cesnet

Role SOC v organizaci

Jan Kolouch
Andrea Kropáčová
CESNET

7. února 2023
Seminář o bezpečnosti sítí a služeb 2023

cesnet

SOC?

https://www.escapeall.gr/en/EscapeRoom/Details/the-holy-grail

http://qbhackers.com/how-to-build-and-run-a-security-operations-center/

cesnet

SECURITY/SAFETY

IDEÁLNÍ CÍL BEZPEČNOSTI?

vytvoření stavu **„absolutního bezpečí“.**

Utopie…

Stavu není možné reálně dosáhnout. **Vždy bude existovat hrozba či riziko,** které nebylo do konceptu tvorby bezpečnosti zahrnuto, nebo bylo záměrně opomenuto.

cesnet

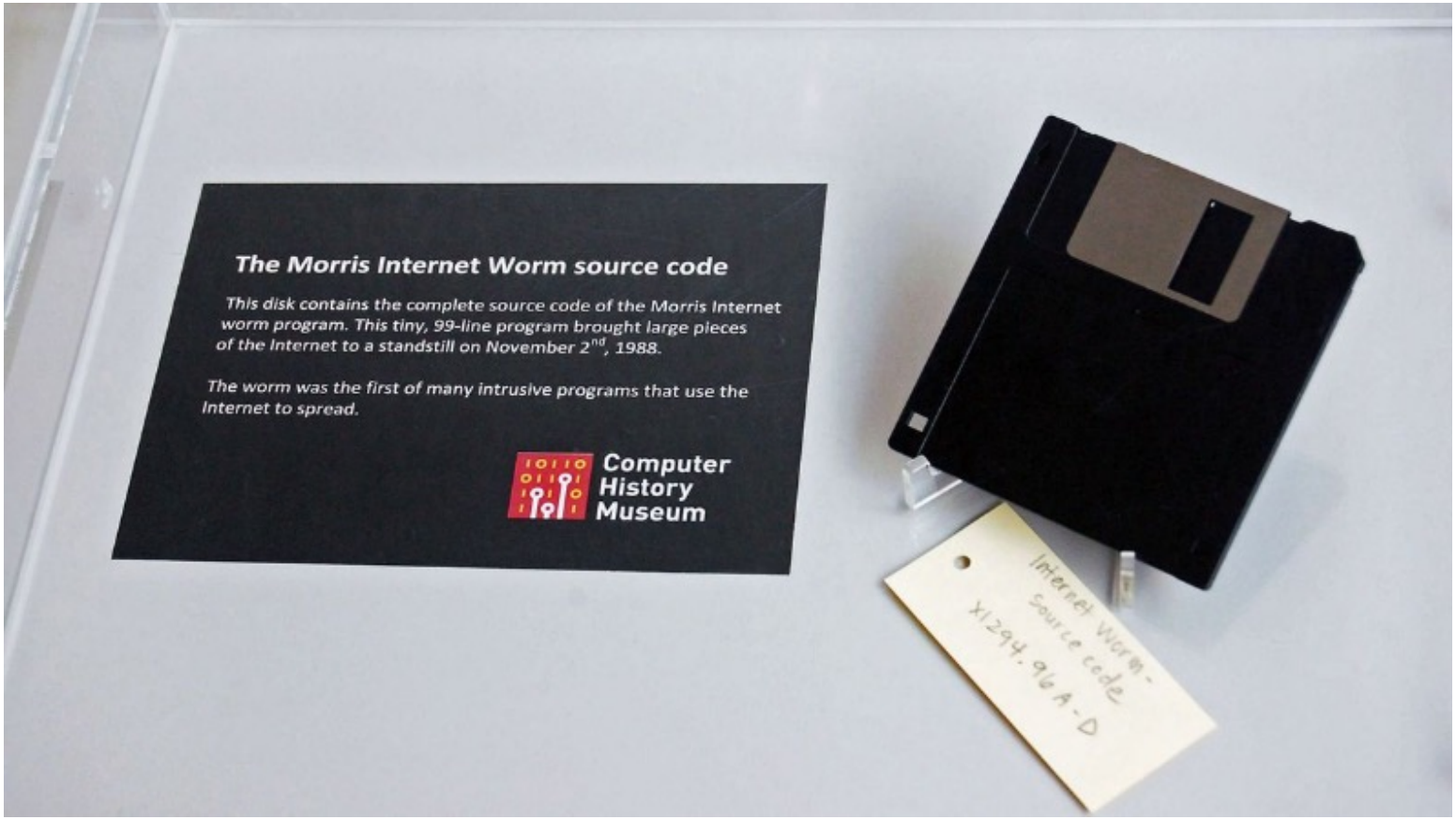
CO JE TŘEBA ŘEŠIT?

- **O čí bezpečnost se jedná** (mezinárodní organizace, stát, organizace, jednotlivec aj.)**?**
- **Jaké hodnoty jsou chráněny** (organizace, osoby, data aj.)**?**
- **Před čím jsou (mají být) tyto hodnoty chráněny** (fyzické, kybernetické, kombinované útoky aj.)**?**
- **Jaké prostředky je třeba vynaložit k ochraně těchto hodnot?**
- **Umožním někomu jinému řešit moji bezpečnost místo mě** (do jaké míry/úrovně aj.)**?**

cesnet

GENEZE

2.11.1988 (ROBERT TAPPAN MORRIS)



https://www.kaspersky.com/blog/morris-worm-turns-25/3065/

cesnet

CARNEGIE MELLON UNIVERSITY

cesnet

BEZPEČNOSTNÍ TÝM VS. CERT/CSIRT

- reakce na hrozbu („***response***“)
- **spolupráce**
- **koordinace činností** při řešení incidentů

- zapojení do **světové bezpečnostní komunity**
- **sdílení informací** v rámci této komunity
- dodržování **stanovených formálních postupů**
- ověření stupně vyspělosti týmu (SIM3 CSIRT Maturity model)

*...**souhrn** organizačních, politických, právních, technických a vzdělávacích **opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru...***

https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

http://zpravy.ckait.cz/vydani/2020-01/lze-stavet-zaroven-rychle-levne-a-kvalitne/

cesnet

SOC!

Buzzword/Ultimátní řešení/Cesta/Holy Grail?

https://www.youtube.com/watch?v=O-t0WjiQg48

DEFINICE

CISCO

SOC je služba/činnost při které dochází k:

- identifikování,
- ochraně,
- detekci,
- reakci,
- obnovení

ve vztahu ke kybernetickým hrozbám či incidentům

IBM

Interní/externí tým odborníků zabývajících se bezpečností IT,

(24/7) monitoruje celou ICT infrastrukturu organizace, aby v reálném čase zjišťoval kybernetické bezpečnostní události a tyto řešil co nejrychleji a nejefektivněji. **Činnosti SOC lze rozdělit do kategorií:**

- příprava, plánování a prevence
- monitoring, detekce a reakce
- obnova, zdokonalení se a respektování právních norem (compliance).

MITRE

tým bezpečnostních analytiků schopných:

- detekovat
- analyzovat
- reagovat
- podávat zprávy
- předcházet

kybernetickým bezpečnostním incidentům.

Symantec

Cyber Defense Center. Bezpečnostní politiky jako služby. **Katalog služeb**. Hlavní kategorie služeb CDC zahrnují:

- Strategické řízení CDC,
- Analýza v reálném čase,
- Hloubková analýza,
- Reakce na incidenty,
- Kontrola a vyhodnocení,
- Shromažďování, analýza a vyhodnocování zpravodajských informací o hrozbách,
- Vývoj a údržba platforem CDC,
- Podpora interní reakce na podvody,
- Aktivní vztahy s externími stranami.

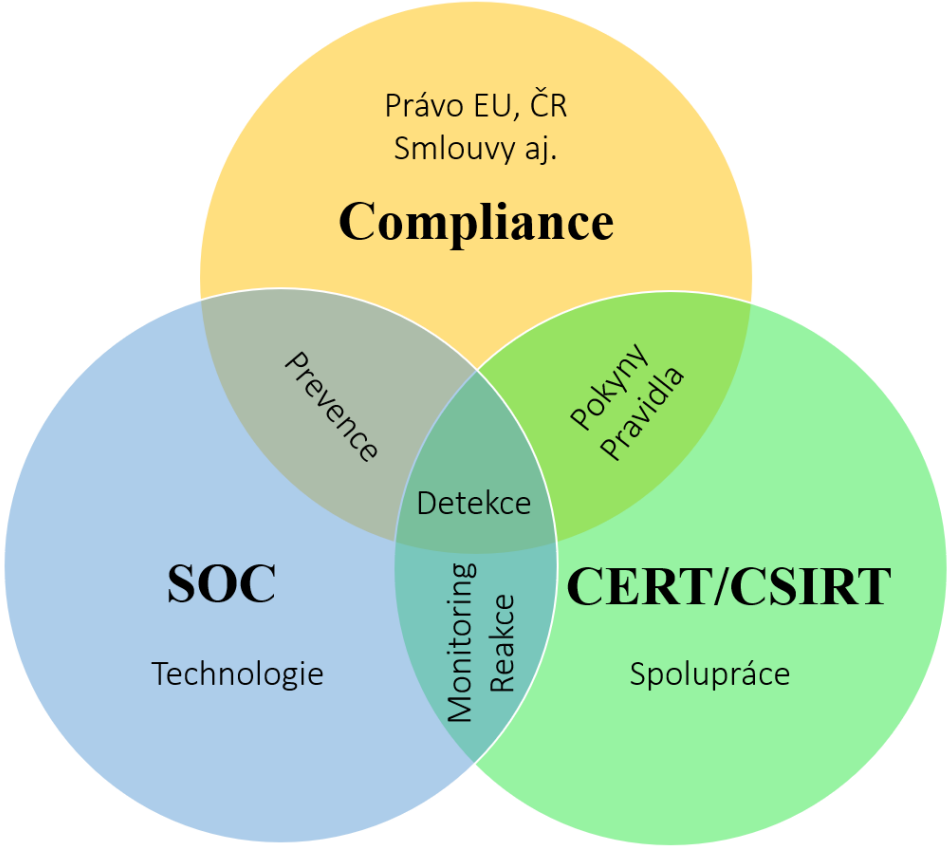
relativně komplexní prostředí implementující triády:

1. Lidi, Technologie a Procesy

2. Prevence, Detekce a Reakce

+

Compliance



Účel

- Sběr dat,
- Analýza dat,
- Detekce definovaných událostí,
- Threat Intelligence,
- Budování situačního povědomí,
- Reakce na kybernetické bezpečnostní události a incidenty,
- Reportování,
- Edukace aj.

ÚČEL/ROZSAH/CÍL

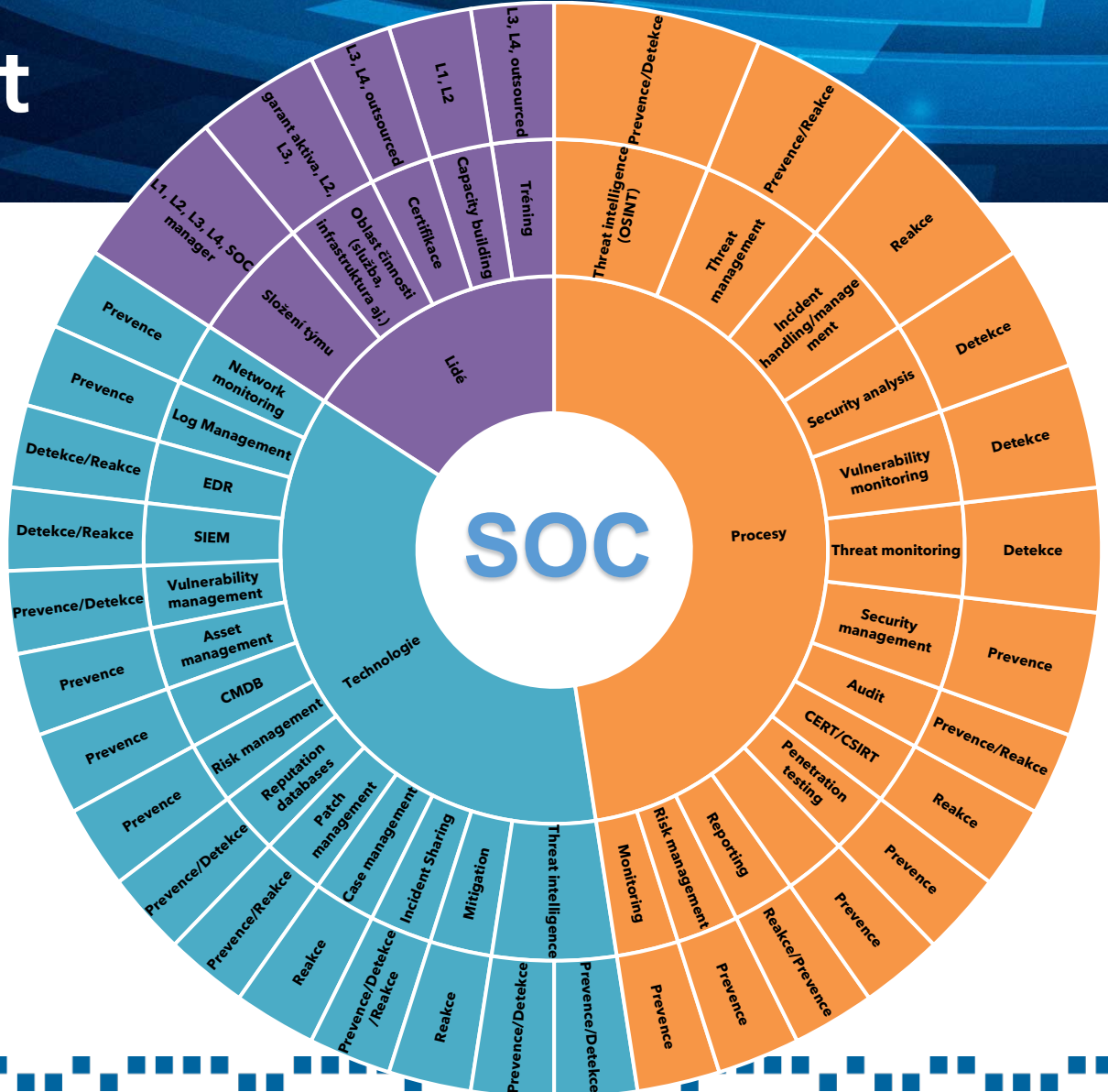
Rozsah

- Organizace jako celek,
- Určená infrastruktura,
- Definované služby,
- Kompetence aj.

Cíl

- Monitoring a predikce (tj. prevence),
- Reakce a eskalace

cesnet


SOC
Lidé
Složení týmu
L1, L2, L3, L4, SOC manager
garant aktiva, L2, L3,
L3, L4, outsourced
Oblast činnosti (služba, infrastruktura aj.)
L1, L2
Certifikace
L3, L4, outsourced
Capacity building
Trénink
Procesy
Threat intelligence (OSINT)
Prevence/Detekce
Threat management
Prevence/Reakce
Incident handling/management
Reakce
Security analysis
Detekce
Vulnerability monitoring
Detekce
Threat monitoring
Detekce
Security management
Prevence
Audit
Prevence/Reakce
CERT/CSIRT
Reakce
Penetration testing
Prevence
Reporting
Reakce/Prevence
Risk management
Prevence
Monitoring
Prevence
Technologie
Threat intelligence
Prevence/Detekce
Mitigation
Reakce
Incident Sharing
Prevence/Detekce/Reakce
Case management
Reakce
Patch management
Prevence/Detekce
Reputation databases
Prevence/Reakce
Risk management
Prevence
CMDB
Prevence
Asset management
Prevence
Vulnerability management
Prevence/Detekce
SIEM
Detekce/Reakce
EDR
Detekce/Reakce
Log Management
Prevence
Network monitoring
Prevence

MODELY SOC

1. Umístění (určení) služby SOC

- In-house,
- Outsourced,
- Hybrid.

2. Velikost

- Virtuální,
- Malý,
- Velký,
- Stupňovitý.

cesnet

OK...MÁM $...


cesnet
KOUPÍM SI TO!

- **Kam jsem ochoten někoho jiného pustit?**
- **Mohu outsourcovat vše?**
- **Compliance?**
  - SLA, limity a termíny plnění?
- **Jaký reálný přínos pro mě tento přístup bude mít?**
  - Co skutečně dostanu? SOC? SIEM? ….
- **Co to bude stát?**
- **Pokud outsourcujeme…potřebujeme?**
  - vlastní IT, bezpečnost, aj.

cesnet

O ČEM JE BEZPEČNOST?

- **Prostředků**, které je organizace ochotna na danou činnost vynaložit,
- **lidských zdrojů**, které jsou dostupné v organizaci, či které budou dedikovány na zajištění činnosti SOC pro organizaci,
- **velikost a druh činnosti organizace,**
- **definovanou úroveň kompetencí,**
- **počet využívaných prostředků ICT, poskytovaných služeb,** zabezpečovaných uživatelů, přenášených a ukládaných dat aj.,
- **objem a typy bázových dat** proudících z organizace,
- **míru rizika kybernetické bezpečnostní události** či incidentu pro danou organizaci,
- útoky prováděné na segment, ve kterém organizace působí aj.

cesnet

IN-HOUSE SOC CESNET

cesnet

FTAS, netflow, ipfix, sFlow, honeypots, IDS, IPS, Logs aj.

Externí zdroje

bezpečnostní události, NÚKIB, partneři aj.

- **Příjem**
- **Zpracování**
- **Obohacení**
- **Analýza**
- **aj.**

DATA

- **FTAS**
- **exaFS**
- **NERD**
- **Warden**
- **Mentat**
- **Logmgmt**
- **SIEM**
- **VM**
- **aj.**

cesnet certs

(incident handling)

FTAS a síťová analytika

Situational Awareness analytika

Analytik

Analytik

Analytik

Analytik

Zásahy
(filtry, blokace aj.)

konzultace, spolupráce

Incident reports, event reports, vulnerability reports.

konzultace, spolupráce

cesnet flab

Připojená organizace
(univerzita, nemocnice aj.)

Response
Disaster recovery

- Postupy
- Asset management
- DRP
- Analýza rizik
- Dopady aj.

cesnet

HYBRIDNÍ MODEL?

cesnet

cesnet

FTAS, netflow, ipfix, sFlow, honeypots, IDS, IPS, Logs aj.

Externí zdroje

bezpečnostní události, NÚKIB, partneři aj.

Členové

Logy - @, NAT, DHCP, FW, dom. controller, radius, IDM…
Scans, vulnerability mgmt…

- **Příjem**
- **Zpracování**
- **Obohacení**
- **Analýza**
- **aj.**

DATA

- **FTAS**
- **exaFS**
- **NERD**
- **Warden**
- **Mentat**
- **Logmgmt**
- **SIEM**
- **VM**
- **aj.**

cesnet certs

(incident handling)

FTAS a síťová analytika

Situational Awareness analytika

Analytik Analytik Analytik Analytik

Zásahy
(filtry, blokace aj.)

konzultace, spolupráce

Incident reports, event reports, vulnerability reports.

konzultace, spolupráce

cesnet flab

Připojená organizace
(univerzita, nemocnice aj.)

Response
Disaster recovery

- Postupy
- Asset management
- DRP
- Analýza rizik
- Dopady aj.

cesnet

Činnost	Oblast	Procesy	Technologie (možnosti zajištění přístupu)	Lidé (minimální požadavky)	Možnosti spolupráce v rámci hybridního SOC [mezi Poskytovatelem služeb (ISP, SOC aj.) a koncovou organizací]
Prevence	Network Monitoring	NetFlow monitoring	Vhodné, výkonné a správně nastavené síťové prvky a/nebo Specializované síťové sondy	Správce sítě, systémů a služeb Datový analytik Specialista KB Dohledové centrum	**Poskytovatel služeb** • Network Monitoring (sběr, analýza flow dat, reporting událostí) na perimetru organizace • ochrana perimetru organizace (např. vůči DoS a DDoS útokům) • poskytnutí nástrojů pro Network Monitoring uvnitř organizace • poskytnutí služeb svěřené správy/externího Dohledového centra na základě uvnitř organizace instalovaných sond **Organizace** • poskytuje zpětnou vazbu pro nastavení síťového monitoringu a reportingu • zřídí přístup pro sběr dat uvnitř organizace pro poskytovatele služby • zajišťuje monitoring a analýzu stavu služeb • DPI a zajištění dohledu je vhodné i z hlediska ochrany citlivých informací a dat řešit na úrovni organizace
			Síťové kolektory		
		Deep Packet Inspection (DPI)	Repozitář datasetů		
		Zajištění dohledu (SNMP, telemetrie)	Nástroj pro provozní dohled (např. Nagios, Icinga, Zabbix).		
	Log Management	Logy z infrastruktury	Nástroj pro sběr dat (např. Syslog, Rsyslog, Sysmon)	Správce sítě, systémů a služeb Datový analytik Specialista KB	**Poskytovatel služeb** • poskytnutí nástrojů pro Log Management uvnitř organizace • může zajistit analýzu dat **Organizace** • musí umožnit instalaci nástrojů třetí strany nebo • musí zajistit předání logů pro potřeby analýzy dat
		Logy z operačních systémů	Datová platforma (např. ELK stack, OpenSearch).		
		Logy ze služeb			

Vysvětlivka: **Oranžově** označená pole vyznačují oblasti (procesy a technologie), které musí být řešeny interně v rámci dané organizace; **Modře** vyplněná, či ohraničená pole představují oblasti, ve kterých je možná součinnost s poskytovatelem služeb (ISP, SOC aj.). Tabulka rozděluje činnosti do oblastí prevence, detekce a reakce, nicméně některé tyto oblasti se překrývají (viz graf SOC capabilities).

cesnet

Prevence	Vizualizace	Dat ze sítě	Topologie sítě Asset management (např. NetBox).	Správce systémů Specialista KB Manažer KB	Vizualizace slouží k lepšímu pochopení situace a primárně se jedná o podpůrný mechanismus.
			Datová platforma (např. ELK stack, OpenSearch)		
		Dat ze zařízení a služeb	Datová platforma (např. ELK stack, OpenSearch)		
		Dat z forenzní analýzy	Vizualizace vektoru útoku (např. STIX, IDMEF, IODEF, IDEA)		
	Penetration Testing	Identifikace zranitelností	Nástroj pro automatizované testy zranitelností (např. Nessus, Arachni, Nikto)	Správce sítě, systémů a služeb Specialista KB Manažer KB	**Poskytovatel služeb** • poskytne služby penetračního testování • využívá zázemí, zkušeností a znalostí z již provedených testů **Organizace** • umožní testování sítě a služeb a jejich zabezpečení • zajistí potřebnou součinnost (např. prostupy, umístění na Whitelist aj.)
		Penetrační testování • White-box • Black-box	Manuální testy zranitelností (např. Metasploit, Burp Suite, FoxyProxy, FirefoxCookie Manager, FireBug)		
		Red Teaming			
		Zátěžové („stress“) testy	Paketové generátory (Spirent, IXIA aj.)		
	Školení/ Vzdělávání/ Konzultace	Kybernetická a informační bezpečnost pro uživatele	Pravidelné školení a rozvoj kompetencí zaměstnanců. Typy školení: • Fyzická on site • E-learning • Hands-on • Cvičení Konzultace: • Knowledge management • Data governance	Zaměstnanci organizace Správce sítě, systémů a služeb Specialista KB Manažer KB Management organizace Odborný konzultant	**Poskytovatel služeb** • podpora rozvoje kompetencí uvnitř organizace • forenzní tréninky • ad hoc školení, tréningy a cvičení • osvětové aktivity • pracovní skupiny věnující se problematice kybernetické bezpečnosti • konzultace individuálně, nebo v rámci komunity **Organizace** • kontinuální rozvoj kompetencí • zařazení kybernetické bezpečnosti do povinného školení zaměstnanců • zapojení IT pracovníků do bezpečnostních komunit • analýza a aplikace dalších školících materiálů do organizace (např. NÚKIB) • rozvoje kompetencí a vzdělávání IT pracovníků (např. CompTIA Security, MITRE aj.)
		Vzdělávání IT profesionálů			
		Red Teaming			
		Purple Teaming			
	Security Management	Nastavení systému řízení kybernetické a informační bezpečnosti v organizaci	ISMS.online Eremba WebArat Aphinit	Správce sítě, systémů a služeb (garanti aktiv) Architekt KB Manažer KB Management organizace	**Poskytovatel služeb** • poskytuje poradenství a konzultace • organizuje sdílení znalostí a dobrých zkušeností • pomoc s implementací ISMS • poskytnutí bezpečnostních rolí **Organizace** • poskytnutí informací pro tvorbu bezpečnostní dokumentace • zajištění podpory managementu organizace pro zavedení ISMS

cesnet

Detekce	Network Monitoring	Honeypot		Nástroj pro zachycení potencionálního útoku (např. LaBrea, Honeyd, Kippo atd.)	Správce sítě, systémů a služeb Datový analytik Specialista KB	**Poskytovatel služeb** • poskytnutí služeb IDS/IPS • analýza dat, reporting • definice pravidel • proškolení správců systému organizace **Organizace** • provoz IDS/IPS • poskytnutí zpětné vazby k nastaveným pravidlům • předávání dat poskytovateli služby
		IDS/IPS		Nástroj pro detekci anomálií (např. Surricata, Snort) a/nebo Komerční IDS/IPS		
	Vulnerability Monitoring	Detekce a vyhodnocování zranitelností	Interní	Burp Suite (týká se pouze webových aplikací) Nessus OpenVas	Specialista KB Manažer KB	**Poskytovatel služeb** • poskytuje nástroje • provádí analýzu • reportuje zjištěné skutečnosti **Organizace** • musí provádět kontroly dle zjištěných zranitelností • vyhodnocuje zranitelnosti a aplikuje optření • zajistí konfiguraci exportu dat do systémů poskytovatele služeb • umožní testování sítě a služeb a jejich zabezpečení • zajistí potřebné součinnosti (např. prostupy, umístění na Whitelist aj.)
			Externí	Shodan Censys AUDIT SNER Shadowserver		

cesnet

Detekce	Vulnerability Management	Systematický přístup k datům zjištěným z vulnerability monitoringu	Asset management (např. NetBox) CMDB (např. Insight, CMDBuild)	Specialista KB Architekt KB Manažer KB	**Organizace** • aplikuje doporučení a opatření vůči zranitelnostem zjištěným z Vulnerability Monitoringu
	Reputation Databeses	Znalostní báze zaměřená na reputaci daného zdroje v čase	NERD Cisco Talos VirusTotal	Specialista KB Datový analytik	**Poskytovatel služeb** • provozuje a poskytuje technologii • vytváří reputační databázi **Organizace** • musí provádět kontroly dle zjištěných zranitelností • vyhodnocuje zranitelnosti
	Threat Management	Threat Monitoring Threat Intelligence	OSINT Mentat AlienVault – Open Threat Exchange Intel Owl IntelMQ	Specialista KB Architekt KB Manažer KB	**Poskytovatel služeb** • poskytuje nástroje • provádí analýzu • reportuje zjištěné skutečnosti • může definovat hrozby pro daný sektor **Organizace** • zasílání informace o útocích • vyhodnocuje zranitelnosti • zajistí konfiguraci exportu dat do systémů poskytovatele služeb
	Endpoint Detection and Response (EDR)	Antivir EDR	Avast, ESET, Symantec, Microsoft Defender McAfee, Bitdefender, F-Secure, Sophos, Norton aj.	Správce systémů Specialista KB Datový analytik	**Organizace** • musí analyzovat a vyhodnocovat informace z EDR/antivirového řešení • může napojit EDR systémy na systémy SIEM
	Security Information and Event Management (SIEM)	Zpracování provozních a bezpečnostních dat a detekce událostní na základě nastavených pravidel	Splunk IBM QRadar Microsoft Sentinel ArcSight ESM ELK stack AlienVault OSSIM Mentat	Správce systémů Specialista KB Datový analytik Manažer KB Architekt KB	**Poskytovatel služeb** • poskytuje nástroje • provádí analýzu • reportuje zjištěné skutečnosti • definuje pravidla • poskytuje zpětnou vazbu na aplikovaná pravidla **Organizace** • poskytuje zpětnou vazbu na aplikovaná pravidla • umožní sběr dat uvnitř organizace pro poskytovatele služby nebo • zasílá data poskytovateli služby

Reakce	Reporting	Periodické	Nejčastější způsob představuje předání dat v plain textu (např. .csv, .pdf, .xml, .json)	Správce sítě, systémů a služeb Specialista KB Manažer KB Management organizace	**Poskytovatel** • poskytnutí nástrojů, jejich konfigurace a vyhodnocování, případně napojení na Dohledové centrum **Organizace** • nastavení systému reportingu v rámci organizace a mezi organizací a poskytovatelem služby • možnost napojení na externí systémy
		Na vyžádání On-line	On-line Dashboard (např. Kibana, Grafana).		
	Mitigace	Centralizovaný přístup	Stavový firewall Access Control List (ACL) DNS-RPZ AAI Scrubbing centrum	Specialista KB Manažer KB	**Poskytovatel služeb** • poskytuje nástroje • definice pravidel • může blokovat definovaný provoz na perimetru organizace na základě definovaných pravidel **Organizace** • spolupracuje na definici pravidel • poskytuje zpětnou vazbu • zasílá data poskytovateli služby
		Decentralizovaný přístup	RTBH BGP FlowSpec		

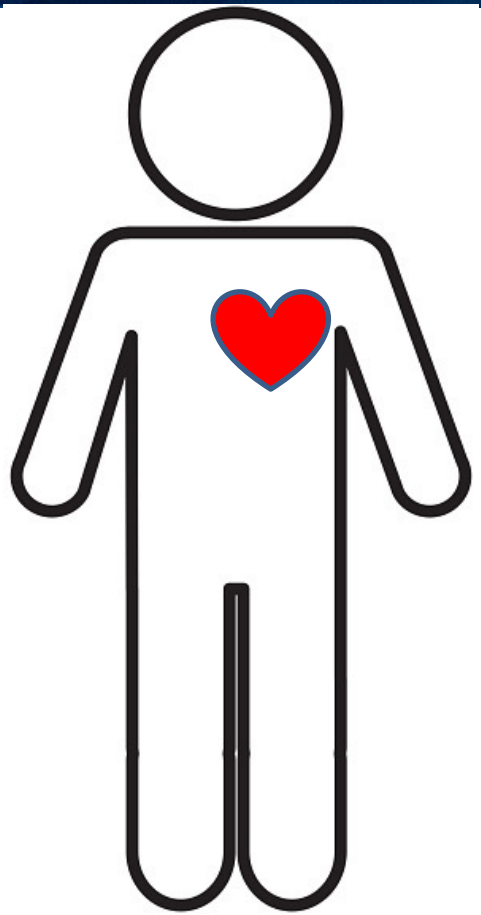
Reakce	CERT/CSIRT	Incident handling	Triage Ticket/Case Management Forenzní analýza Log Management Network monitoring Threat Management Vulnerability Management Reputation Databeses Security Information and Event Management (SIEM)	Správce sítě, systémů a služeb Specialista KB Manažer KB Člen CERT/CSIRT týmu Management organizace	**Poskytovatel konektivity, resp. poskytovatel služeb (pokud je zároveň ISP)** • poskytuje platformu pro sdílení informací v rámci Incident Sharingu • provádí filtraci nahlášených incidentů • provádí pokročilou analytickou činnost nad incidenty a definuje hrozby **Organizace** • předává informace o bezpečnostních incidentech • poskytování informací o úrovni kvality jednotlivých sdílejících stran • mohou pomoci s odhalováním „false positive“
		Incident Response	Incident Response Playbooks EDR Mitigace Vydání varování Hlášení CSIRT.CZ, NÚKIB, komunitě		
		Incident Sharing	e-mail Warden MISP STIX/TAXII Předání informací o incidentu (CSIRT.CZ, NÚKIB, komunitě, veřejnosti)		
	Case management	Sledování a řízení procesu řešení konkrétní kybernetické bezpečnostní události, hrozby, incidentu	RTIR The Hive ServiceNow – Serurity Incident Response Jira Atlassian	Dohledové centrum Správce sítě, systémů a služeb Specialista KB Člen CERT/CSIRT týmu	**Poskytovatel služeb** • realizuje koordinaci, konzultaci a podporu při řešení bezpečnostních událostí • poskytnutí forenzní analýzy • propojení s dalšími bezpečnostními týmy **Organizace** • poskytuje informace o bezpečnostních incidentech • průběžně dodává informace vztahující se k řešenému incidentu
	Forenzní analýza	Interní / Externí	Sandbox	Specialista KB Odborný konzultant Člen CERT/CSIRT týmu	**Poskytovatel služeb** • poskytuje služby Forenzní laboratoře • zajištění a analýza artefaktů pro forenzní analýzu • definice IoC **Organizace** • poskytuje informace o bezpečnostním incidentu • zajištění artefaktů bezpečnostního incidentu • odhalování „false positive“ • ověřování zjištěných IoC
		Statická / Dynamická	Cuckoo Sandbox Autopsy/The Sleuth Kit SANS SIFT VirusTotal Whireshark		

cesnet

SPRÁVNÉ ŘEŠENÍ?

cesnet

CO CHYBÍ?



cesnet

SYSTEMATIČNOST...
PROCES...

http://zpravy.ckait.cz/vydani/2020-01/lze-stavet-zaroven-rychle-levne-a-kvalitne/

cesnet

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it".

Stephane Nappo

cesnet

DĚKUJEME ZA POZORNOST

doc. JUDr. Jan Kolouch, Ph.D.
jan.kolouch@cesnet.cz
Andrea Kropáčová
andrea.kropacova@cesnet.cz