Visitech

SOC 365
Security Operation Center

VYUŽITÍ SECURITY OPERATIONS CENTER VE VEŘEJNÉ SPRÁVĚ

Ing. Pavel Meletzký, MBA

pavel.meletzky@visitech.cz

30 let praxe v ICT

oblastní ředitel VISITECH a.s.

člen Finančního výboru MSK

předseda Komise informatiky Rady Statutárního města Opavy

#1 BEZPEČNOSTNÍ CENTRUM V ČR

Jaký je stav kybernetické bezpečnosti v ČR?

… píííííp …

Panika na trhu s elektřinou. Někteří dodavatelé odmítají nové zákazníky a skrývají ceníky

Jaké bylo mládí lídrů? Babiš u koní, Šlachta za bicími nebo Bartoš s autíčkem

Od autora Skleněného pokoje: audiokniha Dívka, která spadla z nebe zdarma

Hrad se stal terčem kybernetického útoku. Data šla k hackerům do zahraničí

Fotogalerie +4

3. března 2020

Kybernetický útok stál nemocnici v Brně desítky milionů, klesly odběry krve

17. dubna 2020 10:12

Fakultní nemocnici Brno vznikla při březnovém kybernetickém útoku škoda v desítkách milionů korun. Nemocnice přišla například o některá administrativní a ekonomická data nebo o internetový objednávkový systém u dárců krve. Objednala nový, fungovat by měl do dvou týdnů.

Vstup do Fakultní nemocnice Brno v Bohunicích | foto: Filip Bednář

Kybernetický útok na olomoucký magistrát. Jaká je právě situace?

V Česku se zastavila těžba černého uhlí. Počítače OKD ochromil hackerský útok

ČESKO

Hackeři vydírají české nemocnice. Třetina zařízení čelila útokům, které ohrožují i péči o pacienty

Fotogalerie +5

DNES V LN

Loni v červnu se vedení Léčebny tuberkulózy a respiračních nemocí v Janově na Rokycansku probudilo do nepříjemného dne. Počítačové systémy nemocnice se 170 lůžky napadli hackeři. Zablokovali důležitá data a za jejich uvolnění požadovali výkupné ve virtuální měně bitcoin.

Martin Shabu 5. listopadu 2019 5:00

DENÍK N

2. srpna 2019 6:25

Novým terčem kybernetických útočníků jsou města. Příště možná i to vaše

PETR ŠPIŘÍK + Odebírat e-mailem

Kyberútok na nemocnici v Benešově způsobil škodu přes 59 milionů. Pachatele se vypátrat nepodařilo

Loňský kybernetický útok na Nemocnici Rudolfa a Stefanie Benešov způsobil škodu přes 59 milionů korun. Pachatele se nepodařilo dohledat, policie případ odložila, informovala v úterý policejní mluvčí Barbora Schneeweissová.

AKTUALIZOVÁNO Benešov 9:12 18. 8. 2020 (Aktualizováno: 9:49 18. 8. 2020)

Ilustrační foto | Foto: Fotobanka Pixabay

ČTENÍ +

Kybernetických útoků přibývá a Česko na ně není připravené, shodují se odborníci



4 fotografie

Hackeři využili karantény a útočí, zaměstnanci na home office se neumí bránit

3. dubna 2020


Řidič nabourал do stojících aut, v převráceném voze se zranil malý chlapec


Spojení na letiště a do Kladna se prodraží o 10 miliard, stavba začne napřesrok

Jaké bylo mládí lídrů? Babiš u koní, Šlachta za bicími nebo Bartoš s autíčkem

Hackeři napadli informační systémy městské části Prahy 3 a Povodí Vltavy

7. dubna 2020 20:04

V úterý napadli hackeři informační systémy městské části Prahy 3 i státního podniku Povodí Vltavy. Nutné fungování podniku bylo zachované, nedošlo ani k ohrožení přehrad či dodávek povrchové vody. Úřad městské části bude kvůli kybernetickému útoku ve středu uzavřen.

Impozantní je stavba především v noci, kdy je osvětlena. | foto: Tomáš Krist, MAFRA

DOMOV

Další kybernetický útok v Česku. Hackeři zasáhli Povodí Vltavy

HACKERSKÝ ÚTOK

ECHO24, ČTK 7. dubna 2020

Na informační systém státního podniku Povodí Vltavy v úterý zaútočili hackeři. Napadli systém pro administrativní činnosti – nefungovaly tak maily nebo spisová služba a další interní systémy. Přehrady nebo

Německá generální prokuratura začala vyšetřovat kybernetické útoky, které úřady připisují Rusku

Generální prokuratura v Německu ve čtvrtek uvedla, že začala vyšetřovat kybernetické útoky proti německým politikům, které úřady připisují hackerské skupině Ghostwriter napojené na Rusko. Učinila tak na základě informací dodaných tajnými službami, informovala agentura DPA s odvoláním na sdělení státního zastupitelství v Karlsruhe. Moskva nařčení odmítá.

Karlsruhe (Německo)/Moskva 21:40 9. září 2021

SVĚT

Na náš obranný průmysl útočili hackeři z KLDR, oznámil Izrael

KYBERNETICKÉ ÚTOKY

Podle Washingtonu skupinu Lazarus ovládá severokorejská vojenská rozvědka RGB. Foto: Shutterstock

ECHO24, ČTK 13. srpna 2020

Hackeři útočí na instituce, které bojují proti koronaviru, hlásí USA a Británie

5. května 2020 21:32

Hackeři, které nejspíše podporují zahraniční vlády útočí na orgány a instituce zapojené do boje proti covid-19, ať už na národní či mezinárodní úrovni. V úterý to uvedly americká a britská agentura pro kybernetickou bezpečnost. Pachatelé zřejmě cílí na zdravotnické orgány, dále pak na farmaceutické společnosti či lékařské výzkumné organizace.

ilustrační snímek | foto: Depositphotos

Využívají při tom metodu označovanou jako „kropení hesel“, což znamená, že se snaží proniknout do interních systémů aplikováním databáze často používaných přístupových klíčů jako jsou „123456“ nebo „qwerty“.

Kdo bude další?

Otázka nezní, zda se Vám to stane,

ale kdy se Vám to stane!

Zpráva NUKIB za měsíc říjen

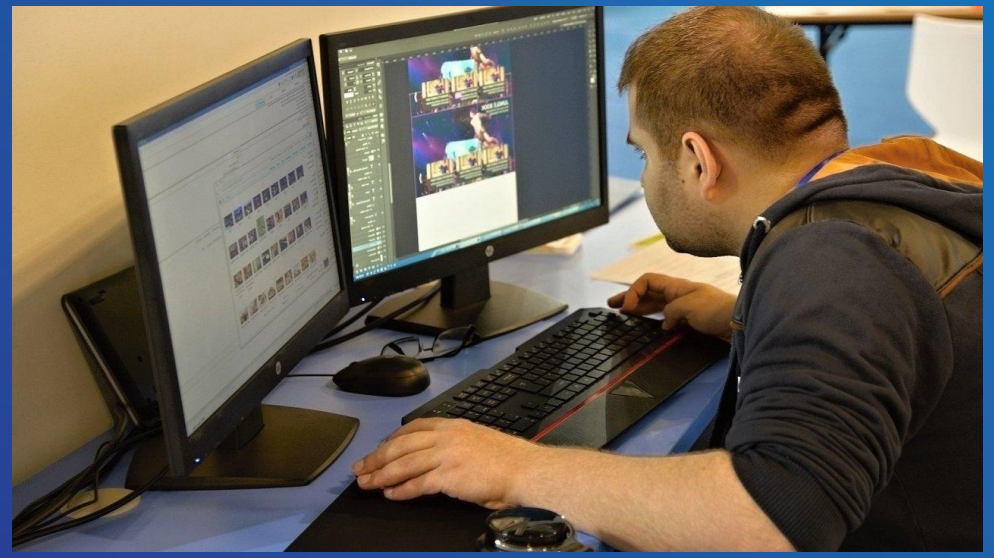
- *Říjen se co do počtu incidentů stal druhým nejrušnějším měsícem tohoto roku.*
- *Podobně jako v předchozích měsících se v hlášení objevovaly DDoS útoky, phishingové kampaně nebo škodlivé kódy v sítích českých organizací. Mezi incidenty byl také jeden ransomware, který zašifroval část infrastruktury oběti a následně na svých stránkách vyhrožoval zveřejněním jejích dat.*
- ***Počet incidentů neustále narůstá a zároveň se zvyšuje i jejich sofistikovanost.***

Zdroj: Národní úřad pro kybernetickou a informační bezpečnost

Co útoky přinášejí?

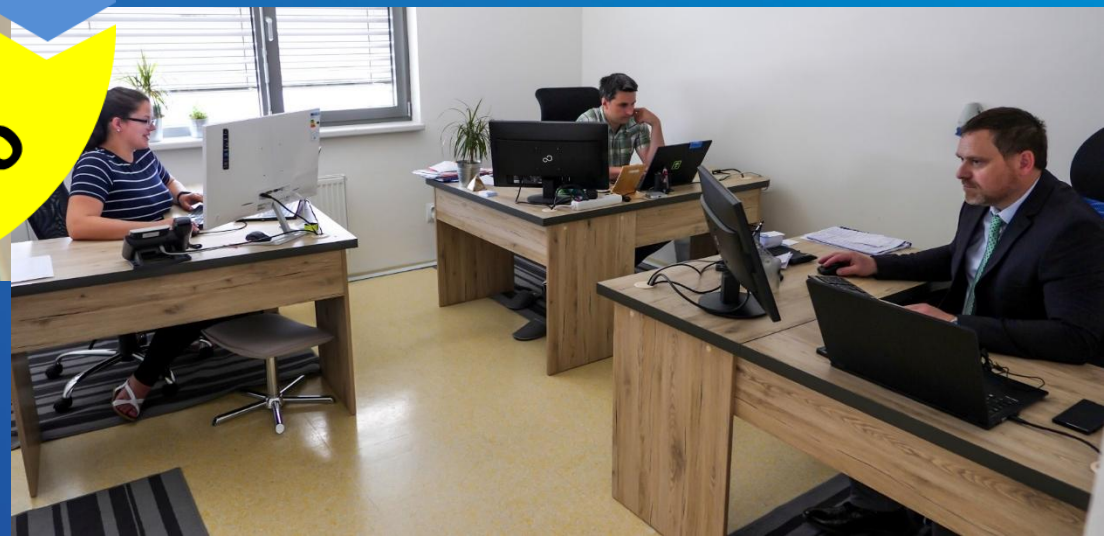
- *Škody řádově stovky miliónů Kč*
- *Všeobecný zájem o téma*
- *Zjištění, že veřejná správa JE závislá na ICT*
- *Zjištění, že skoro vše je závislé na ICT*

Zdroj: Adam Kučínský, NUKIB
Ředitel Odboru regulace




MEET
THE
PRESS

Bezpečnostní dohledové centrum SOC365



Jaké jsou možnosti veřejné zprávy pro zajištění kybernetické bezpečnosti?

1. *Nic neřešit, zůstat v současném stavu, čekat a doufat*
2. *Pokrýt zajištění kybernetické bezpečnosti vlastní silou, vlastními zdroji*
3. *Využít k zajištění kybernetické bezpečnosti partnera, využít službu*

Jak to tedy vypadá v praxi, pokud řešíte vlastní SOC?

TAKŽE:

- *Vytvořili jsme koncepci*
- *Vytvořili jsme partnery*
- *Popsali jsme současný stav*
- *Navrhli jsme cílový stav*
- *Spočítali a porovnali jsme to*

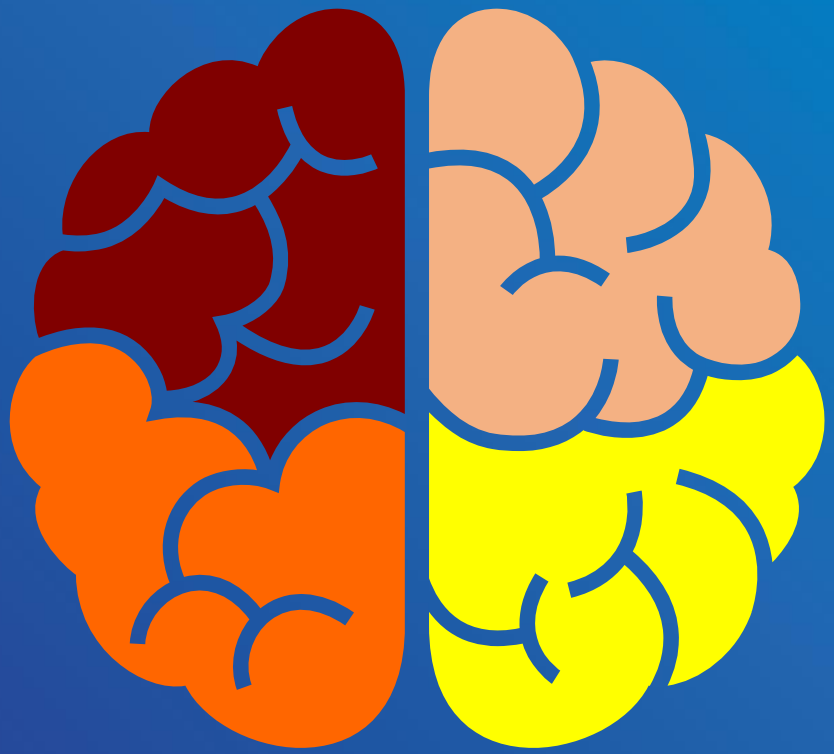
Zdroj: Ing. Dušan Chvojka, MBA
Náměstek ředitele pro informační technologie
NEMOCNICE NA HOMOLCE

SOC 365
Security Operation Center

– Jak to děláme?

SOC 365
Security Operation Center

– Jak to děláme?



SOC 365 – Jak to děláme?

Security Operation Center

Funkčnost

- Zajistíme **funkčnost** Vaší sítě v celém jejím spektru – od komunikace k procesům.

Nastavení

- **Pomůžeme Vám nastavit správné provozní prostředí** a umíme jej pravidelně optimalizovat.

Jsme o krok napřed

- Víme co se děje v sítích. Umíme **předcházet nežádoucím stavům.**

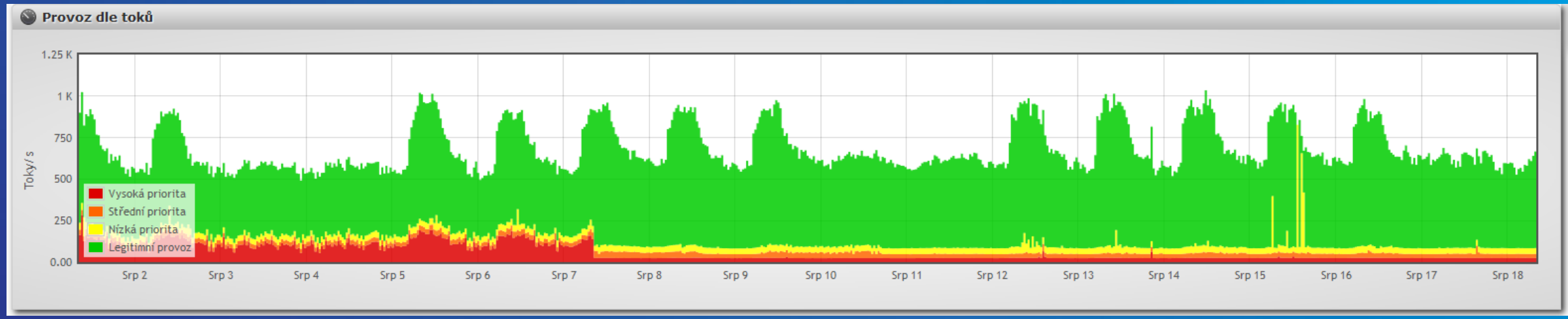
Interpretace

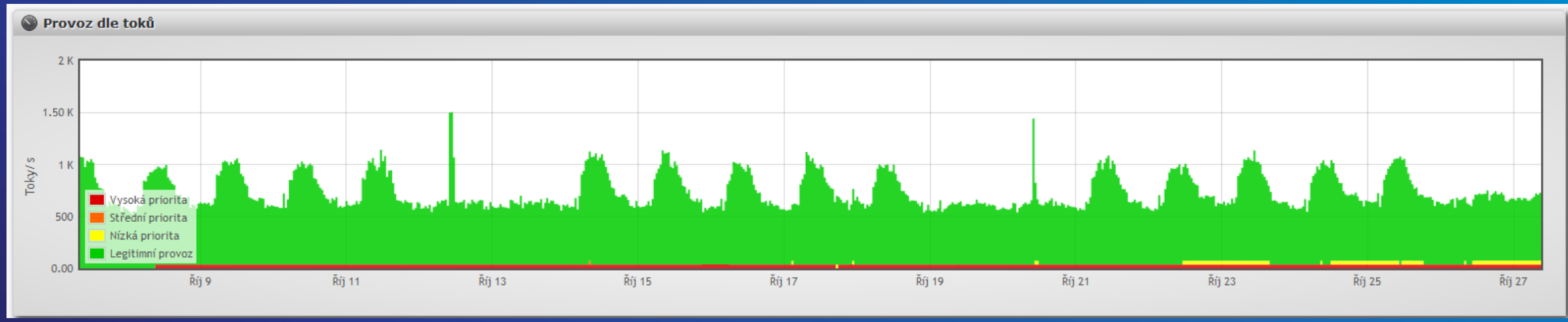
- Poznáme falešné poplachy, **umíme správně interpretovat** různé stavy ve Vaší síti.

SOC 365
Security Operation Center

– Jak to děláme?

Odladění – vyladění všech systémů

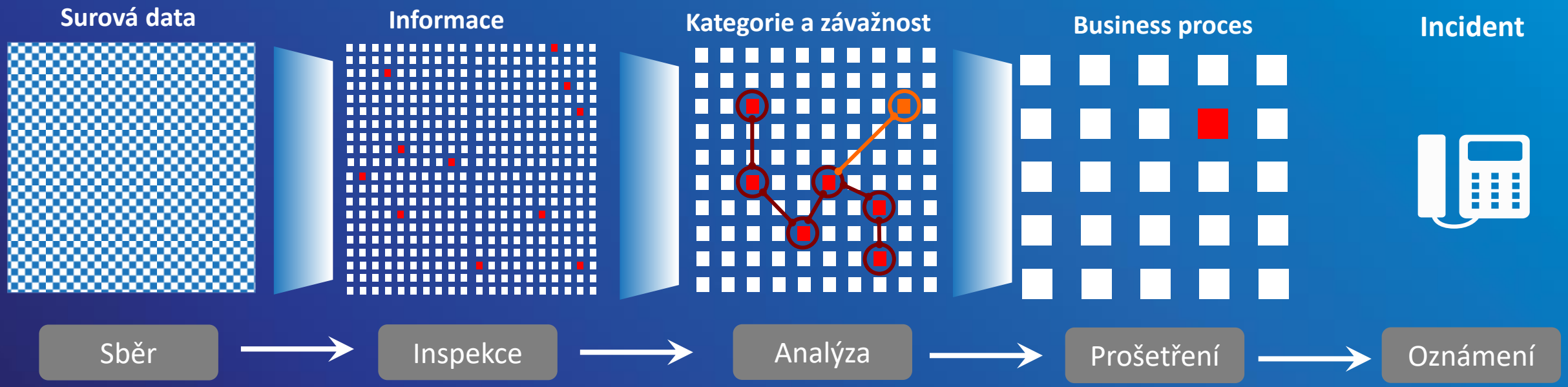




SOC 365
Security Operation Center

Analytický postup zpracování

1. Z neviditelných dat tvoříme **Parsingem** a **Filtrováním** viditelné informace.
2. Viditelné informace přes **Inspekci** vkládáme do kategorií.
3. **Analýzou** kategorií stanovujeme kořenovou příčinu nebo následky.
4. **Prošetřením** kořenové příčiny **Oznamujeme** kompetentní osobě relevantní nález.



DOHLED NENÍ SOC!

Dohled:

„Spadnete na ledu a bolí Vás ruka“

- *Rentgen ruky -> zlomenina*
- *Sádra*
- *Neschopenka*
- *Kontrola za 3 týdny*
- *Vyřešeno!*

SOC:

„Spadnete na ledu a bolí Vás ruka“

- *Rentgen -> zlomenina*
- *Návrh inovativního způsobu léčby zlomeniny, návrh podpůrné léčby*
- *Celkové CT, zda nedošlo k dalšímu zranění*
- *Hledání příčiny, proč došlo ke zlomenině*
- *Analýza celkového stavu pacienta*
- *Doporučení, jak další zlomenině předejít*
- *Umístění „možnosti zlomeniny“ do rizikové skupiny a upozorňování pacienta na rizikové aktivity*
- *Průběžná kontrola pacienta*
- *Hlídáno!*

Bezpečnostní zpráva = report

Strojový report vs. Bezpečnostní zpráva v interaktivním grafickém zobrazení

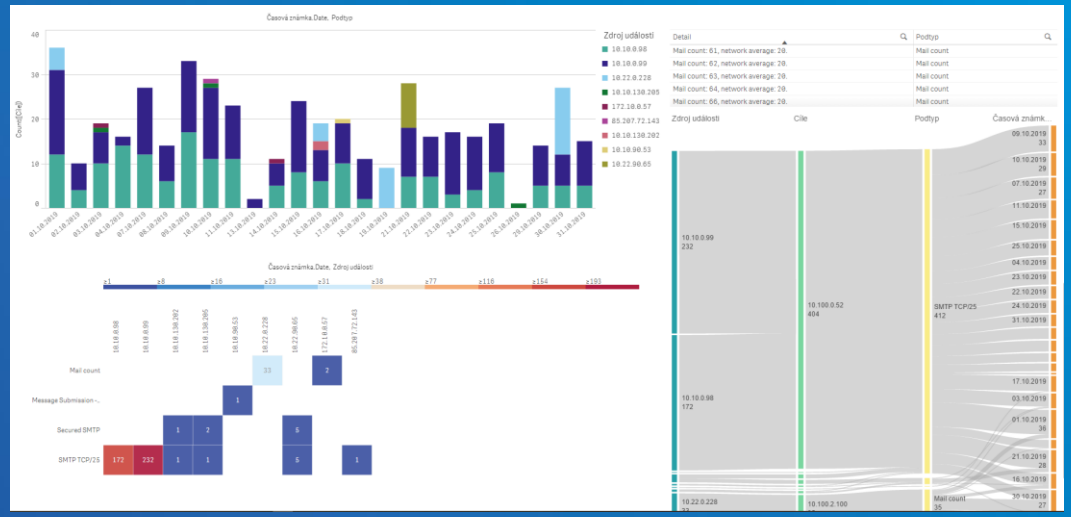
- MANAŽERSKÝ SOUHRN
- SOUHRNNÁ PODROBNÁ TECHNICKÁ ZPRÁVA
  - Podrobný popis bezpečnostních incidentů a seznam všech řešených ticketů
  - Bezpečnostní zjištění v rámci SIEM technologie
  - Bezpečnostní zjištění v rámci monitoringu datových toků
  - Bezpečnostní zjištění v rámci vnějšího scanu zranitelnosti
  - Bezpečnostní zjištění v rámci vnitřního scanu zranitelnosti

Bezpečnostní zpráva = report – PŘÍKLAD POŽADAVKU

Analýza příchozí komunikace do interní sítě

Zadavatel požaduje souhrnnou Analýzu příchozí komunikace do interní sítě v minimálním rozsahu:

- Graf dle názvu anomálií
- Graf nejčastějších zdrojových IP adres
- Graf nejčastějších cílových IP adres
- Graf nejčastějších cílových portů
- Graf dle nejčastějších názvů služeb
- Distribuční graf
- Souhrnný relační graf
- Graf nejčastějších zdrojů příchozí komunikace v závislost na geolokaci



ZÁVĚREČNÝ SOUHRN

- *Vybírejte z CERTIFIKOVANÝCH SOCů (min. požadavek na CSIRT tým)*
- *Požadujte fyzickou prohlídku SOCu*
- *Zvažte, zda požadujete nákup HW nebo službu*
- *Striktně trvejte na ODDĚLENÍ A NEZAMĚNITELNOSTI JEDNOTLIVÝCH ROLÍ (operátor, analytik, architekt, manažer kybernetické bezpečnosti)*
- *Vyzkoušejte službu v rámci min. 3 měsíčního PoC (proof of concept)*
- *Důsledně si vydefinujte požadované výstupy Bezpečnostní zprávy = reportu (za to si platíte)*
- *Požadujte předložení ANONYMIZOVANÉ Bezpečnostní zprávy*

Děkuji za pozornost

www.visitech.cz