/L3

5x10 business onsite
7x24 standby

Identity & Access Management L2/L3

5x10 business onsite
7x24 standby

Atos – Váš partner pro bezpečnost



Agenda

Přístup ATOSu ke kybernetické bezpečnosti

S čím Vám ATOS může pomoci

Co nás odlišuje?

Kontakty



Shrnutí

Co poskytujeme a v čem se odlišujeme

OBLAST

ŘÍZENÍ BEZPEČNOSTI

KYBERNETICKÁ OCHRANA

PŘIPRAVENOST NA HROZBY

DIGITÁLNÍ IDENTITA A ŘÍZENÍ PŘÍSTUPU

BEZPEČNÁ KOMUNIKACE

KONKRÉTNÍ ŘEŠENÍ

Expertíza v bezpečnosti, IAM, ochraně dat, technické audity

Expertiza v integraci bezpečnostních technologií (McAfee, Qradar, Verint ATP)

6 Security Operations Center po celém světě z toho 3 v Evropě. Efektivita + redukce nákladů

Expertíza v Identity & Access Managementu
Návrh a integrace silných řešení Identity & Access Management Solutions (Evidian, DirX)

HSM and Crypto řešení
Inovativní řešení (Hoox)

Ne technologie, ale lidé a procesy

Co poskytujeme a v čem se odlišujeme



Znalost legislativy, norem, regulací

Zkušenost, znalost rozsahu, jaké metriky

Přehled o možnostech technologie

Účinnost zavedených opatření?

Jaká metrika?

Kybernetická bezpečnost jako řízená služba

Zaujali jsme Vás?

Tomáš Hlavsa
+420-604-290-196
tomas.hlavsa@atos.net
cz.atos.net
