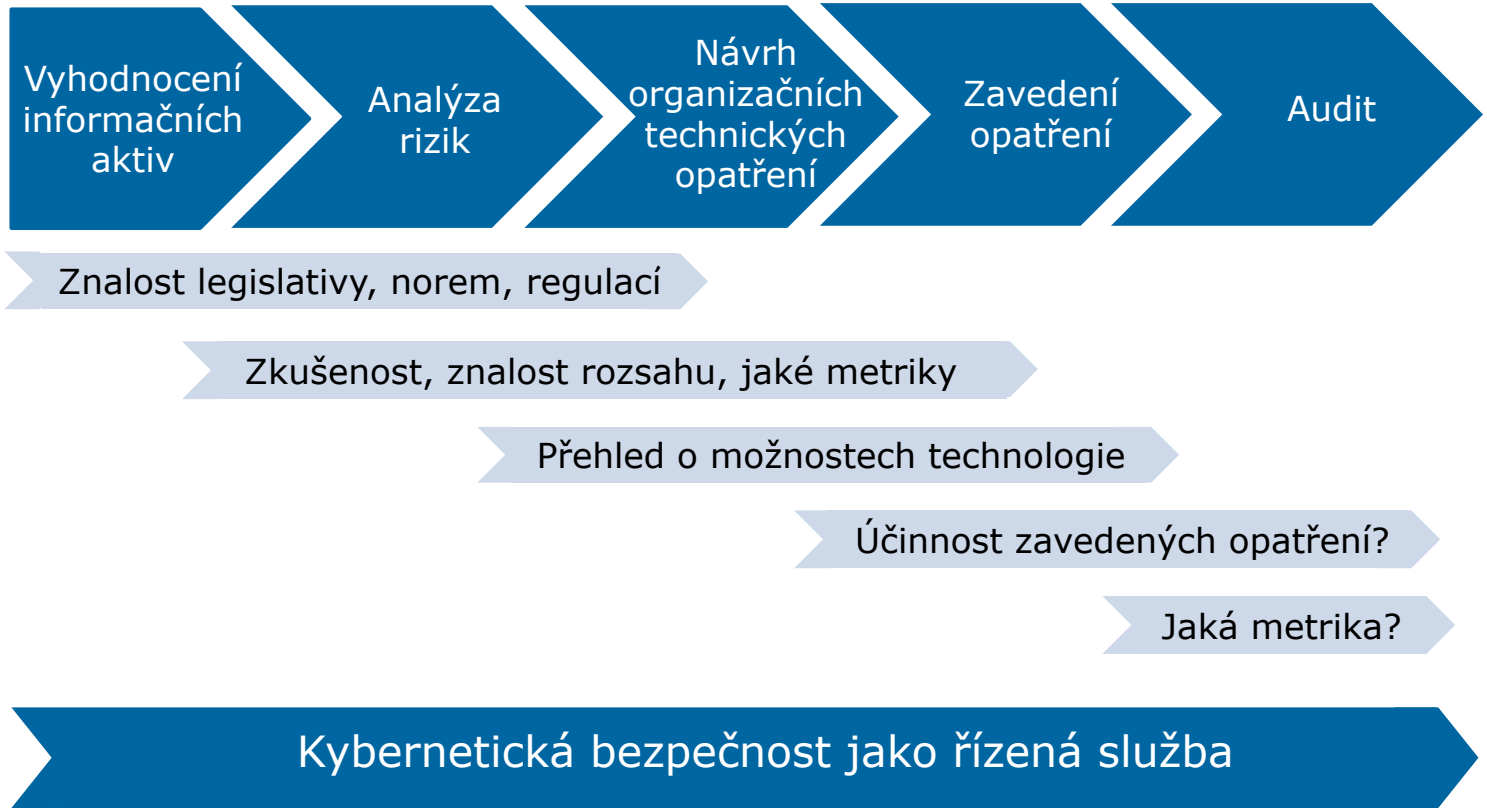
Výzvy kybernetickej bezpečnosti na Slovensku

Kde začít?

Investice do lidí versus Investice do technologií



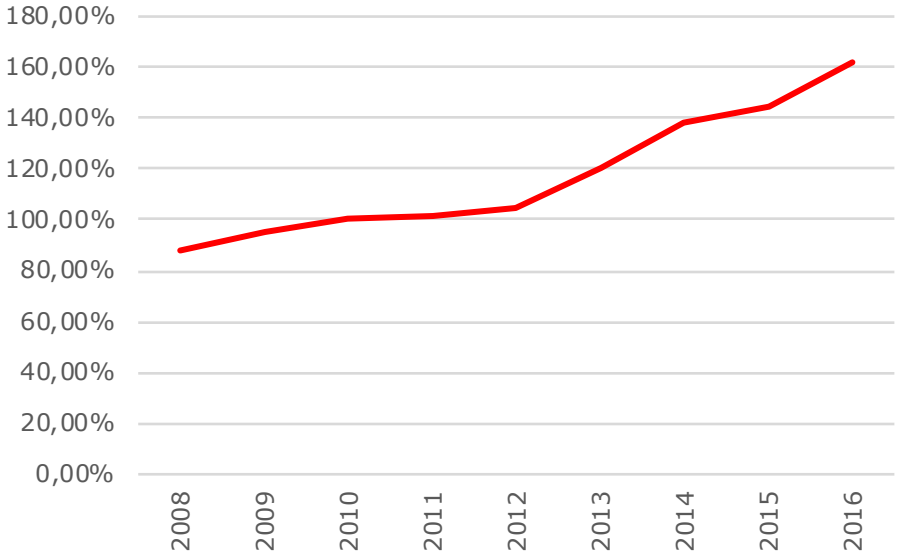
Lidé
Motivace x Kvalifikace

Kvalifikovaní nebo Motivovaní lidé

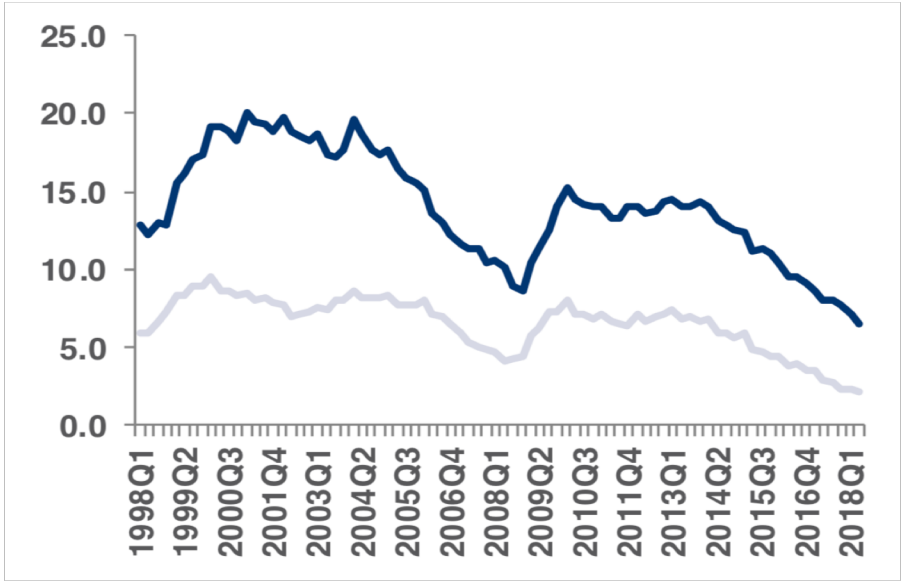
kybernetická bezpečnost jako ideální start pro absolventy

Atos CYBER security

Mzdy kvalifikovaných zaměstnanců



Nezaměstnanost



Atos

A když už motivovaného člověka najdete

…co ho budete chtít naučit?

Technické znalosti

Zkušenosti z obdobné pozice

Certifikace

CompTIA Security+

Anglický jazyk

B2 Common European Framework of Reference for Languages

Nástroje

Sentinel Training

NetIQ

NetIQ Sentinel

SIEM McAfee Training

McAfee

IBM Qradar Training

IBM QRadar

Jiné podobné nástroje?

Pracovní náplň

ITIL Foundation

- Event Mgmt
- Incident mgmt
- Change mgmt
- Problem mgmt

Interní procesy organizace na zvládání incidentů

Řešení incidentů

Rozsah monitoringu

Security Incident Response proceduresv

CSIRT Incident Management

Eskalační procedury

Management

Peníze
…a jde to bez nich?

Nejnižší nabídková cena se vymstí Zadavateli

13. **Hodnoticí kritéria a způsob hodnocení nabídek**

a. Základním hodnotícím kritériem pro hodnocení VZ je ve smyslu § 78 odst. 1 písm. b) ZVZ **nejnižší nabídková cena**.

b. Pro hodnocení nabídek je rozhodující **nejnižší celková nabídková cena v Kč včetně DPH.**

Název	Outsourcing role specialisty na kybernetickou bezpečnost
Druh veřejné zakázky	
Druh plnění	Služby
Kriterium Nabídková cena	
Název	Nabídková cena
Váha	100,00
Absolutní omezení hodnot	

Způsob podání nabídky

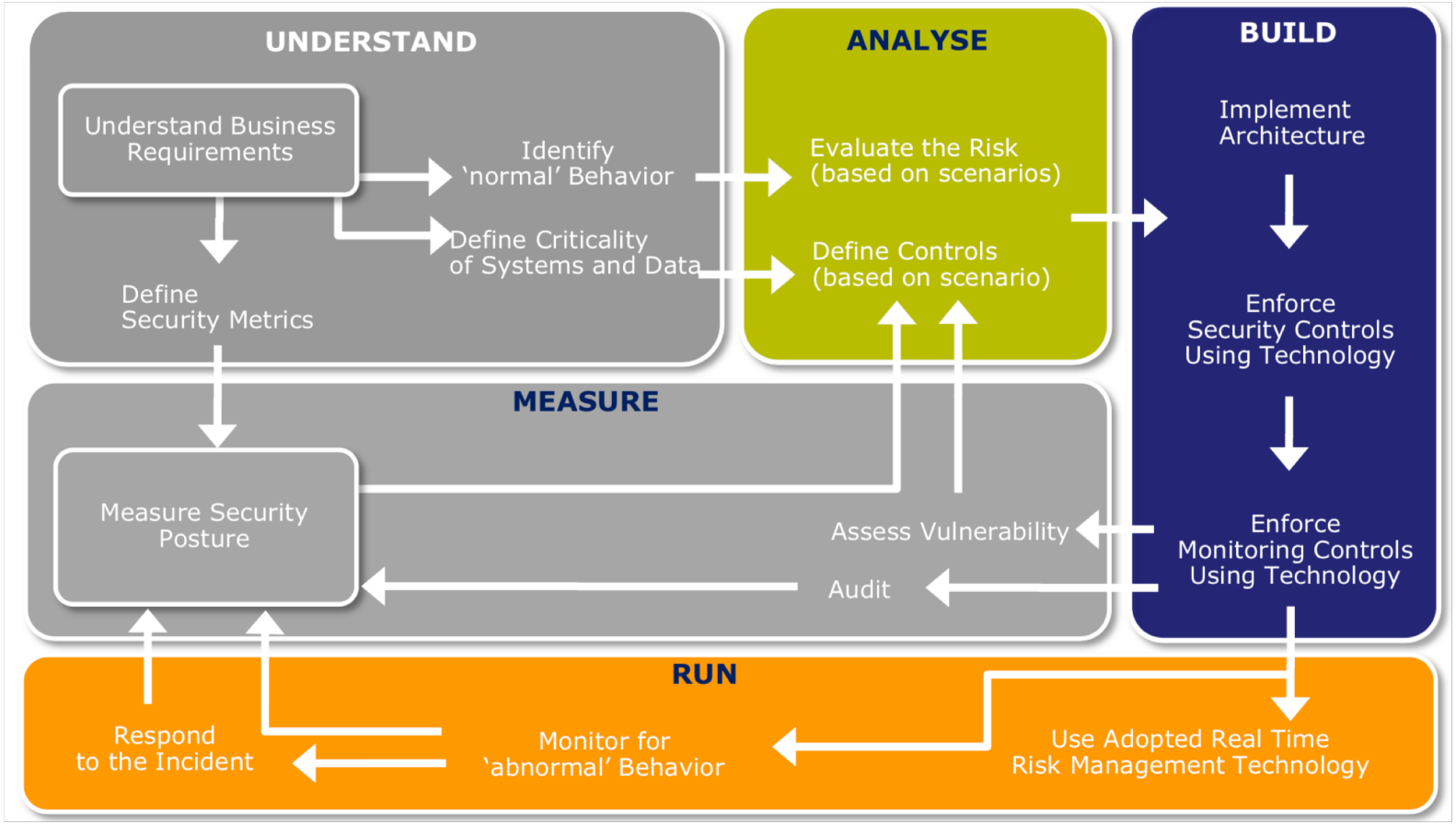
Dodavatel podává nabídku elektronicky pros

Specifikace hodnotících kritérií a metody hodnocení

Základní hodnotící kritérium Nejnižší nabídková cena

Procesy
.....milujeme procesy.....

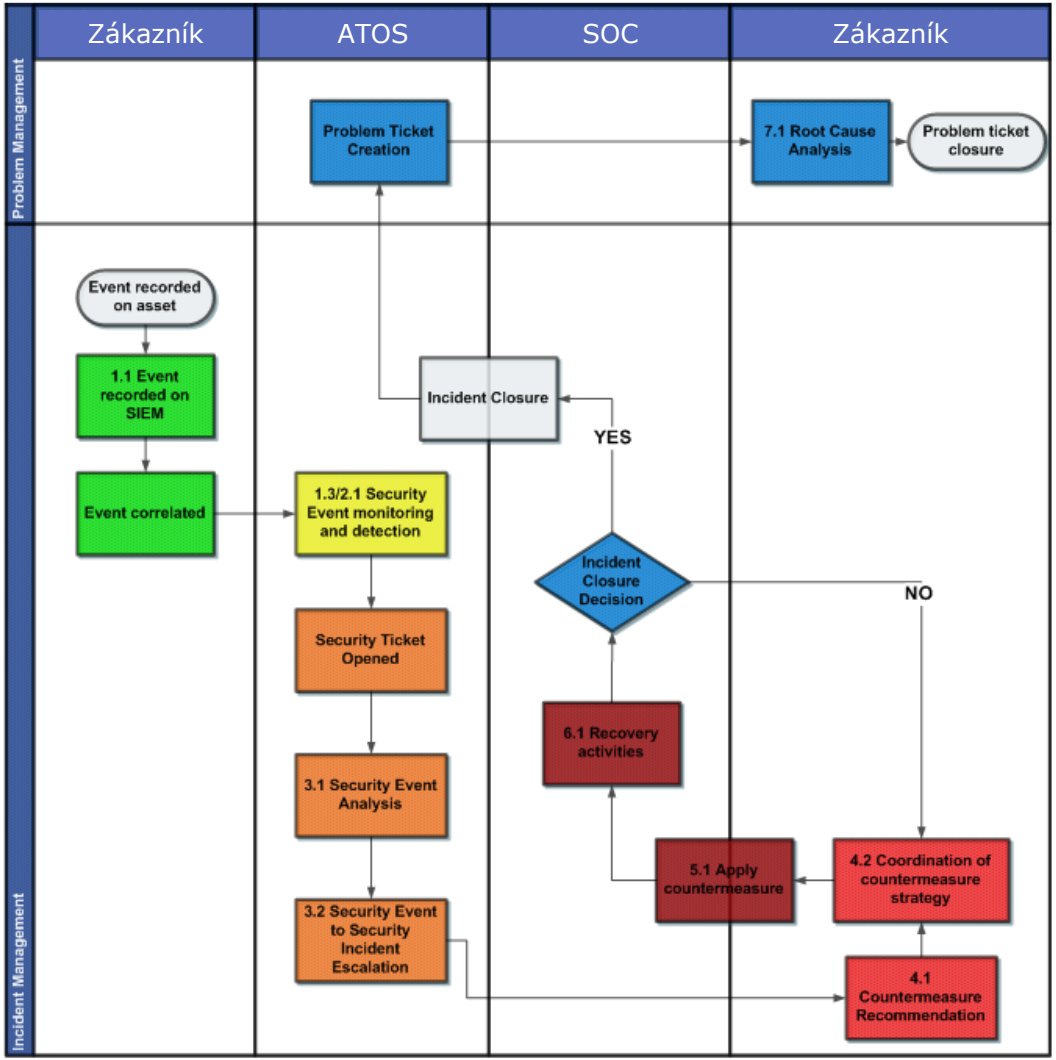
…a procesy….ty popsat umíte?



Odpovědnost

Odpovědnost

- Je definováno kdo je za co odpovědný?
- Kontrolujete to?
- Je odpovědnost vynutitelná?
- Zastupitelnost?
- Pracujete s motivací zaměstnanců?



Produkty
…ano ale až po….

Technologie, produkty, řešení

Zapomeňte na produkty

1. Co je ve Vaší organizaci důležité? Jaká aktiva?
2. Jak jste je chránili a nakládali s nimi do dneška?
3. Tužka a papír + hodina přemýšlení > než analýzy renomovaných firem

ATOS

….a kdo, když ne my …

ATOS - a to proč jako?

Přenos zkušeností ze zahraničí

(Polsko, Izrael, Francie …….)
(SOC centra, informační zajištění Olympijských her ….)

Vzdělávání

(eLearning, kontinuální vzdělávání …)

Bezpečnostní řešení nejen v oblasti CYBER

Národní bezp. integrátor (Švýcarsko, Francie ….)

Věda a výzkum

Bezpečnostní výzkum, H2020 ……

Síla největší evropské IT firmy

Kapacitní pokrytí,
expertiza, partnerská síť

ATOS - milujeme bezpečnost

10 základních bezpečnostních

1. Buďte odpovědní

Atos zavedl systém řízení bezpečnosti, který zahrnuje aspekty ochrany dat, fyzickou bezpečnost, ochranu zdraví a majetku. Všechna aktiva (data, majetek, dokumenty, výrobní prostředky, intelektuální vlastnictví) Atosu, jakožto aktiva zákazníků, musí být adekvátním způsobem chráněna vůči známým hrozbám. Proto Atos definoval pravidla a směrnice, které byste měli znát a řídit se jimi. Všechny naleznete na Sharepointu v sekci Organization - Support functions - Group security.

2. Hlašte bezpečnostní incidenty

Bezpečnostní incidenty musí být bezodkladně hlášeny. Ať jde o incidenty fyzické bezpečnosti, informační bezpečnosti nebo incidenty ochrany zdraví. Cílem je především bezpečnost a zdraví zaměstnanců. Teprve poté bezpečnost a ochrana majetku společnosti Atos. Seznamte se se směrnicí „Jak hlásit bezpečnostní incidenty".

5. Při používá e-mailu a in buďte opatr

Víceméně všechny druhy m mohou být součástí e-mailu n stránek. Nikdy neotevírejte er která vypadá podezřele. Poz sítě, pohyb na nich není an zranitelnější než si myslít soubory z nedůvěryhodných či neautorizovaných strá obsahovat škodlivý software. odkazy v nevyžádaných e-mai obsahovat hrozby typu p

6. Chraňte vaše koncová zařízení (notebook, smartphone, tablet)

Zálohy jsou jediným rozumným způsobem, jak obnovit ztracenou, či poškozenou informaci. Ujistěte se, že všechny relevantní informace ukládáte na servery, které jsou automaticky zálohovány. Notebooky, tablety a mobilní telefony, které opouští prostředí Atosu, jsou velmi zranitelné a hodnota ztraceného hardwaru je často mnohem

9. pravidla a opatření v Atos prostorách

Každý zaměstnanec má jeden či více vstupních průkazů opravňující přístup do prostor Atosu. Noste vstupní karty viditelně. Každý zaměstnanec je odpovědný za své návštěvy. Návštěvníci bez řádných vstupních průkazů nezůstávají po dobu svého pobytu v prostorách Atosu bez doprovodu. Neváhejte nabídnout neznámým, či neoznačeným osobám svůj doprovod na recepci.

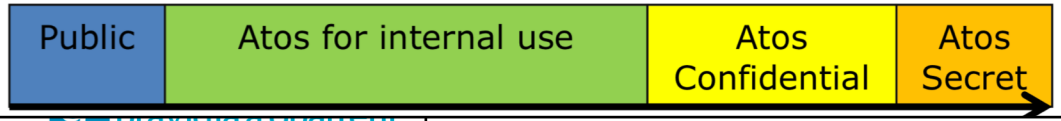
Information Classification Scheme

This document specifies the classification attached to Atos Information and how it must be treated through its life from creation to disposal. Atos staff who handle classified documents belonging to customers must handle them in accordance with the customer's classification standard. When a security policy, procedure or process is absent at a customer location, staff should propose to the customer to follow this standard.

All information must be classified by the owner or author as either:

1. Public;
2. Atos for internal use;
3. Atos Confidential;
4. Atos Secret.

By default, any information whose classification is not explicitly defined is presumed to belong to the "Atos for internal use" classification.



Thanks

For more information please contact:
tomas.hlavsa@atos.net
+420 604 290 196

Atos