



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Prednáška 1

Koncept operačného centra pre kybernetickú bezpečnosť



Riešenie bezpečnostných incidentov
(CyberOps Associate v1.02)

Mgr. Jana Uramová, PhD.
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU



Výsledky vzdelávania

Študent po absolvovaní predmetu získa vedomosti a zručnosti potrebné na úspešné zvládnutie úloh, povinností a zodpovedností bezpečnostného analytika v operačnom centre bezpečnosti.

Študent po absolvovaní predmetu bude vedieť:

- Vysvetliť rolu **analytika** v rámci kybernetickej bezpečnosti
 - Vysvetliť prostriedky **operačného systému** Windows a Linux a charakteristiky pre podporu analýzy v rámci kybernetickej bezpečnosti
 - Analyzovať operácie v rámci **sieťových protokolov a služieb**
 - Vysvetliť operácie **sieťovej infraštruktúry**
 - Klasifikovať rôzne typy sieťových **útokov**
 - Použiť sieťové **monitorovacie** nástroje na identifikáciu útokov proti sieťovým protokolom a službám
 - Použiť rôzne metódy na **prevenciu** škodlivého prístupu do počítačových sietí, k používateľom a k dátam
 - Vysvetliť **vplyvy kryptografie** v rámci monitorovania bezpečnostných sietí
 - Vysvetliť, ako skúmať **zraniteľnosti** a útoky koncových zariadení
 - Identifikovať **hlásenia** v rámci sieťovej bezpečnosti
 - Analyzovať sieťovú prevádzku na overenie **potencionálneho zneužitia** siete
 - Aplikovať **reakčné modely** na incident, a získať prostriedky na manažovanie sieťových bezpečnostných incidentov
- Prerekvizity:
- Princípy IKS, Počítačové siete 1, Úvod do OS

Preliminary version of topics for lectures

Planning

Week	CyberOps Modules in lectures	Exam from:
1	Chapter 1 The Danger Chapter 2 Fighters in the War Against Cybercrime Chapter 3: The Windows Operating System	none
2	Chapter 4: Linux Overview Chapter 5 Network Protocols Chapter 6 Ethernet and Internet Protocol (IP) Chapter 7 Connectivity Verification Chapter 8 Address Resolution Protocol Chapter 10 Network Services Chapter 11 Network Communication Devices	1-2
3	Chapter 9 The Transport Layer (+nmap) Chapter 12 Network Security Infrastructure	3-4
4	Chapter 13 Attackers and Their Tools Chapter 14 Common Threats and Attacks	5-10

Week	CyberOps Modules in Lectures	Exam from:
5	Chapter 15 Network Monitoring and Tools (<i>SIEM, SOAR</i>) Chapter 16 Attacking the Foundation (<i>L2, L3 protocols vulnerabilities and attacks</i>) Chapter 17 Attacking What We Do (<i>L7 vulnerabilities and attacks</i>)	11-12
6	Chapter 18 Understanding Defense (<i>security management</i>) Chapter 19 Access Control (<i>AAA</i>) Chapter 20 Threat Intelligence (<i>commercials, CVE database</i>)	13-17
7	Chapter 21 Cryptography Chapter 22 Endpoint Protection	18-20
8	Chapter 23 Endpoint Vulnerability Assessment Chapter 24 Technologies and Protocols	none
9	Chapter 25 Network Security Data Chapter 26 Evaluating Alerts (in Security Onion)	21-23
10	Chapter 27 Working with Network Security Data (Security Onion and ELK) Chapter 28 Digital Forensics and Incident Analysis and Response	24-25
11	Expert talk (invited lecture)	26-28

Odporúčaná literatúra

1. Materiály Cisco Networking Academy: Cisco Certified CyberOps Associate, v angličtine
2. CCNA Cybersecurity Operations Companion Guide, Jun 17, 2018, Cisco Press, ISBN-10: 0-13-516624-1, ISBN-13: 978-0-13-516624-6 (**obsolete**)
3. Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, November 26, 2020, ISBN: 0136807836, Cisco Press.

☰ CISCO CyberOps Associate v1.0

1 The Danger ^

1.0 Introduction ^

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Why Should I Take this Module?

1.0.5 What Will I Learn in this Module?

1.0.6 Class Activity - Top Hacker Shows Us How It's Done

1.1 War Stories v

1.2 Threat Actors v

1.3 Threat Impact v

1.4 The Danger Summary v

2 Fighters in the War Against Cybercrime v

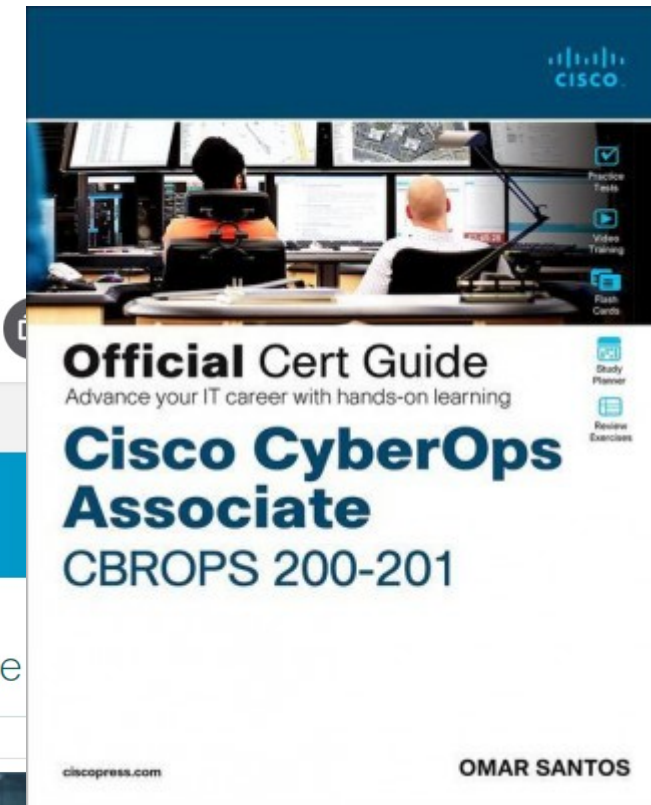
Introduction

1.0.1

First Time in This Course

ciscopress.com

OMAR SANTOS



Certifikácia – Cisco Certified CyberOps Associate

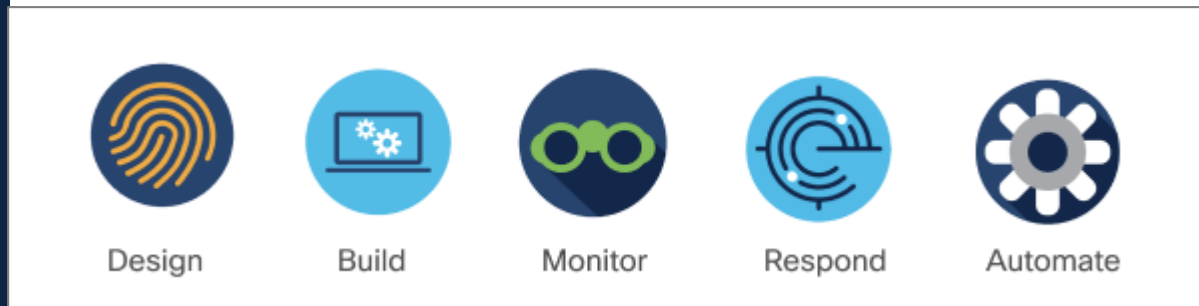
- 200-201 CBROPS exam
 - <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/cyberops-associate.html>
 - Platnosť: 3 roky
 - Recertifikácia: exam alebo získať 30 kreditov (tzv. continuing education credits)

Each associate-level certification requires

One Exam:

1 = 

Core Exam = CyberOps Associate



CyberOps Certifications Community
<https://learningnetwork.cisco.com/s/topic/0TO3i0000008jY7GAI/cyberops-certifications-community>

Reasons for successful graduates of the certification exam

Why get certified

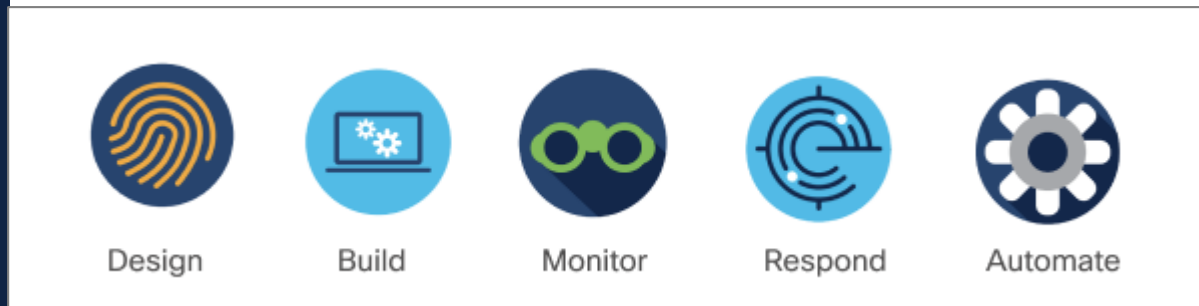
- Stronger knowledge in key cybersecurity areas (38%)
- Increased confidence in the team's handling of security challenges (30%)
- Higher-level personnel in-house with security expertise (27%)
- Staying up to date on the latest security and privacy trends (27%)

Each associate-level certification requires

One Exam:

1 = 

Core Exam CyberOps Associate



CyberOps Associate → CyberOps Professional

Subsequent certification... professional level

- Cisco Certified CyberOps **Professional** Certification and Training
 - <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/cyberops-professional.html>

Required exam

Recommended training

Core exam:

[350-201
CBRCOR](#)

[Performing CyberOps Using Cisco Security Technologies \(CBRCOR\)](#)

Concentration exam:

[300-215 CBRFIR](#)

[Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps \(CBRFIR\)](#)



Job Opportunities?

- Connect to opportunities based on your experiences, education, and certifications
- <https://www.netacad.com/portal//careers/talent-bridge-program>

The screenshot shows the 'Skills' section of the NetAcad portal. It features a navigation bar with 'Net Acad', 'Skills', 'Profile', 'Education', 'Certifications', 'Opportunity', 'Documents', and 'Finish'. Below the navigation bar, there are two main sections: 'Technical Skills' and 'Business Skills'. Each section includes a 'Learn More' link and a table for selecting years of experience for various skills.

Technical Skills

Learn More about how you can translate your Cisco Networking Academy courses to career skills to match with industry jobs in the Matching Engine.

Skills	Years Of Experience
Technical Skills	
Cloud (migration and deployment, serverless architecture)	
Design (discover, plan, analyze, scope)	<input type="radio"/> N/A <input type="radio"/> <1 year and/or trained <input type="radio"/> 1-2 Years <input type="radio"/> 3-4 Years <input type="radio"/> 5+ Years
Deploy (develop, implement, install, configure, customize)	<input type="radio"/> N/A <input type="radio"/> <1 year and/or trained <input type="radio"/> 1-2 Years <input type="radio"/> 3-4 Years <input type="radio"/> 5+ Years
Manage (support, maintain, helpdesk, troubleshoot)	<input type="radio"/> N/A <input type="radio"/> <1 year and/or trained <input type="radio"/> 1-2 Years <input type="radio"/> 3-4 Years <input type="radio"/> 5+ Years
Collaboration (VoIP, voice, video, unified communications)	
Design (discover, plan, analyze, scope)	<input type="radio"/> N/A <input type="radio"/> <1 year and/or trained <input type="radio"/> 1-2 Years <input type="radio"/> 3-4 Years <input type="radio"/> 5+ Years
Deploy (develop, implement, install, configure, customize)	<input type="radio"/> N/A <input type="radio"/> <1 year and/or trained <input type="radio"/> 1-2 Years <input type="radio"/> 3-4 Years <input type="radio"/> 5+ Years

Business Skills

Learn More about how you can translate your Cisco Networking Academy courses to career skills to match with industry jobs in the Matching Engine.

Skills	Years Of Experience
Business Skills	
General Office/Professional Skills	
Administrative Support (operations, backoffice, office mgmt/admin, business mgmt)	<input type="radio"/> N/A <input type="radio"/> <1 year and/or trained <input type="radio"/> 1-2 Years <input type="radio"/> 3-4 Years <input type="radio"/> 5+ Years
Facilities (building/mechanical oversight, maintain safety, equipment mgmt)	<input type="radio"/> N/A <input type="radio"/> <1 year and/or trained <input type="radio"/> 1-2 Years <input type="radio"/> 3-4 Years <input type="radio"/> 5+ Years
Finance (account receivable, accounts payable, payroll, budget, finance reports)	<input type="radio"/> N/A <input type="radio"/> <1 year and/or trained <input type="radio"/> 1-2 Years <input type="radio"/> 3-4 Years <input type="radio"/> 5+ Years
Human Resources (recruit, hire, onboard, train, benefits, cooperation)	<input type="radio"/> N/A <input type="radio"/> <1 year and/or trained <input type="radio"/> 1-2 Years <input type="radio"/> 3-4 Years <input type="radio"/> 5+ Years

Hodnotenie

V dlhšom horizonte

- Uplatním sa v praxi
- Dáva mi zmysel to čo robím
- Viem to robiť
- Uživím rodinu 😊
- ...

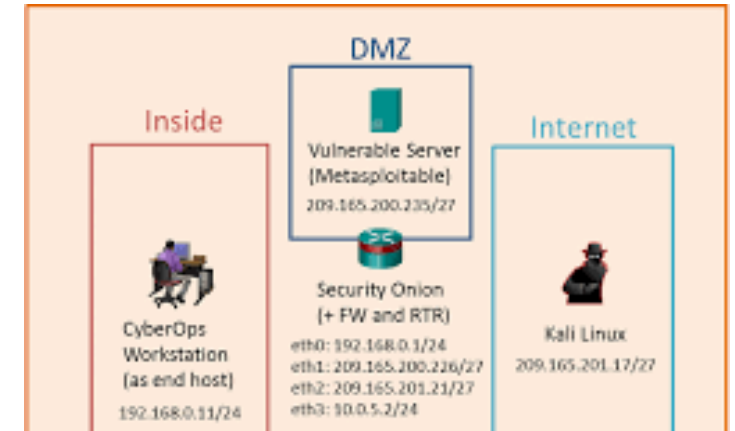
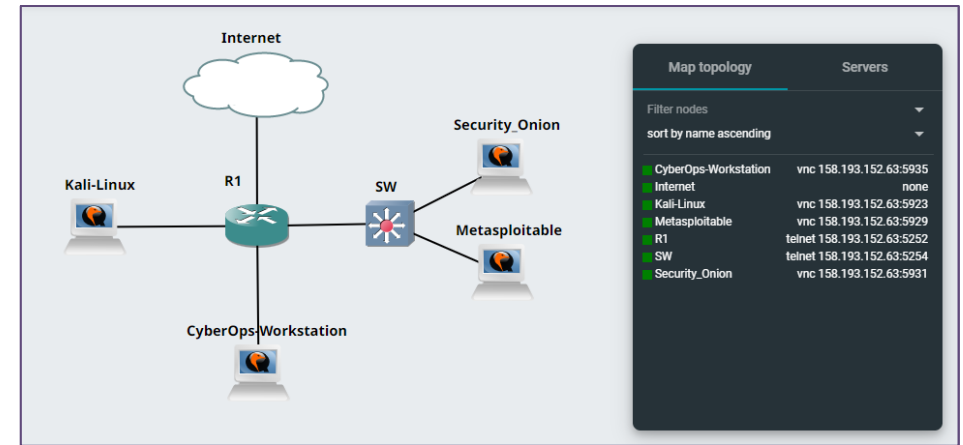
V tomto predmete



Formy a metódy hodnotenia	Váha %
Priebežné písomné testy	30%
Vyriešenie zadaných problémov v rámci praktických zadaní	40%
Záverečný písomný test	10%
Vyriešenie komplexného problému v rámci praktického zadania alebo projektu	20%

Lab environment

Course-specific VMs for labs

- Three options where and how to work in the topology with the given VMs:
 - GNS3 server (only for slovak students)
 - Oracle VM VirtualBox Manager**
 - NDG Online lab



VMs description	File Name	Ova file size	Minimum RAM requirements
 CyberOps Workstation VM	cyberops_workstation.ova	3,51 GB	1 GB
 Security Onion VM	security_onion.ova	2,86 GB	4 GB

Výber prostredia - labs

Pracovať možno s danými VMs v týchto prostrediach:

A: remote (práca na remote GNS3 server)

- **A1. remote KIS GNS3 server:**

- GNS3 server dostupný cez web/GNS3 klienta v prostredí siete UNIZA (alt. VPN)
- Výhody: menšia záťaž na úvodný rozbeh, nezaťažujete zdroje svojho PC
- Nevýhody: pri väčšom vytážení servera, na ktorom pracujú aj iní študenti, môže byť server pomalšie responzívnejší (limitovaný výkon)
- Pozn.: práca na našom KIS servery - IP adresu servera oznámi vyučujúci na cvičení

Výber prostredia - labs

B. local (práca s lokálnou virtualizáciou na vlastnom alebo školskom PC)

Pozn.: podmienkou je CPU aspoň 4 jadrá/8 vlákien (4C/8T) s podporou virtualizácie a RAM aspoň 12GB

- **B1. Virtualbox + GNS3**

- Riešenie postavené na lokálnej stanici s virtualizáciou pomocou VirtualBoxu (alt. VMware s licenciou) a networking pomocou GNS3 VM (GNS3 server).
- Výhody: študent má správu nad svojím projektom v GNS3, nikto mu ho nezmaže, s nikým sa nedelí o zdroje svojho PC, na ktorom pracuje
- Nevýhody: potrebné mať PC s dostatočným výkonom, a venovať čas rozbehnutiu projektu s VMs v GNS3
- Pozn.: Podmienkou je aby študent pracoval na zariadení s podporou vnorenej virtualizácie

- **B2. Virtualbox only**

Výber prostredia - labs

- **B2. Virtualbox only**

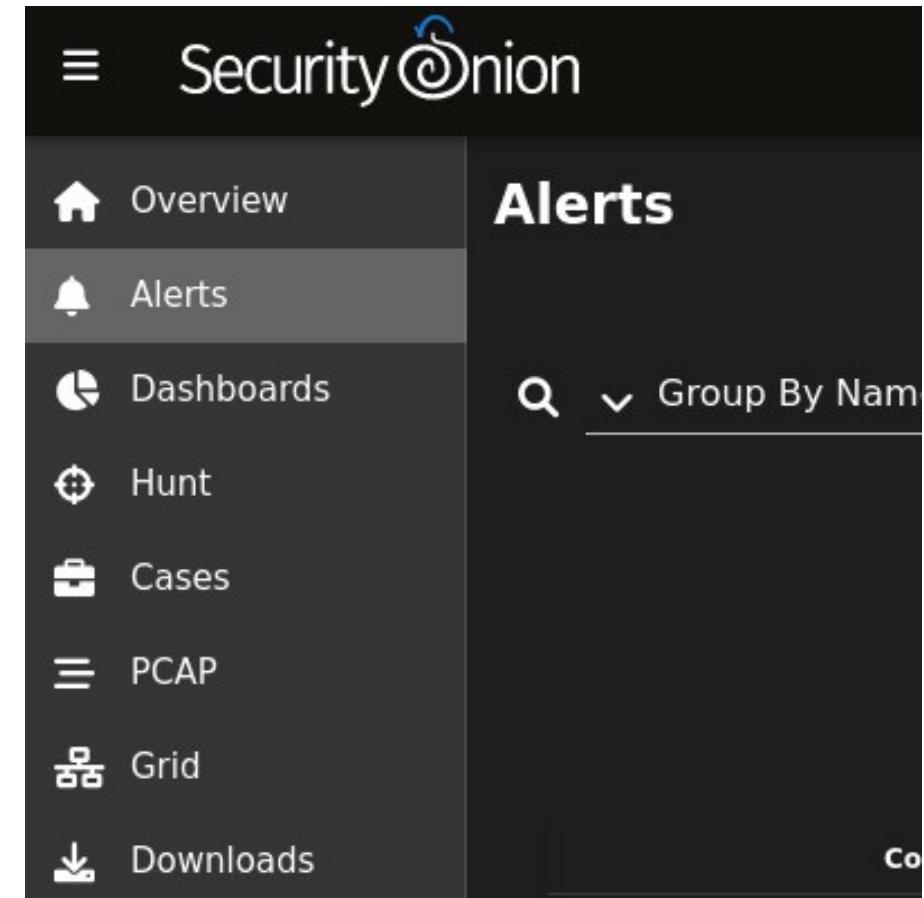
- Riešenie postavené na virtualizácii zariadení pomocou Virtualbox (alt. iný hypervízor)
- Výhody: máte správu nad svojím projektom, nikto vám ho nezmaže, s nikým sa nedelíte o zdroje svojho PC, na ktorom pracujete
- Nevýhody: potrebné mať PC s dostatočným výkonom, a venovať čas rozbehnutiu projektu a VMs, neobsahuje funkcie GNS3 (onitoring linky s WireShark, etc), linky medzi zariadeniami riešené pomocou virtualbox sieťového rozhrania zdieľaného medzi zariadeniami
- Pozn.: Táto varianta je až posledné riešenie pre prípad, že študent nedokáže využiť GNS3 spolu s VirtualBox-om

Course-specific VMs for labs

Security Onion



- Security Onion Solutions (* 2008)
 - a free and open platform (Linux distribution) for
 - threat hunting
 - network security monitoring
 - log management
 - SIEM
 - incident response
 - compliance
 - includes best-of-breed free and open third-party tools:
 - Suricata (NIDS, HIDS)
 - Zeek (formerly known as Bro) (NIDS)
 - Snort (NIDS, also HIDS)
 - OSSEC (HIDS)
 - Wazuh (all features)
 - Stenographer (full packet capture), Wireshark, ...
 - CyberChef (encrypt, encode, compress, data analysis)
 - NetworkMiner (NFAT for Windows+, packet analyzer)
 - Elastic Stack (Elasticsearch, Logstash, Kibana)
 - Squil (main NSM dashboard and event driven analysis)
 - ... and many others



Main web: <https://securityonionsolutions.com/>

Youtube: securityonion.net/youtube

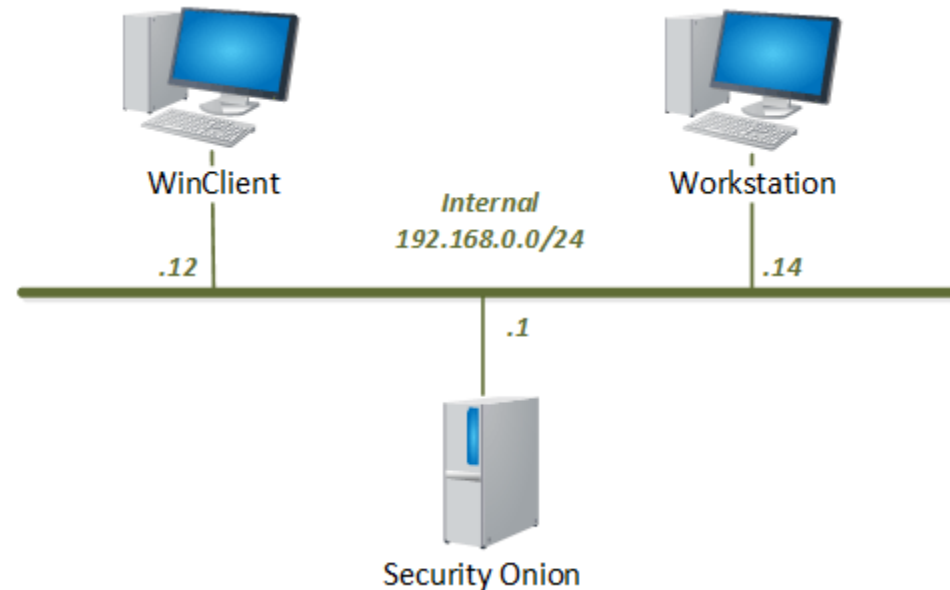
Docu: <https://docs.securityonion.net/en/2.3/>

- Latest version: 2.3.140 (up to date 11.8.2022)

A third option for securing access to the practice topology

Online LAB for 20 - 40 dollars from NDG

- All NETLAB+ supported CyberOps Associate labs are supported by the [CyberOps Associate Pod](#)
- https://www.netdevgroup.com/content/cnap/labs/cyberops_associate.html
- The NDG Cisco CyberOps Associate labs are available at **\$39.95** for 6 months of unlimited access
 - \$20 for 3 months...



Virtual Machine	OVF/OVA	Initial Master Pod (thin provisioning)
Security Onion	3.2 GB	8.1 GB
WinClient	12 GB	26.7 GB
Workstation	3.7 GB	7.8 GB
Total	18.9	42.6

How to get to NDG online labs (1)


- After logging in to netacad.com
- In the class **202X_CyberOps** (202X – current year)

Home / I'm Teaching / 2022_CyberOps


2022_CyberOps

Welcome to CyberOps Associate 1.0 (CA)

Introduction to NDG Online Lab Service

 Introduction to NDG Online Lab Service
Restricted Available until end of 9 August 2023

Modules 1 - 2

 Modules 1 - 2 Content
Restricted Available until end of 9 August 2023

How to get to NDG online labs (2)

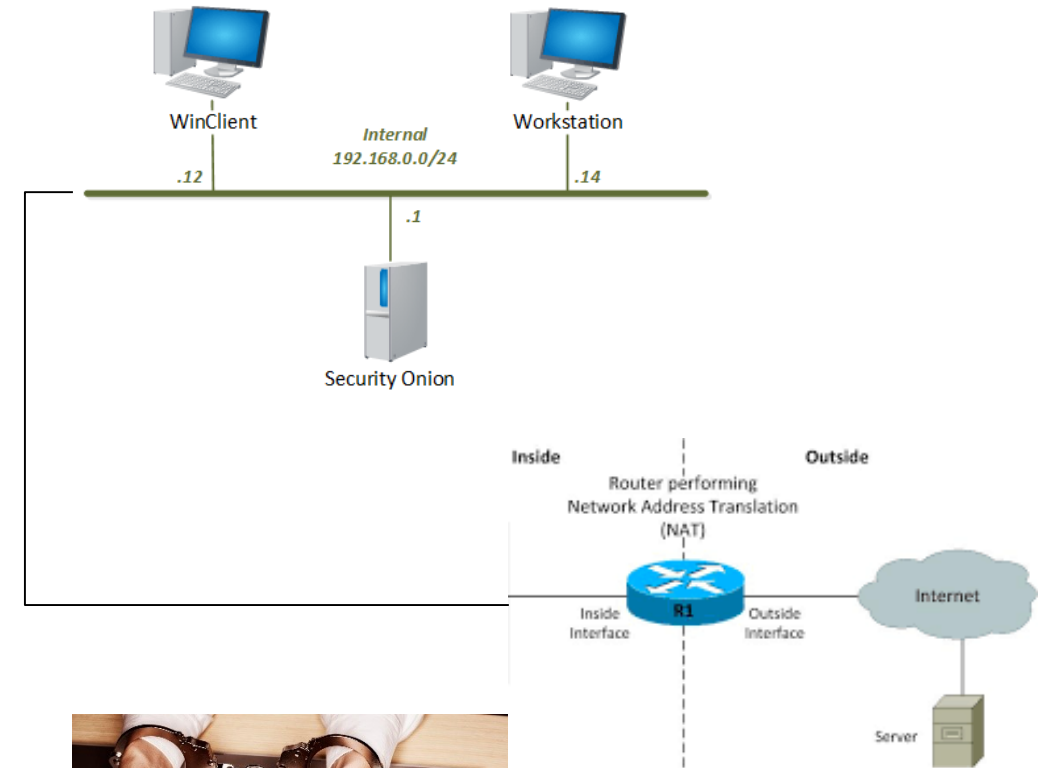
The screenshot shows a web browser window with two tabs. The active tab is titled 'Course Access Required | NDG'. The address bar shows the URL: `portal.netdevgroup.com/learn/573dd43b-1418088/payment`. The page header includes the user ID `408653_1660036379_2292091` and the course name `2022_CyberOps`. A dark blue sidebar on the left contains navigation icons for 'Learn', 'Account', and 'Help'. The main content area features a prominent yellow box with the heading 'Course Access Required' and the text: 'This course may require payment before you can access the labs. Please choose a payment option below to start your lab access.' Below this is a section titled 'Purchase Course Access' with a blue box stating: 'Course access is sold and fulfilled by FastSpring — an authorized reseller. Charges will appear on your bill as FS* NetDevGroup.' The text explains that the CyberOps Associate labs help learners earn the Cisco Certified Cyberops Associate Certification and lists topics like security concepts, monitoring, and analysis. It also notes that there are multiple purchase options based on the time needed to complete the labs. At the bottom, three purchase options are listed in a table:

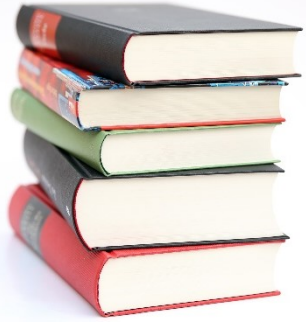
\$11.95	One Month Access
\$29.95	Three Month Access
\$39.95	Six Month Access

A 'Purchase Access' button is located at the bottom of the purchase options section. The Cisco Networking Academy logo is visible in the top right corner of the page.

Ethical Hacking Statement

- Security holes and vulnerabilities that are created in this course **should only be used in an ethical manner and only in this “sandboxed”** virtual environment.
- Experimentation with these tools, techniques, and resources **outside** of the provided sandboxed virtual environment is at the **discretion of the instructor** and local institution.
- **Unauthorized access** to data, computer, and network systems is a **crime** in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator’s motivations.
- It is the learner’s **responsibility**, as the user of this material, to be **cognizant of and compliant** with computer use laws.





Obsah dnešnej prednášky

- **Module 1 The Danger**
- **Module 2 Fighters in the War Against Cybercrime**
- **Module 3: The Windows Operating System (prečítať samostatne z Netacadu, nie je súčasťou tejto prednášky, na 2. cvičení bude k tomu lab)**



Modul 1

The Danger

Module Objective: Explain why networks and data are attacked.

Topic Title	Topic Objective
War Stories	Explain why networks and data are attacked.
Threat Actors	Explain the motivations of the threat actors behind specific security incidents.
Threat Impact	Explain the potential impact of network security attacks.


1.1 War Stories

Nebezpečné zážitky

Hijacked people, hacked devices

- Každý môže byť cieľ....

Ransomware



daredevil@cock.li



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail daredevil@cock.li
Write this ID in the title of your message: D03761CB
In case of no answer in 24 hours write us to these e-mails: hells_kitchen@zoho.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

daredevil@cock.li

Free decryption as guarantee
Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
<http://www.coindesk.com/information/how-can-i-buy-bitcoins/>

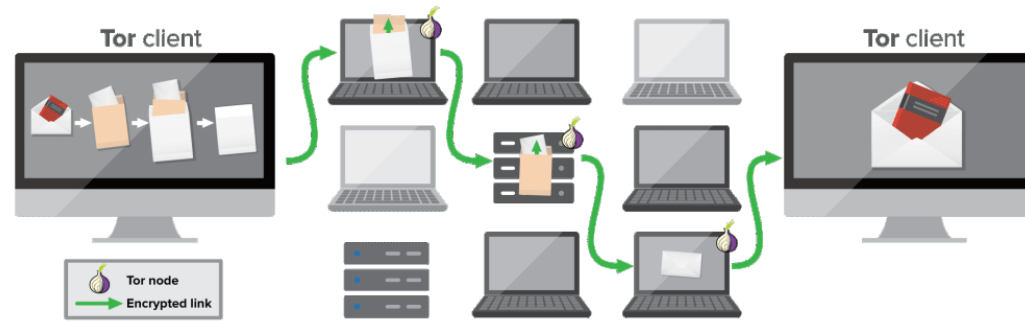
Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

12:42
17.10.2017

ToR node a pretakajúci nedovolený obsah

This Is How Information Travels Between You And Your Peer Through The Tor Network



<https://www.expressvpn.com/blog/tor/>



<https://www.acunetix.com/blog/web-security-zone/data-breaches-exposed-databases/>

Brute force na VoIP telefón



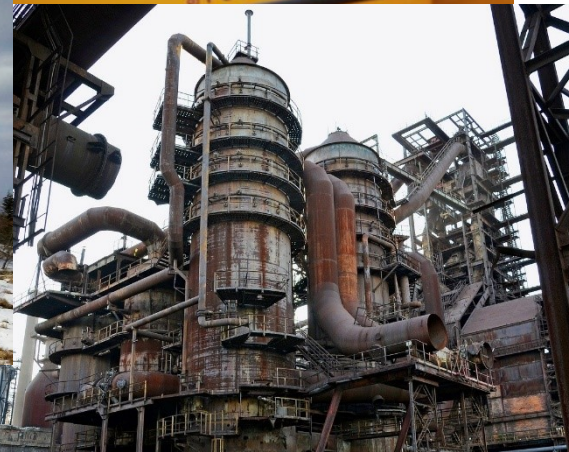
Malware and other types of attacks

- **Virus** – type of malware which has the primary objective of spreading across the network. A virus is a type of malicious software that needs a user to spread.
- **Trojan horse** – is not self-replicating and disguises itself as a legitimate application when it is not.
- **Worm** - the main purpose of a worm is to self-replicate and propagate across the network
- **Rogue hot spot** – that appears to be from a legitimate business but was actually set up by someone without the permission from the business. Many free and open wireless hotspots operate with no authentication or weak authentication mechanisms. Attackers could easily capture the network traffic in and out of such a hotspot and steal user information. In addition, attackers might set up a "rogue" wireless hotspot to attract unsuspecting users to it and then collect information from those users.
- **Botnet** – network of infected computers that are controlled as a group. A botnet is a series of zombie computers working together to wage a network attack.
- **DoS** – One method of executing a DDoS attack involves using a botnet. The zombies continue to create more zombies which carry out the DDoS attack.
- **Ransomware** – involves the hackers preventing user access to the infected and controlled system until the user pays a specified amount.
- **Spyware** – software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Pohľad z „vtácej“ / štátnej perspektívy

Kritická infraštruktúra

1. Doprava
2. Elektronické komunikácie
3. Energetika
4. Informačné a komunikačné technológie
5. Pošta
6. Priemysel
7. Voda a atmosféra
8. Zdravotníctvo



Únik databázy pacientov testovaných na covid-19

Moje eZdravie (17.9.2020)

- triviálna zraniteľnosť
 - Únik viac ako **390 000** osobných údajov pacientov (testovaných v SR na COVID-19)

Aká zraniteľnosť?

- Únik formátu API volaní verejným vyhľadávačom
- Umožnenie neautorizovaného prístupu k samotným volaniam API
- Možnosť získať informácie o všetkých pacientoch
- Absencia mechanizmov, ktoré by znemožňovali masívne sťahovanie uvedených údajov
- Všetky dáta boli v nešifrovanej (v “plaintext”) forme

Ako sa získali dáta?

```
#!/bin/bash
for (( i=8966; i < 391000; i++ )); do
wget https://mojeezdravie.nczisk.sk/api/cntnt.dnld.php/$i
done
```

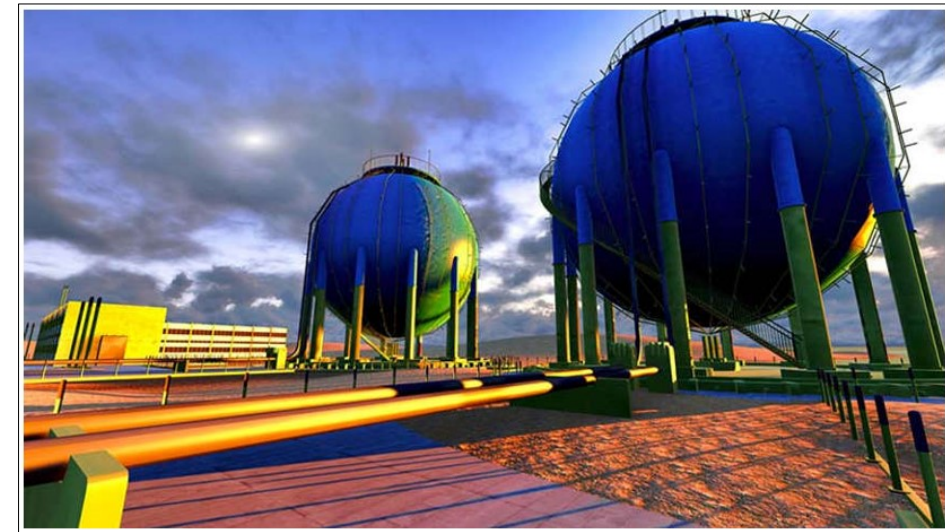


<https://zive.aktuality.sk/clanok/148928/detaily-o-nedavnom-megauniku-dat-pacientov-kde-vsade-zlyhal-stat-ake-chyby-opravit-a-preco-s-tym-meskal/>

<https://nethemba.com/sk/kriticka-zranitelnost-v-aplikacii-moje-ezdravie-unik-databazy-pacientov-testovanych-na-covid-19/>

Bonusový bod (časť A)

- Nájdí na internete informáciu/video o internetovom prieniku (hack) na Slovensku alebo v svete
 - Rovnomerne budeme hľadať v každom z 8 sektorov **(vid' slajd - Kritická infraštruktúra)**
- Spracuj odpovede na otázky:
 - a. What was the target? What is the vulnerability being exploited?
 - b. What information, data, or control can be gained by a hacker exploiting this vulnerability? What was the motive of the hacker? What was the impact of the attack?
 - c. How was the hack performed? What method of attack was used?
 - d. Who was the attacker? What organization or group is the attacker associated with, if any? What about this particular hack interested you specifically?
 - e. How could this attack be prevented or mitigated?
 - f. URL na najlepší zdroj o danom útoku
- Najlepšie zverejníme na KIS webe (podstránka pre predmet RBI)



The Danger

Ransomed Companies

- Employees of an organization are often lured into opening attachments that install ransomware on the employees' computers.
- This ransomware, when installed, begins the process of gathering and encrypting corporate data.
- The goal of the attackers is financial gain, because they hold the company's data for ransom until they are paid.



The Danger

Targeted Nations

- Some of today's **malware** is so **sophisticated** and **expensive** to create that security experts believe only a nation state or group of nations could possibly have the influence and funding to create it.
- Such malware can be targeted to attack a **nation's vulnerable infrastructure**, such as the water system or power grid.
- One such malware was the **Stuxnet** worm that infected USB drives and infiltrated Windows operating systems. It then targeted Step 7 software that was developed by Siemens for their Programmable Logic Controllers (PLCs).



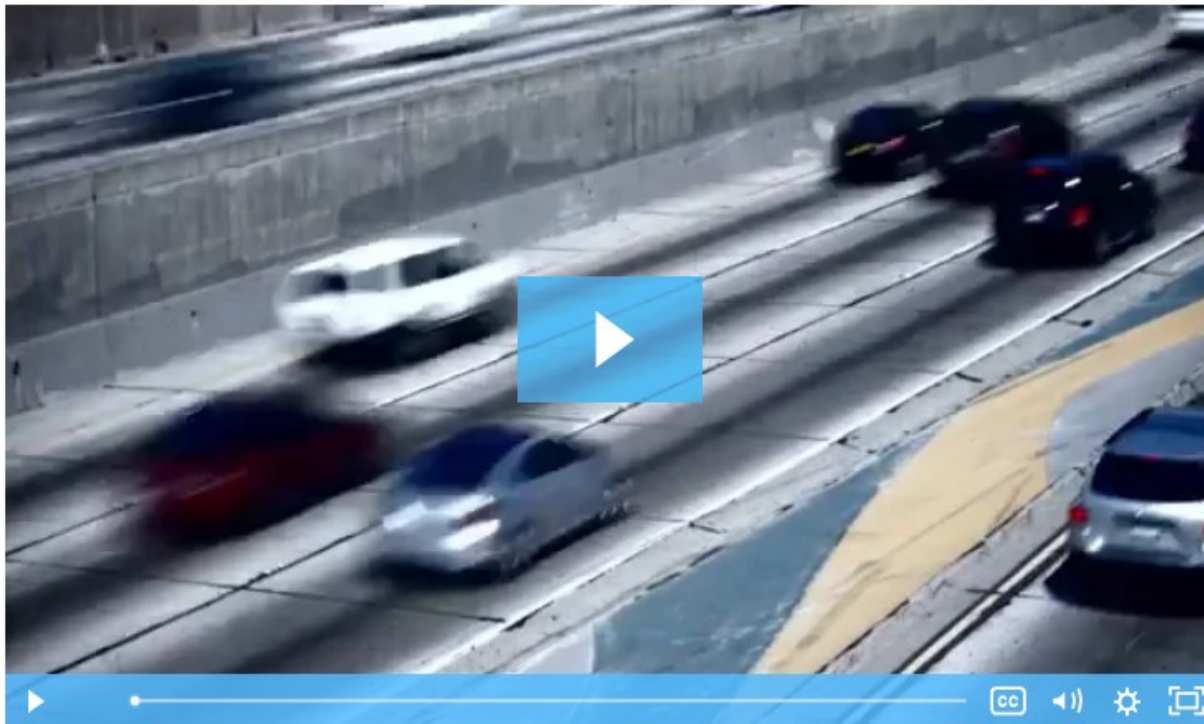
The Danger

Video - Anatomy of an Attack

- Watch this video to view details of a complex attack.

https://www.youtube.com/watch?v=hqKafI7Amd8&ab_channel=TEDxTalks

Pablos Holman, 2012



- TED is a nonprofit devoted to spreading ideas, usually in the form of short, powerful talks (18 minutes or less)
- TED began in 1984 as a conference where Technology, Entertainment and Design converged, and today covers almost all topics
 - from science to business to global issues
 - in more than 100 languages
 - Meanwhile, independently run TEDx events help share ideas in communities around the world.

1.2 Threat Actors

Threat Actors

Hacker – ten čo rieši vs. vyrába problémy



Hacker..

“kvalifikovaný počítačový expert, ktorý využíva svoje technické znalosti na prekonanie problému”

Za rôznym účelom...



- dobrý, zlý a škaredý
- biely, čierny a šedý klobúk



Threat Actors / Aktéry hrozieb

- Threat actors are individuals or groups of individuals who perform cyberattacks. They include, but are not limited to:
 - Amateurs
 - Hacktivists
 - Organized crime groups
 - State-sponsored groups
 - Terrorist groups
- Cyberattacks are intentional malicious acts meant to negatively impact another individual or organization.



Threat Actors (Contd.)



Amateurs

- They are also known as script kiddies and have little or no skill.
- They often use existing tools or instructions found on the internet to launch attacks.
- Even though they use basic tools, the results can still be devastating.



Hacktivists

- These are hackers who publicly protest against a variety of political and social ideas.
- They post articles and videos, leaking sensitive information, and disrupting web services with illegitimate traffic in Distributed Denial of Service (DDoS) attacks.



Financial Gain

- Much of the hacking activity that consistently threatens our security is motivated by financial gain.
- Cybercriminals want to gain access to bank accounts, personal data, and anything else they can leverage to generate cash flow.

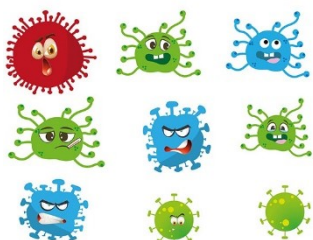
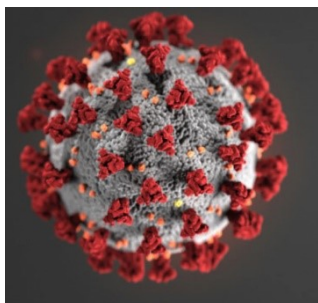


Trade Secrets and Global Politics

- At times, nation states hack other countries, or interfere with their internal politics.
- Often, they may be interested in using cyberspace for industrial espionage.
- The theft of intellectual property can give a country a significant advantage in international trade.

Zoznam hrozieb

Ľudské hrozby



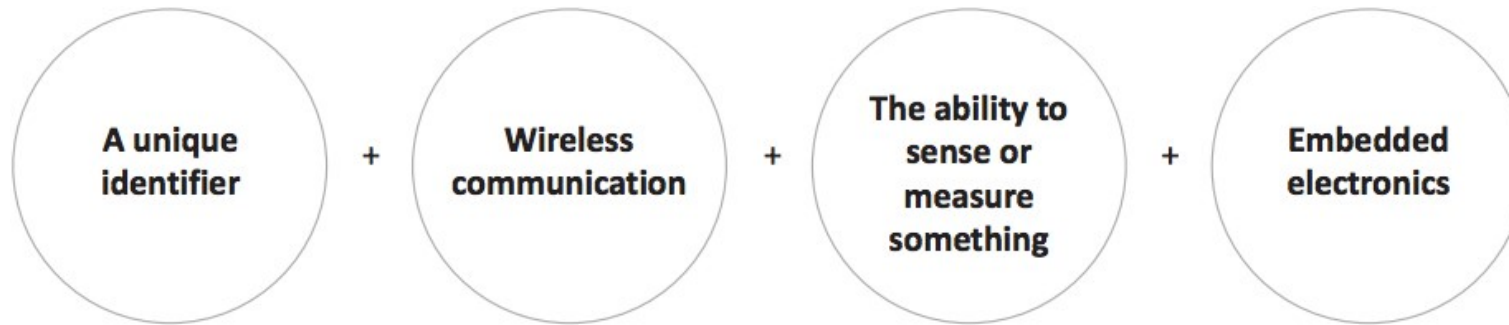
Pôvod hrozby	Motivácia
Heker, kreker	Výzva Ego Postavenie / status Peniaze Povstanie
Terorista	Vydieranie Zničenie Finančný zisk Náboženský fanatizmus Pomsta Politický zisk Mediálne pokrytie
Počítačový kriminálnik	Ničenie informácií Nelegálne zverejňovanie informácií Finančný zisk Neoprávnená zmena údajov
Priemyselná špionáž	Finančný zisk Ekonomická špionáž
Členovia (študenti, zamestnanci)	Zvedavosť Neúmyselné chyby (slabé heslá) Ego Spravodajstvo Peňažný zisk Pomsta



TYP	HROZBY	Pôvod
Fyzické poškodenie	Požiar	NUE
	Poškodenie vodou	NUE
	znečistenie	NUE
	závažná havária	NUE
	zničenie zariadenia alebo médií	NUE
	prach, korózia, mrznutie	NUE
Prírodné udalosti	Klimatický jav	E
	Seizmický jav	E
	Vulkanický jav	E
	Meteorologický jav	E
	Povodeň	E
Strata základných služieb	Porucha klimatizácie alebo vodovodu	NU
	Strata energetického napájania	NUE
	Porucha telekomunikačného zariadenia	NU
Narušenie v dôsledku radiácie	Elektromagnetická radiácia	NUE
	Termálna radiácia	NUE
	elektromagnetické impulzy	NUE
Vyzradenie informácií	Veľa rôznych	...
Technické zlyhanie	Zlyhanie zariadenia	N
	Porucha zariadenia	N
	Saturácia informačného systému	NU
	Softvérová porucha	N
	porušenie udržateľnosti informačného systému	NU
Neautorizované činnosti	Neautorizované používanie zariadenia	U
	Podvodné kopírovanie systému	U
	Použitie falošného alebo kopírovaného softvéru	NU
	poškodenie dát	U
	Nelegálne spracovanie dát	U
Vyzradenie funkcií	Chyba pri použití	N
	Zneužitie práva	NU
	Falšovanie práv	U
	Odopretie činností	U
	Porušenie dostupnosti personálu	NUE

IoT Device Characteristics

- four characteristics of smart devices:



- The applications of smart devices include:
 - Learn things
 - Monitor things
 - Search things
 - Manage things (like cities and traffic)
 - Control things
 - Play with things

<https://smartbear.com/blog/internet-of-things-101/>

Implanted medical devices that monitor metrics of a patient's health—or a wrist-worn fitness meter



Sensors in automobiles that monitor tire pressure and display a light on the dashboard when the tire pressures vary



Consumer appliances that alert owners via text message when a load of laundry is finished or when the user needs milk

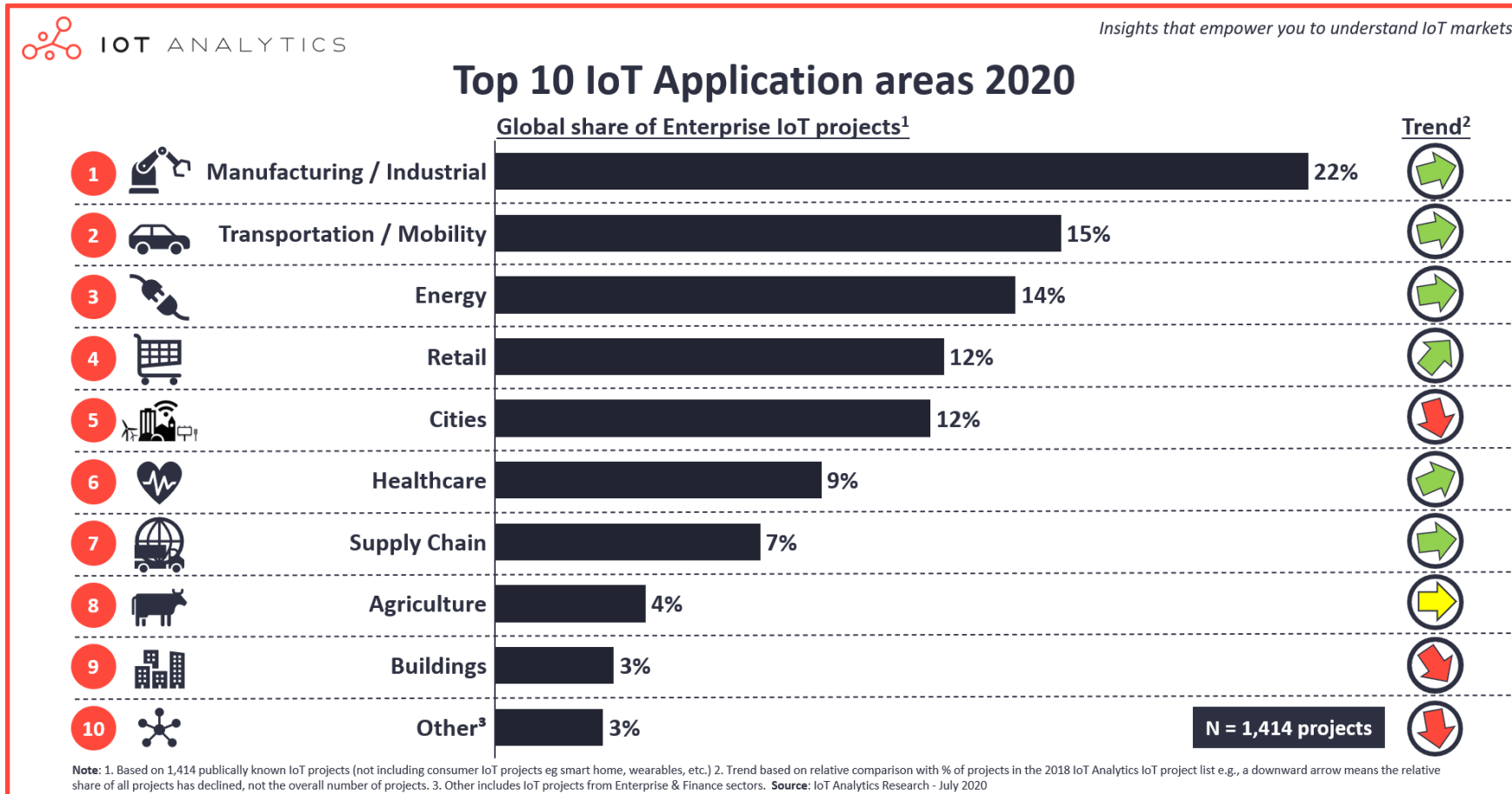


Flow control systems in wastewater treatment plants that determine water volume and act accordingly



Threat Actors: How Secure is the Internet of Things?

IoT Statistics: IoT Application Areas



<https://iot-analytics.com/top-10-iot-applications-in-2020/>

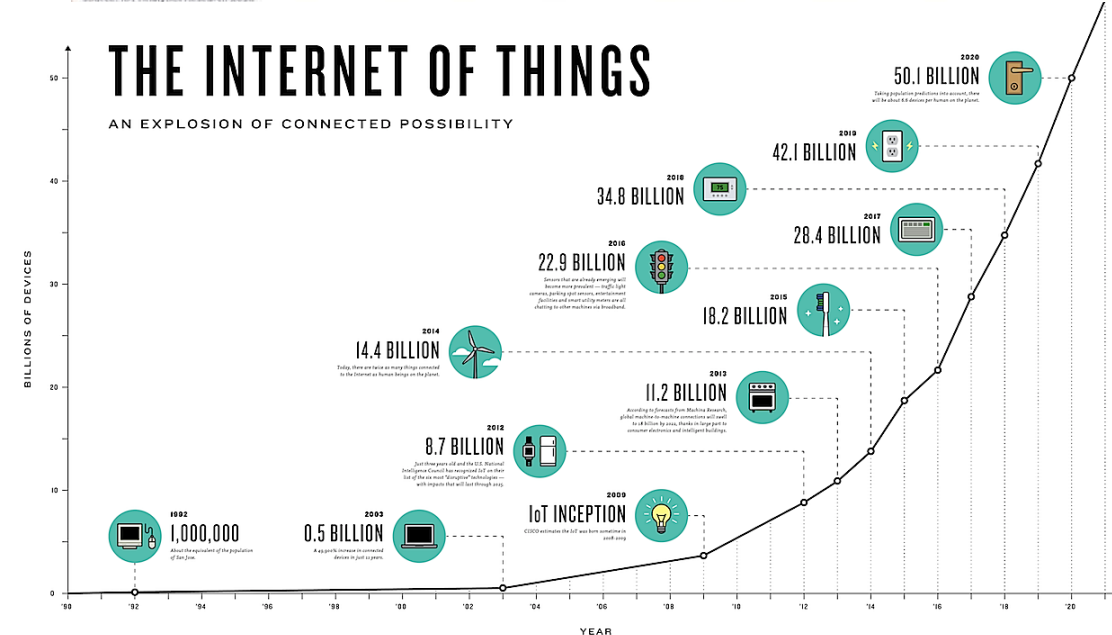
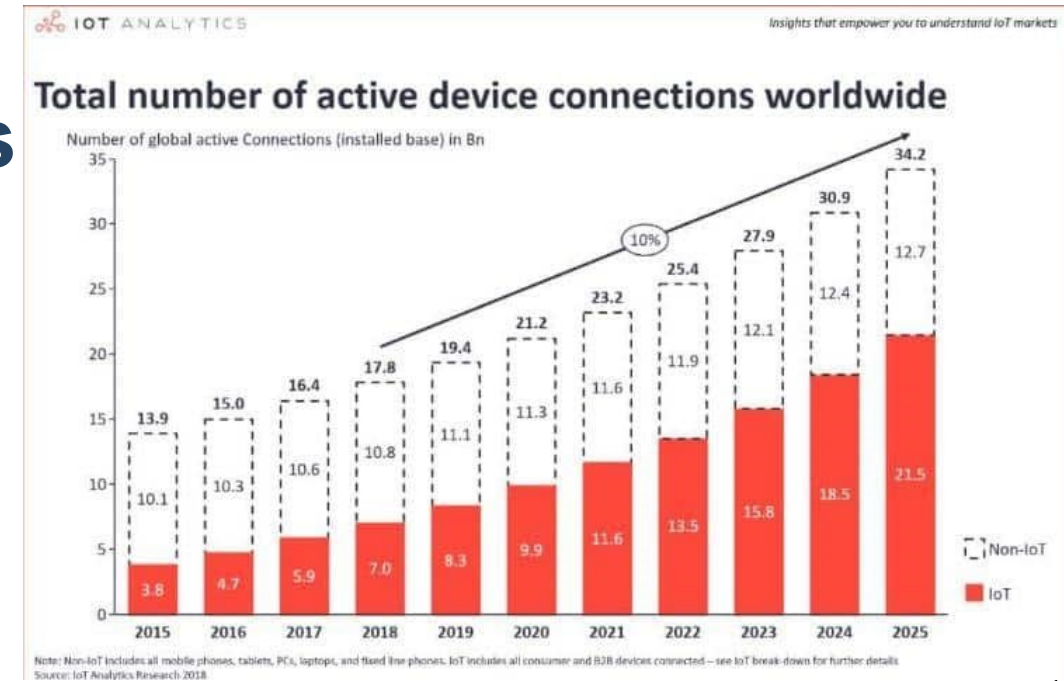
- Nearly 70% of all new vehicles globally will be connected to the internet by 2023. (IDC)
- newer methods of communication that are faster, more efficient, and generally safer for everyone on the road

- On average, an IoT connection is attacked within the first five minutes of connecting to the internet. (NETSCOUT Threat Intelligence Report)

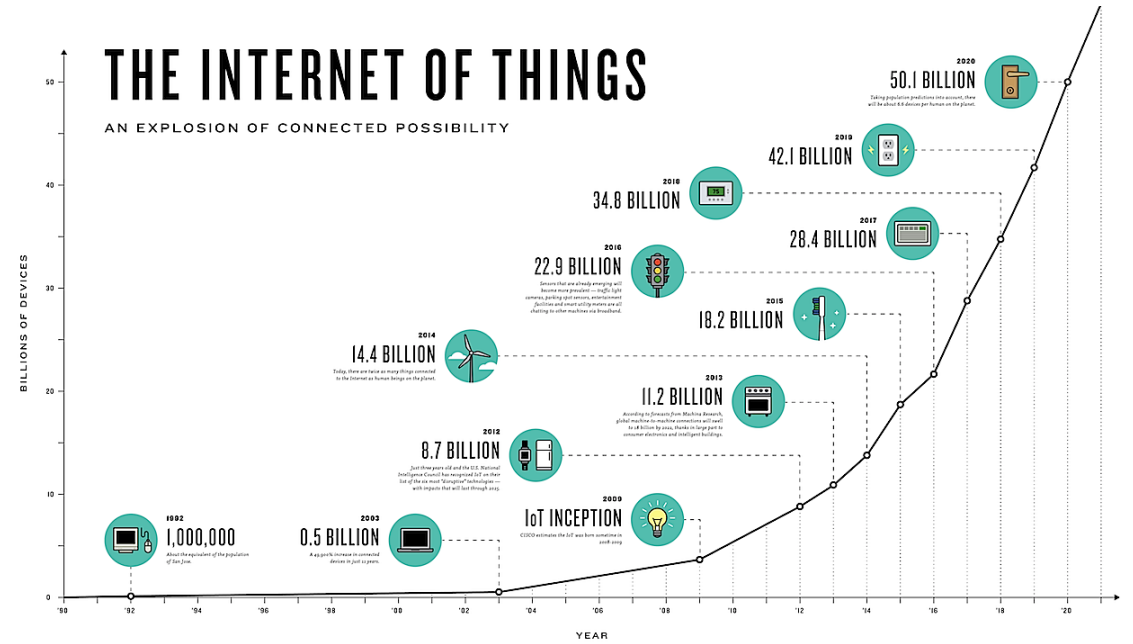
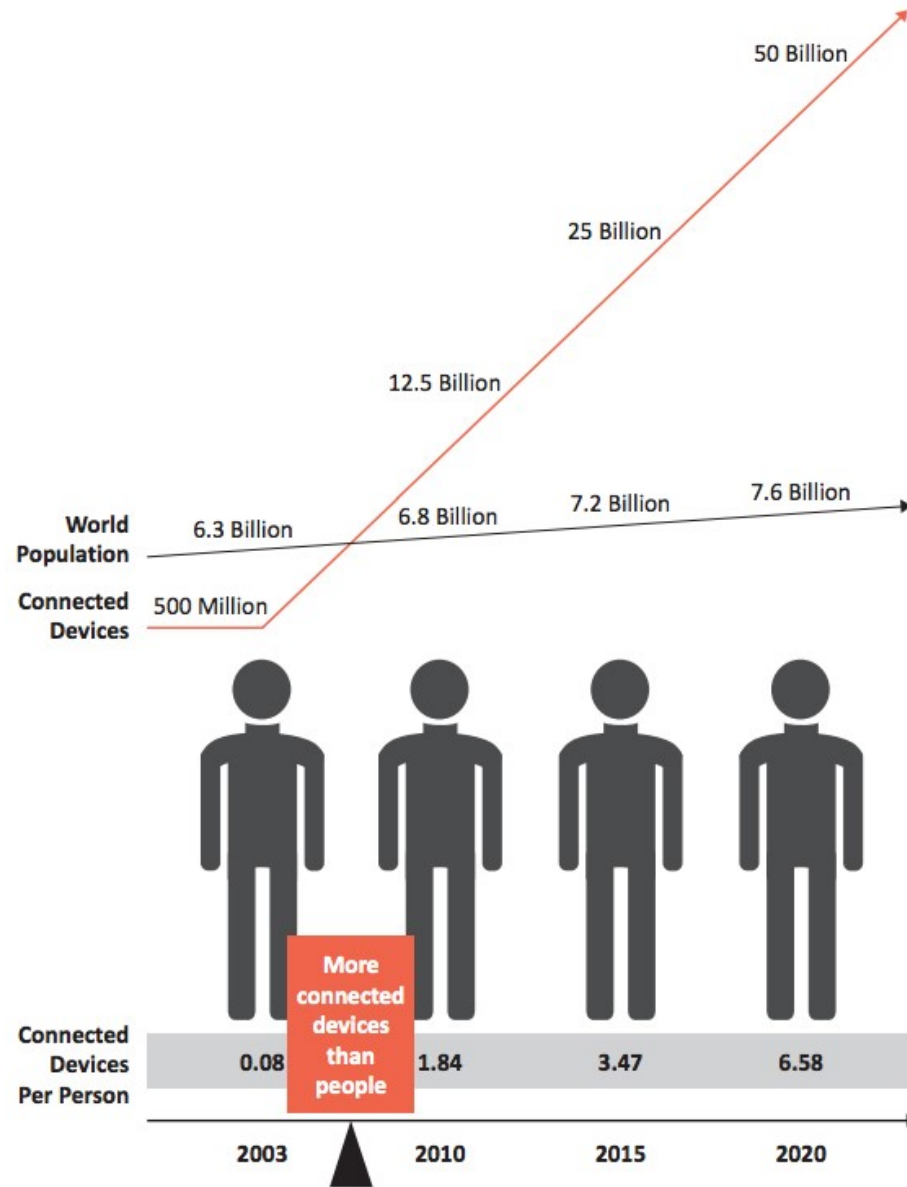
Threat Actors: How Secure is the IoT?

IoT Statistics: Number of devices

- 127 – The number of devices that join the internet every second (*McKinsey Digital*)
- 35% of the IoT market is made up of hardware, zvyšok: sensors, chipsets, ...
- 5G subscriptions will amount to 1.9 Billion by 2024 (*Ericsson*)
 - The introduction of 5G changed many aspects of engaging with technology, including the IoT.



IoT Statistics: Number of devices vs. Number of people



Threat Actors

How Secure is the Internet of Things?

- IoT helps individuals connect things to **improve their quality of life**.
- Problems:
 - Many devices on the internet are **not updated** with the latest firmware.
 - Some older devices were **not even developed to be updated** with patches.
- These two situations create **opportunity** for **threat actors** and **security risks** for the **owners** of these devices.

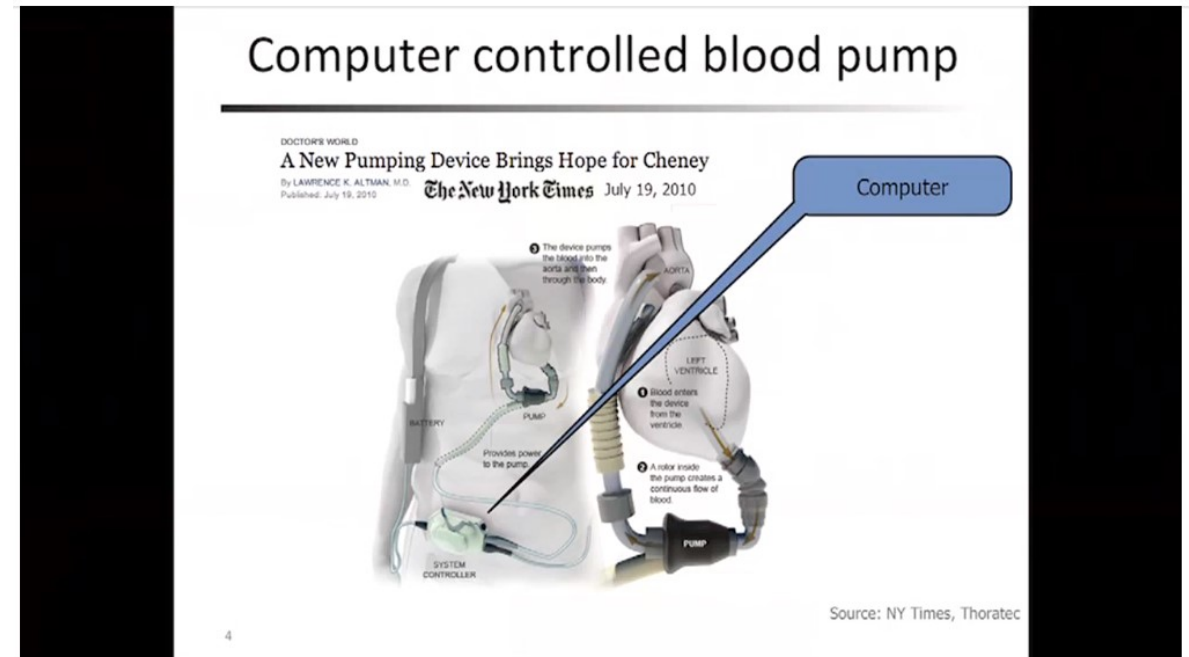


Threat Actors: How Secure is the Internet of Things?

All your devices can be hacked

- Could someone hack your pacemaker?
- Avi Rubin shows how hackers are compromising
 - Cars
 - Smartphones
 - medical devices
- and warns us about the dangers of an increasingly hack-able world.

https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked?language=en



1,334,744 views | Avi Rubin • TEDxMidAtlantic

Like (40K) Share Add

All your devices can be hacked

Read transcript

Conduct a Search of IoT Application Vulnerabilities

Bonusový bod (časť B)

- Nájsi na internete informáciu/video o internetovom prieniku (hack) na Slovensku alebo v svete
 - Rovnomerne budeme hľadať v každom z 10 oblastí **na slajde 37 (Top 10 IoT Application Areas)**
- Spracuj odpovede na otázky:
 - a. What was the target? What is the vulnerability being exploited?
 - b. What information, data, or control can be gained by a hacker exploiting the vulnerability? What was the motive of the hacker? What was the impact of the attack?
 - c. How was the hack performed? What method of attack was used?
 - d. Who was the attacker? What organization or group is the attacker associated with, if any? What about this particular hack interested you specifically?
 - e. How could this attack be prevented or mitigated?
 - f. URL na najlepší zdroj o danom útoku
- Najlepšie zverejníme na KIS webe (podstránka pre predmet RBI)

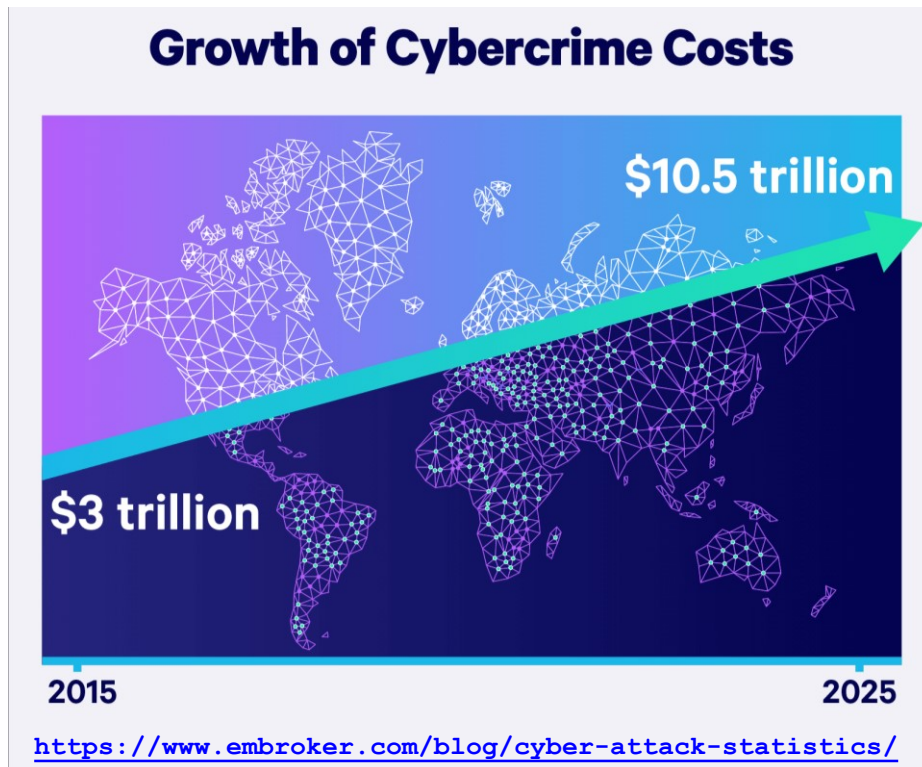


1.3 Threat Impact

Threat Impact

Economic impact of cyberattacks

- The economic impact of cyberattacks is difficult to determine with precision.
- However, it is estimated that businesses will lose over \$10 trillion annually by 2025 due to cyberattacks.



Average annualized cost of cybersecurity (USD)

\$11.7_M

Percentage increase in cost of cybersecurity in a year

22.7%

Average number of security breaches each year

130

Percentage increase in average annual number of security breaches

27.4%

2 > 2017 COST OF CYBER CRIME STUDY

<https://ponemonsullivanreport.com/2017/10/cybercrime-costs-up-23-percent-in-just-two-years-firms-investing-in-wrong-technologies/>

Nástrojov je veľa

Výber produktov je rozmanitý...

Digital Risk Management
crisp, CYBERSPRINT, digital shadows, DigitalStakeout, EXPANSE, LOOKINGGLASS, NAMO-G-O-O, PHISHLABS, RISKIQ, SafeGuard Cyber, ZEROFOX

Mobile Security
appdome, BETTER, BlackBerry, blue cedar, Fyde, Check Point, cellrox, COMMUNITAKE, Cyber@DAPT, INPEIDIC, KODLSPAN, Lookout, mobileiron, prodo, Kaspersky, P-Safe, SaltDNA, SOTI, Symantec, TeleSign, tigerflock, TRUSTLOOK, VAULTO, wander, wickr, ZIMPERIUM

Endpoint Security
AhnLab, avast, Avecto, Avira, Barkly, Bitdefender, BLUEBRIDGE, BUFFERZONE, Carbon Black, Check Point, COMODO, CROWDSTRIKE, CYBERARK, cybereason, CYCLANCE, deepinstinct, ENDGAME, ERICOM, ESET, F-Secure, FARONICS, FORTINET, HYSOLATE, intego, ivanti, KASPERSKY, McAfee, Microsoft, MORPHSEC, NYOTRON, OPSWAT, panda, RECEPTION POINT, SentinelOne, SOPHOS, sparkcognition, STAMENLAB, Symantec, TETRIS, WEBROOT, ZEN

Data Security
anJUNA, boffle, bescrypt, CipherCloud, CLOUDMARK, CryptoMove, DATALOCKER, Fortanix, MyCyber, virtru, clearswift, CODE42, FIDELIS, McAfee, Symantec, BlueTalon, druvo, opentext, SECLORE

Block Chain
Chain, guardtime, IDEE, NuID, remme, vchain, ShoCard, xage

Threat Intelligence
4i@, Blueliv, ANOMALI, LOOKINGGLASS, Malware Hunter, NUCLEON, BlueVoyant, Centripetal, CSISD, Expanded Future, RISKIQ, digital shadows, DOMAINTOOLS, GenexCy, Sigill, SURFWATCH

Security Operations & Incident Response
BlackStratus, CORRELOG, CYSGILANT, DEVO, exabeam, FORTINET, HanSight, Huntsman, IBM, RSA, IGLOO, JASK, logentries, logpoint, LogRhythm, logz.io, McAfee, Palo Alto, Palantir, Securonix, solarwinds, splunk, sumologic, TIBC, Trustwave, Trustlook, ataridos, ayehu, CYBERPOINT, CYBERTRAC, DARKLIGHT, DEMISTO, FIMBI, FIREEYE, Microsoft, Palo Alto Networks, radar, RAPID7, Raytheon, resilient, SEC, servicenow, Security, SIFT, SWIMLANE, THREATPATH, ThreatConnect, UPLEVEL, VERINT, AWAKE, Bay Dynamics, DARKTRACE, DTEX, Fluency, haystack, IronNet, mistnet, observo, patternex, Reservoir Labs, RSA, SEC, SECURONIX, THETARAY, Triplicyber, VECTRA, Veriato

Risk and Compliance
AXONIUS, Balbix, cavin, CYBEROBSERVER, cyberGRX, DELVE, FIREHQ, KENNA, FIEHERRMAN, NOPSEC, OPAG, Outpost24, panaseer, PREVALENT, REDSEAL, riskrecon, SKYBOX, tenable, UpGuard, VENAFT, zeguro, BITSIGHT, CORAX, FICO, RiskLens, SecurityScorecard, ATTACOR, Cobalt, CEONUS, CYBERRAT, CYCIGNTO, CYMULATE, DEPTH, tufin, MAZEBOLT, PCVSY, PICUS, RAPID7, SafeBreach, VERODIN, algosec, SECURE, Lockpath, MetricStream, neturix, Onspring, RESOLVER, RSA, SAI GLOBAL, Eranocada, CYBER, IRONSCALE, proofpoint, RANGEFORCE

Identity & Access Management
Accepto, Auth0, AVERON, BehaviorSec, BIOCATCH, Calsignr, Certify, CLEF, CORE, EXOSTAR, FORGELOCK, FUDD, Google, HPR, imprivata, INTRINSIC ID, nok, pindrop, plainID, SAASPASS, transmit, SECUREPUSH, SILVERFORT, tascent, ThreatMetrix, TransUnion, TRUSONA, UNICJUND, LINKEN, V-KEY, Centrify, IBM, idaptive, Microsoft, okta, RSA, onelogin, ORACLE, THALES, BeyondTrust, PING, CYBERARK, HITACHI, ManageEngine, ONE IDENTITY, Remediant, SECURELINK, thycotic, AXIOMATICS, helpsystems, SailPoint, simeio, Akamai, IDExperts, ID.me, loginradius, Trulioo, vchain, verato, VERIFF

Network & Infrastructure Security
Barracuda, BLUHEXAGON, BLUVECTOR, CISCO, CORSA, lastline, FIREEYE, FORTINET, HUAWEI, HYSOLATE, JOE Security, JUNIPER, McAfee, mimecast, OPSWAT, paloalto, RESEC, GATESCANNER, SONICWALL, SOPHOS, Symantec, VORTEX, WIZARD, aruba, ALCUNET, ARONIUS, Cyber, Cytex, Extreme, FORESCOUT, NANOSEC, SKYPORT, Trustwave, zentao, Geniux, TEMPERED, VERA, Zscaler, Check Point, Imperva, neustar, NERUSGUARD, NSFOCUS, ORACLE, SECURE4, STACKPATH, BLUECAT, neustar, Threat STOP, Quod?, efficient, Infoblox, SECURE, algosec, CATO, endian, FORCEPOINT, GAJSHIELD, HARTNET, OPAG, SANGFOR, seccloud, SONICWALL, STORMSHIELD, tufin, fidelis, ACALVY, Attivo, Ethave, Counter, VIBEX, CyberTrap, SMOKESCREEN, Cymmetria, TRAPX, APERIO, BRYSHORE, BELDEN, CERNICE, CYBERBIT, FIRMITAS, Indegy, dimension, NOZON, RAS, CLARITY, CyberX, DRAGOS, PFP, radiflow, Rhebo, SCANDIA, VERINT, sentryo, AWAKE, BRICTR, CGS, CloudShark, corelight, CORE, Corvil, DARKTRACE, ExtraHop, GREYCORTEX, IronNet, MixMode, NETSCOUT, PERCH, Plixer, SEC, SS8, utimaco, VECTRA

Workload
anchore, aqua, deepfence, NeuVector, Polyverse, portanirt, Qualys, StackRox, Sysdig, Twitlock, PACKET, Cavin, Check Point, CloudGuard, CLOUDWAY, CODEWISE, Guardicore, TRUST, illumio, Lacework, SHIELDX, Inven stack, JAMNOX, AVANIAN, bitglass, CipherCloud, CISCO, DRONET, Managed Networks, Microsoft, netskope

Cloud Security
anchore, aqua, deepfence, NeuVector, Polyverse, portanirt, Qualys, StackRox, Sysdig, Twitlock, PACKET, Cavin, Check Point, CloudGuard, CLOUDWAY, CODEWISE, Guardicore, TRUST, illumio, Lacework, SHIELDX, Inven stack, JAMNOX, AVANIAN, bitglass, CipherCloud, CISCO, DRONET, Managed Networks, Microsoft, netskope

WAF and Application Security
Barracuda, AIO, Akamai, ALERT LOGIC, Citrix, ergon, CyKickLabs, FORTINET, Imperva, NETSPI, Omnisys, netsparker, CONTRAST, portshift, Quoyis, ORACLE, RAPID7, Reblaze, riverbed, Pentasecurity, Radware, riverbed, SUCURI, SEWOKS, SHIELD, THREATX, Signal Sciences, safreen, STACKPATH, TEMPLARBIT, Trustwave, VERACODE, wallarm, Synack, waratek, Whitehat, Virusant, hackerone, IBM

Network
Barracuda, BLUHEXAGON, BLUVECTOR, CISCO, CORSA, lastline, FIREEYE, FORTINET, HUAWEI, HYSOLATE, JOE Security, JUNIPER, McAfee, mimecast, OPSWAT, paloalto, RESEC, GATESCANNER, SONICWALL, SOPHOS, Symantec, VORTEX, WIZARD, aruba, ALCUNET, ARONIUS, Cyber, Cytex, Extreme, FORESCOUT, NANOSEC, SKYPORT, Trustwave, zentao, Geniux, TEMPERED, VERA, Zscaler, Check Point, Imperva, neustar, NERUSGUARD, NSFOCUS, ORACLE, SECURE4, STACKPATH, BLUECAT, neustar, Threat STOP, Quod?, efficient, Infoblox, SECURE, algosec, CATO, endian, FORCEPOINT, GAJSHIELD, HARTNET, OPAG, SANGFOR, seccloud, SONICWALL, STORMSHIELD, tufin, fidelis, ACALVY, Attivo, Ethave, Counter, VIBEX, CyberTrap, SMOKESCREEN, Cymmetria, TRAPX, APERIO, BRYSHORE, BELDEN, CERNICE, CYBERBIT, FIRMITAS, Indegy, dimension, NOZON, RAS, CLARITY, CyberX, DRAGOS, PFP, radiflow, Rhebo, SCANDIA, VERINT, sentryo, AWAKE, BRICTR, CGS, CloudShark, corelight, CORE, Corvil, DARKTRACE, ExtraHop, GREYCORTEX, IronNet, MixMode, NETSCOUT, PERCH, Plixer, SEC, SS8, utimaco, VECTRA



Zdroj: konferencia SecTec, 28.5.2020

Threat Impact

PII, PHI, and PSI

Personally Identifiable Information (PII)

- any information that can be used to positively identify an individual
 - Name
 - Social security number
 - Birthdate
 - Credit card numbers etc.
- Protected by the General Data Protection Regulation (GDPR) in the EU (by HIPAA in the US)
- Cybercriminals aim to obtain these lists of PII
 - can be sold on the dark web
 - and used to create fake financial accounts
 - credit cards
 - short-term loans (pôžičky)
- Subsets of PII:
 - Protected Health Information (PHI)**
 - subset of PII
 - Included in Electronic Medical Records (EMRs) created and maintained by the medical community
 - Personal Security Information (PSI)**
 - usernames, passwords, and other security-related information that individuals use to access information or services on the network.

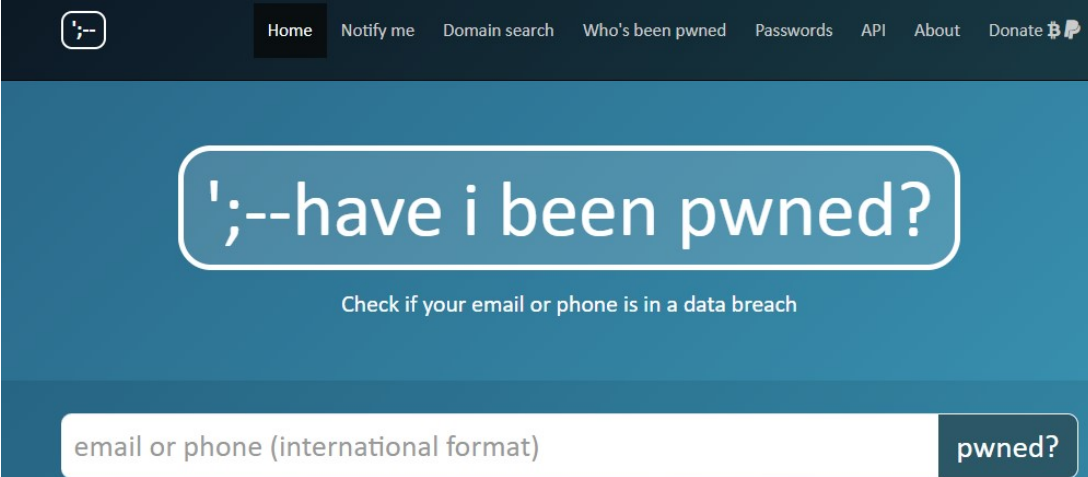


Threat impact – real stories

Hacks which involved stolen PII or PHI

- In 2019, an online **graphic design tool website** experienced a **data breach** in which **PII** for approximately **137 million users** was viewed by hackers with user details for 4 million accounts appearing on the internet.
- In 2020, a major **Chinese social media** company was hacked resulting in theft of **PII**, including phone numbers, stolen from **172 million users**. The theft did not include passwords, so the data was available for a low price on the internet.
- In 2019, a company that makes **games** that are played on **Facebook** was hacked and the **PII** of **218 million users** was stolen.

- <https://haveibeenpwned.com/>

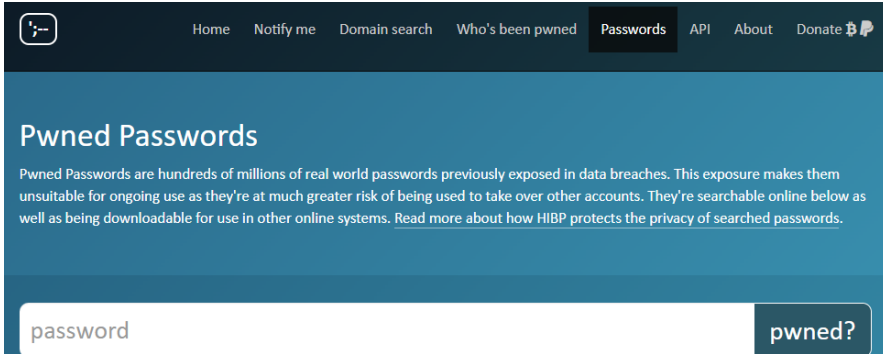


Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) pwned?



Home Notify me Domain search Who's been pwned Passwords API About Donate

Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

password pwned?

PII and Password vaults

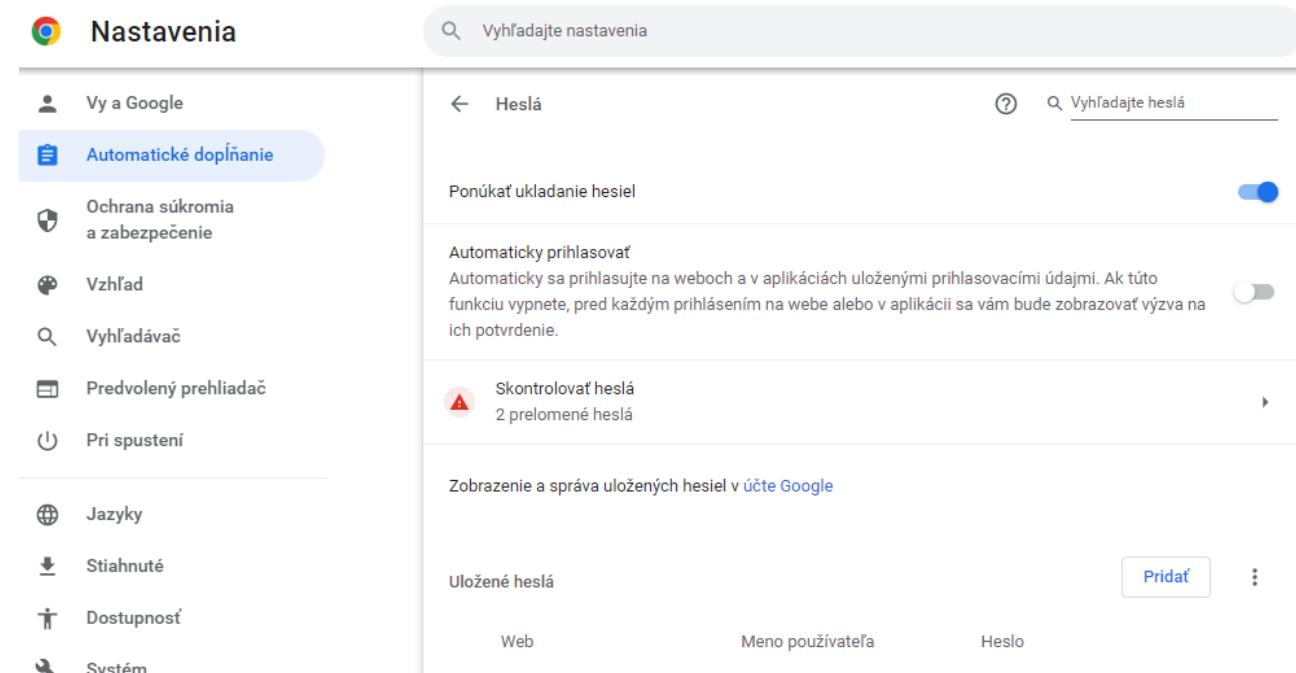
Password managers

- stores and organizes usernames and passwords in the form of:
 - software application / web-based application
 - integrated into web browser
- cloud-based vs. local storage
- variety of services that may include:
 - Site and password breach alerts
 - Syncing across multiple devices
 - Family-sharing
 - Assistance changing old passwords automatically
 - Auto-filled information on forms
 - Encrypted file storage vaults for your financial and other sensitive data
 - Industry-standard encryption
 - Security questions and answers
 - Two-factor authentication or multi-factor authentication
 - Fingerprint and facial recognition
 - Credit monitoring
 - 24/7 customer service

Pros and cons, are password managers secure?

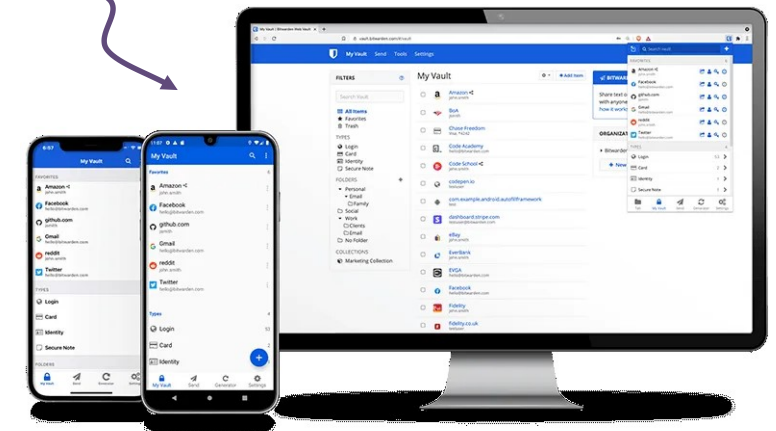
<https://us.norton.com/internetsecurity-privacy-password-manager-security.html#>

Integrated into web browser:



Software applications / web-based applications

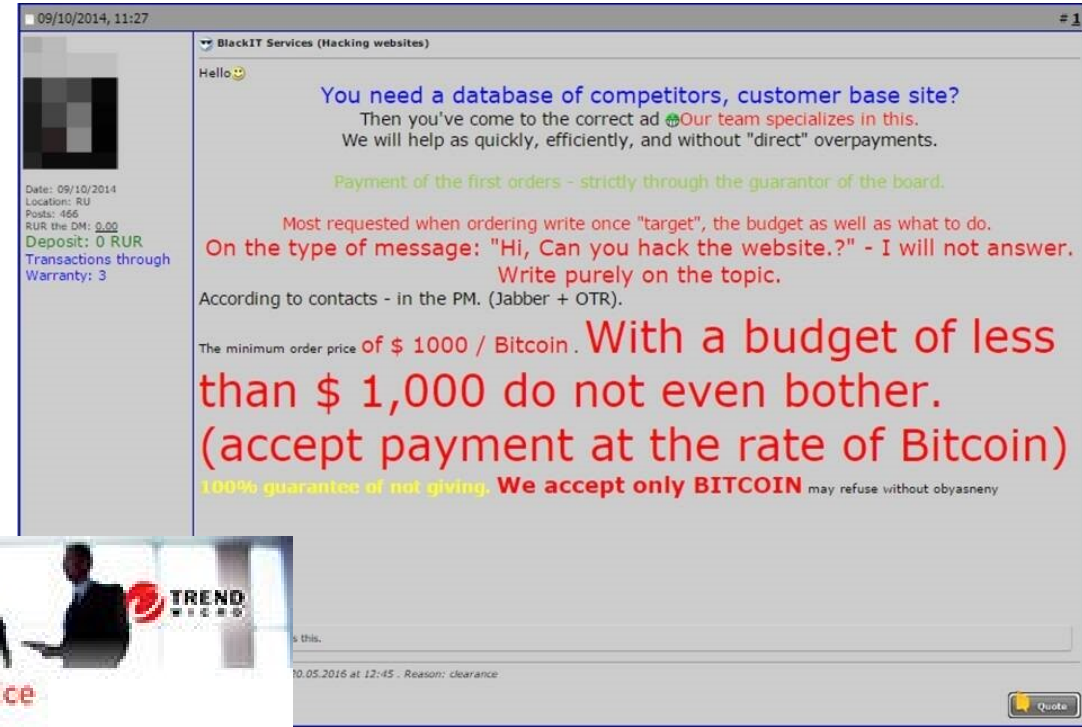
- <https://opensource.com/article/16/12/password-managers>
- <https://bitwarden.com/>



Threat Impact: Bussiness

Lost Competitive Advantage

- The loss of **intellectual property** to competitors is a serious concern.
- An additional major concern is the loss of **trust** that comes when a company is unable to protect its customers' personal data.
- The loss of **competitive advantage** may come from this loss of trust rather than another company or country stealing trade secrets.



<https://documents.trendmicro.com/images/TEEx/guides/exec-brief-espionage-as-a-service.pdf>

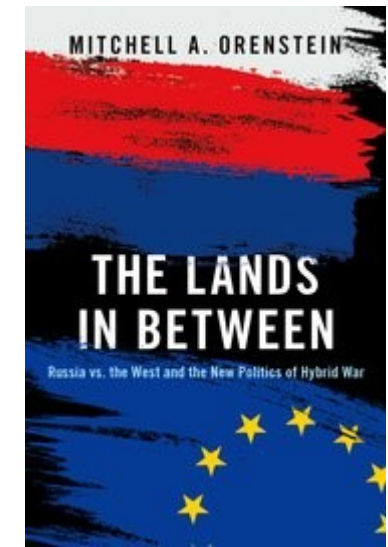
Threat Impact: Cyberwarefare Politics and National Security

- It is not just businesses that get hacked.
- State-supported hacker warriors can cause disruption and destruction of vital services and resources within an enemy nation.
- The internet has become essential as a medium for commercial and financial activities.
 - Disruption of these activities can devastate a nation's economy.
- The **Stuxnet** worm was specifically designed to impede Iran's progress in enriching uranium that could be used in a nuclear weapon.
 - Stuxnet is a prime example of a network attack motivated by national security concerns.
- In February 2016, a hacker published the **personal information** of 20,000 U.S. **FBI employees** and 9,000 U.S. Department of Homeland Security (DHS) employees.
 - The hacker was apparently politically motivated.



<https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/>

Zatiaľ čo politika sa stále viac scvrkáva na „civilizačnú voľbu“ medzi Ruskom a Západom s nulovým súčtom, tí, ktorí sa dostanú na vrchol politického systému v krajinách medzi nimi, sú často neideologickí sprostredkovatelia moci, ktorí našli spôsob, ako profitovať z oboch strán, pričom si berú odmeny z Ruska aj zo Západu. Politické patológie týchto malých, zraniteľných a zaostalých štátov v Európe sú čoraz častejšie aj našimi problémami. V tomto prehlbujúcom sa konflikte sme všetci krajinami medzi nimi.

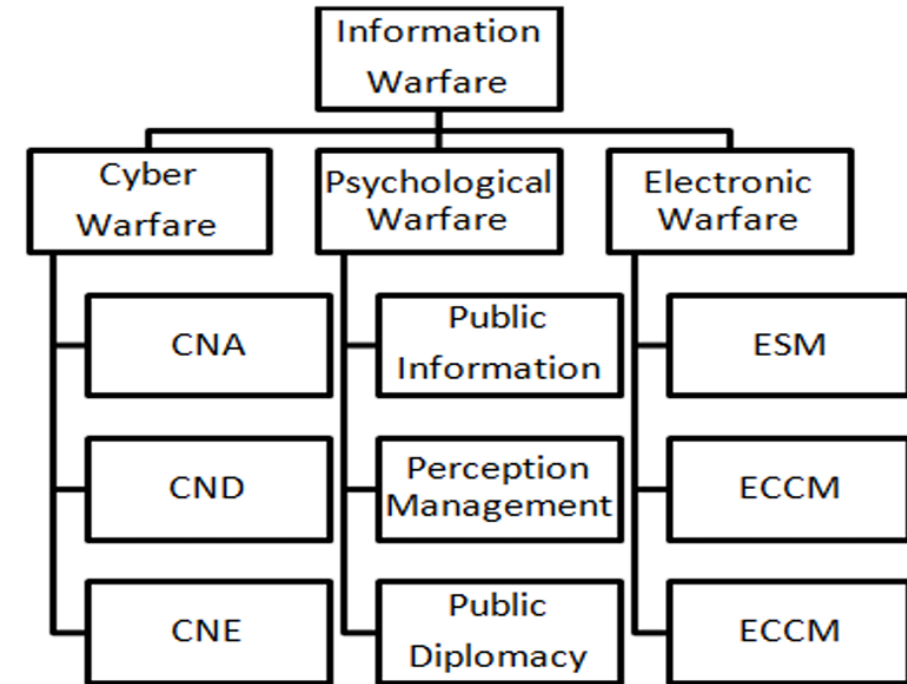


<https://global.oup.com/academic/product/the-lands-in-between-9780190936143>

Threat impact

Cyberwarfare

- Cyberwarfare is a subset of **information warfare**
- Its objective is to... (one or more)
 - disrupt (availability)
 - corrupt (integrity)
 - exploit (confidentiality or privacy)
- It can be directed against
 - military forces
 - critical infrastructures
 - other national interests (economic targets, ...)
- It involves several teams that work together
- **Botnet** might be one of several tools to be used for launching the attack.



http://ijrar.com/upload_issue/ijrar_issue_20542533.pdf

7 Types of Cyberwarfare Attacks



Espionage



Sabotage



Denial-of-service
(DoS) Attacks



Electrical
Power Grid



Propaganda
Attacks



Economic
Disruption



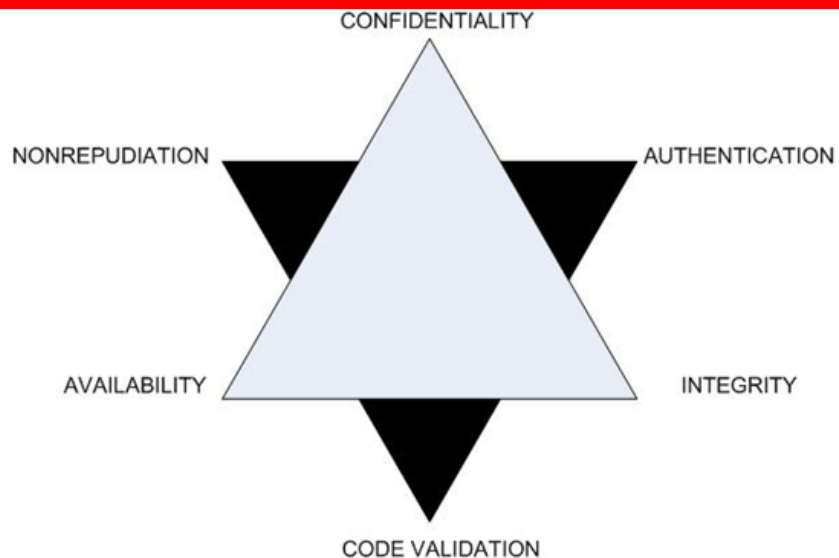
Surprise
Attacks



Threat impact

Atribúty bezpečnosti

- Dôvernosť (confidentiality)
- Integrita (integrity)
- Dostupnosť (availability)
- Autenticita (authenticity)
- Nepopierateľnosť (non-repudiation)
- Správnosť kódu (code validation)



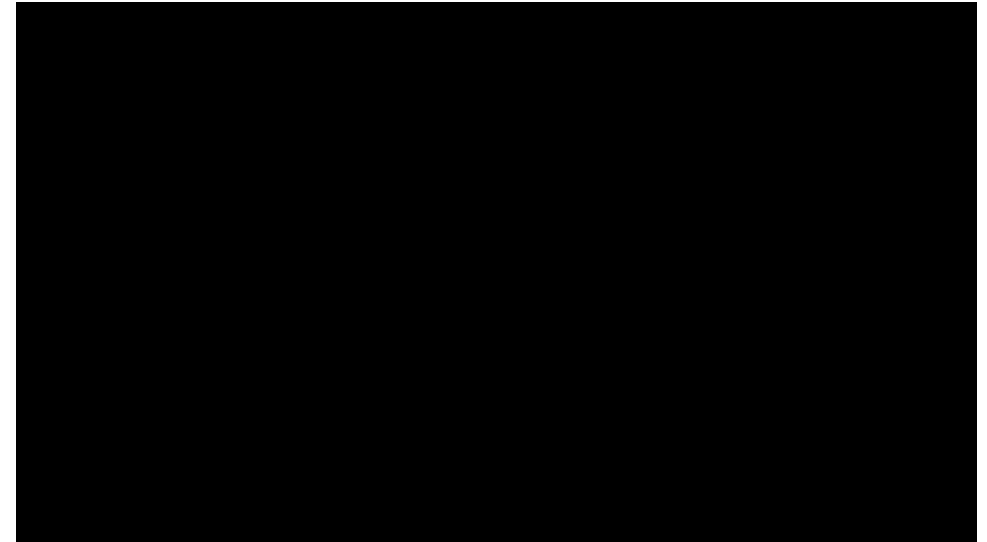
	Integrita	Dostupnosť	Dôvernosť	Existencia motívu útočníka	Existencia prípadu z minulosti	Ohodnotenie
1	+	+	+	+	+	5
2	+	+	-	+	+	5
3	-	+	+	+	+	5
4	+	-	+	+	+	5
5	+	-	-	+	+	4
6	-	+	-	+	+	4
7	-	-	+	+	+	4
8	+	+	+	+	-	4
9	+	+	-	+	-	4
10	-	+	+	+	-	4
11	+	-	+	+	-	4
12	+	-	-	+	-	3
13	-	+	-	+	-	3
14	-	-	+	+	-	3
15	+	+	+	-	+	3
16	+	+	-	-	+	3
17	-	+	+	-	+	3
18	+	-	+	-	+	3
19	+	-	-	-	+	2
20	-	+	-	-	+	2
21	-	-	+	-	+	2
22	+	+	+	-	-	2
23	+	+	-	-	-	2
24	-	+	+	-	-	2
25	+	-	+	-	-	2
26	+	-	-	-	-	1
27	-	+	-	-	-	1
28	-	-	+	-	-	1

Deepfakes are getting better

Zraniteľnosti pre dnešnú spoločnosť' „Nabodobeniny sa zlepšujú“

Obavy:

- „*Môžu deepfakes oslabiť demokraciu?*“
 - .. napodobenina verejnej osobnosti načasovaná na správny okamih..
- Preteky v zbrojení ako ich odhaliť
 - Napr. obava z volieb v roku 2020 v USA
 - Darpa z Pentagonu – 10x miliónov na mediálny forenzný výskumný program
 - V kongrese – výzva na legislatívu zakazujúcu ich škodlivé používanie

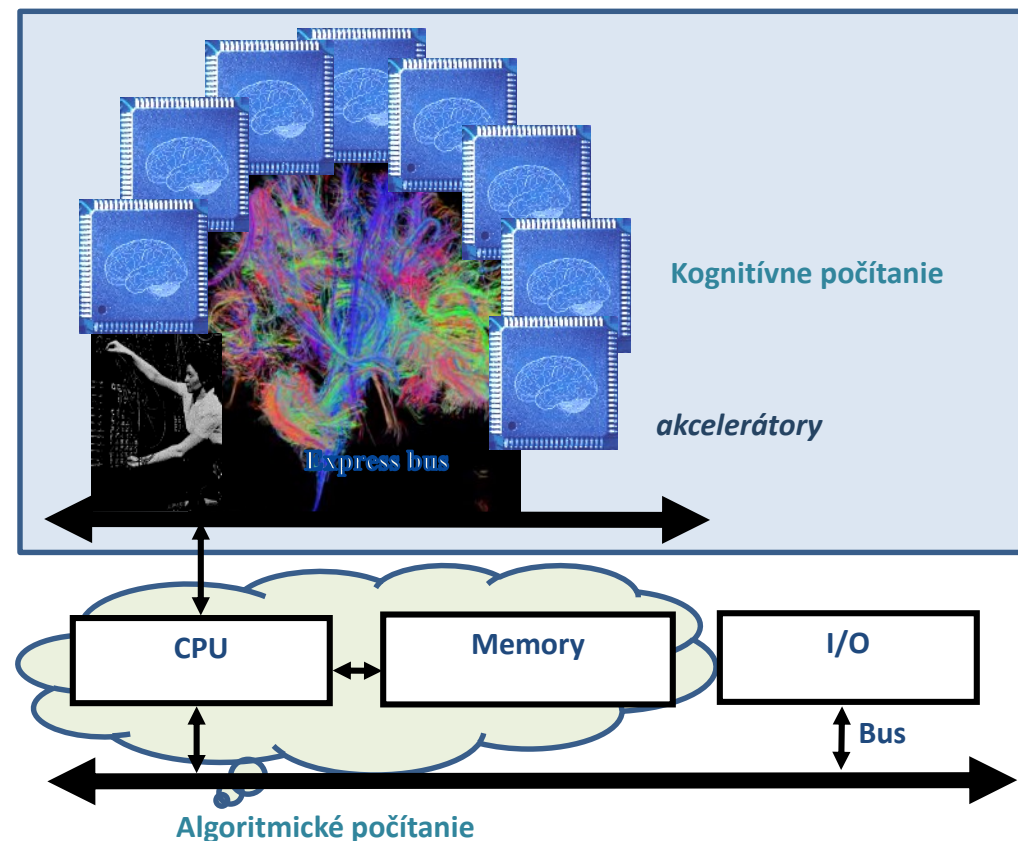


<https://www.youtube.com/watch?v=AmUC4m6w1wo>

Strojové učenie v kybernetickej bezpečnosti

- Ochrancovia:
 - pokiaľ sa vieme strojovým učením natrénovať ako vyzerá legitímna prevádzka, tak potom vieme efektívne detegovať aj útoky, vrátane neznámych/nových typov útokov.
- Útočníci:
 - Môžu strojové učenie použiť na ľahké generovanie takých útokov, ktoré sa budú podobáť na legitímnu prevádzku, a bude ťažké ich detegovať.

Strojové učenie majú k dispozícii ochrancovia aj útočníci.



Search for Attacks that have weakened democracy

Bonusový bod (časť C)

- Nájdi na internete informáciu/video o internetovom prieniku (hack) na Slovensku alebo v svete – ktorý má **dopad na demokraciu**
 - Oslabenie ľudských práv
 - Sledovanie ľudí
 - Manipulácia, ovplyvnenie volieb, ..
 - Rozvrat v štáte
 - Cyber vigilantism
- Spracuj odpovede na otázky:
 - a. What was the target? What is the vulnerability being exploited?
 - b. What information, data, or control can be gained by a hacker exploiting this vulnerability? What was the motive of the hacker? What was the impact of the attack?
 - c. How was the hack performed? What method of attack was used?
 - d. Who was the attacker? What organization or group is the attacker associated with, if any? What about this particular hack interested you specifically?
 - e. How could this attack be prevented or mitigated?
 - f. URL na najlepší zdroj o danom útoku
- Najlepšie zverejníme na KIS webe (podstránka pre predmet RBI)



Future of Democracy in the Digital Age
(Anonymous Survey 2020)

<https://www.elon.edu/u/imagining/surveys/future-of-democracy-2020/anonymous/>

1.4 The Danger Summary

What Did I Learn in this Module?

- Threat actors can hijack banking sessions and other personal information by using “evil twin” hotspots.
- Threat actors include, but are not limited to, amateurs, hacktivists, organized crime groups, state sponsored, and terrorist groups.
- As the Internet of Things (IoT) expands, webcams, routers, and other devices in our homes are also under attack.
- Personally Identifiable Information (PII) is any information that can be used to positively identify an individual.
- The medical community creates and maintains Electronic Medical Records (EMRs) that contain Protected Health Information (PHI), a subset of PII.
- Personal Security Information (PSI) includes usernames, passwords, and other security-related information that individuals use to access information or services on the network.

New Terms and Commands

- Evil twin hotspots
- Programmable Logic Controllers (PLCs)
- Threat Actors
- Hacktivists
- Cyberattacks
- Distributed Denial of Service (DDoS)

- Internet of Things (IoT)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Electronic Medical Records (EMRs)

- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)
- Personal security information (PSI)
- Cyberwarfare



Module 2

Fighters in the War Against Cybercrime

Module Objective: Explain how to prepare for a career in cybersecurity operations

Topic Title	Topic Objective
The Modern SOC	Explain the mission of the security operations center (SOC).
Becoming a Defender	Describe resources available to prepare for a career in cybersecurity operations.

2.1 The Modern Security Operations Center

Fighters in the War Against Cybercrime

Elements of a SOC

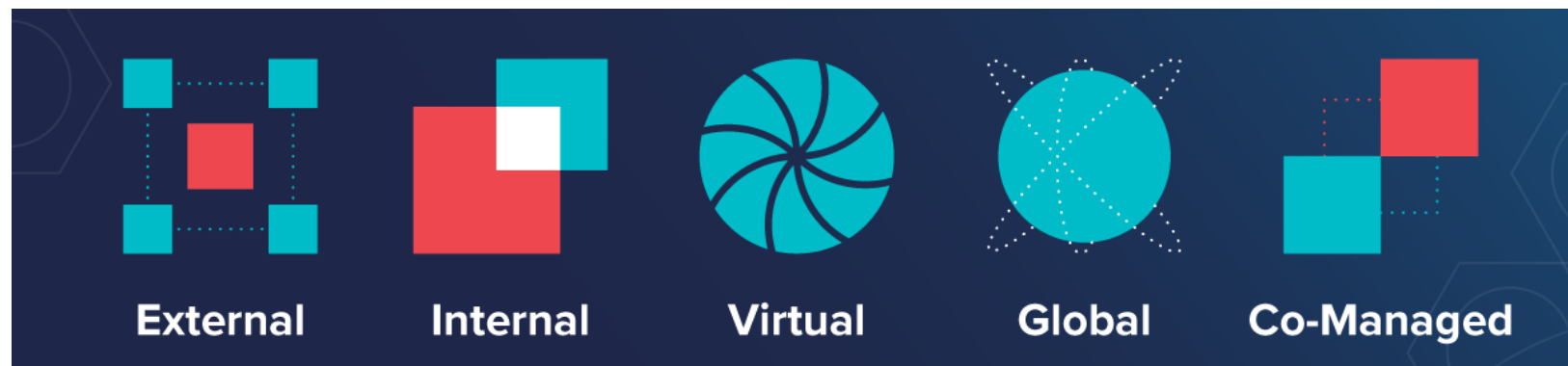
- for defending against cyber threats, organizations typically use the services of professionals from a Security Operations Center (SOC) to use
 - formalized
 - structured
 - and disciplined approach
- SOC provides a **broad range of services**
 - from monitoring and management
 - to comprehensive threat solutions and customized hosted security.

Triad of Security Operations: People, Process and Technology



Type of SOC models

- SOC architecture models:
 - **External SOC** — entire SOC or elements of a SOC can be contracted out to SOC provider, such as Cisco's Managed Security Services.
 - **Dedicated or Internal SOC** — The enterprise sets up its own cybersecurity team within its workforce. Wholly in-house, owned and operated by a business
 - **Virtual SOC** — The security team does not have a dedicated facility and often works remotely.
 - **Global or Command SOC** — A high-level group that oversees smaller SOC's across a large region.
 - **Co-Managed SOC** — The enterprise's internal IT is tightly coupled with an outsourced vendor to manage cybersecurity needs jointly.



Fighters in the War Against Cybercrime

People in the SOC – Tiers (úrovne)

SOCs assign job roles (*pracovné úlohy*) by tiers, according to the expertise and responsibilities required for each.

■ Tier 1 **Alert Analyst**

- **Monitor** incoming alerts (security alert queues in ticketing system)
 - verify that a **true** incident has occurred
 - **Basic threat mitigation**
 - or **forward** tickets to Tier 2 (opens ticket), if necessary
 - otherwise – false alarm/alert
 - and system need to be updated
 - otherwise – can not be resolved => tier 2



■ Tier 2 **Incident Responder**

- **deep investigation** of incidents
- **advise remediation** or action to be taken
(*odporučia nápravu/akciu*)



■ Tier 3 **Threat Hunter**

- expert in network, endpoint, threat intelligence, **malware reverse engineering**
- **tracing** the processes of the malware to determine its impact and how it can be removed (**+ preventive measures**)
- deeply involved in **hunting** for **potential threats** and **implementing threat detection tools**
 - search for cyber **threats that are present** in the network but have not yet been detected.



■ **SOC Manager**

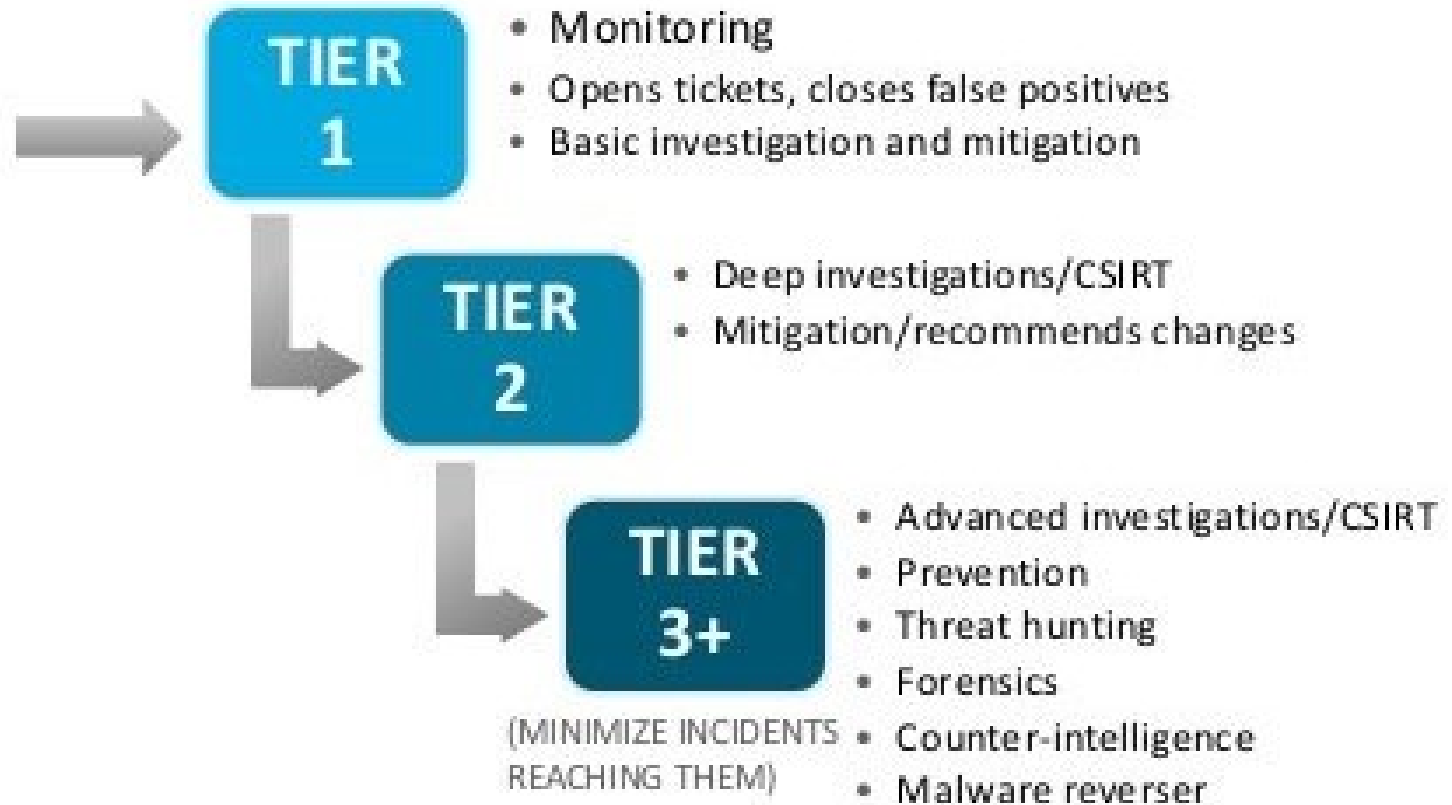
- **manages all the resources** of the SOC
- serves as the **point of contact** for the larger organization or customer.
- develop a workflow model
- implement standardized operating procedures (SOPs) for the incident-handling process that guides analysts through triage and response procedures

Simplified SOC Tiers

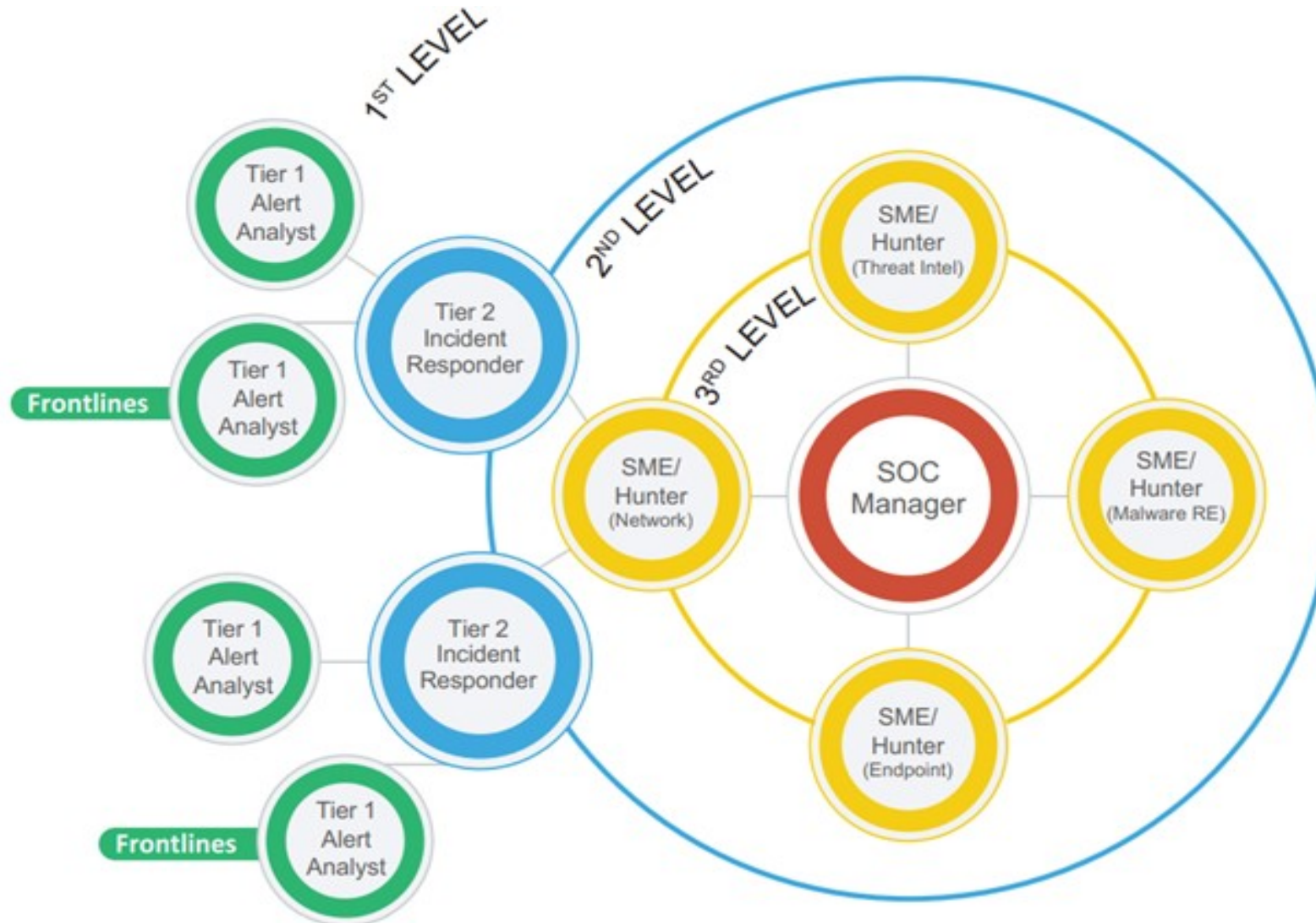


ALERTS FROM:

- Security Intelligence Platform
- Help Desk (Users)
- Other IT Depts.



People in the SOC – interaction between job roles

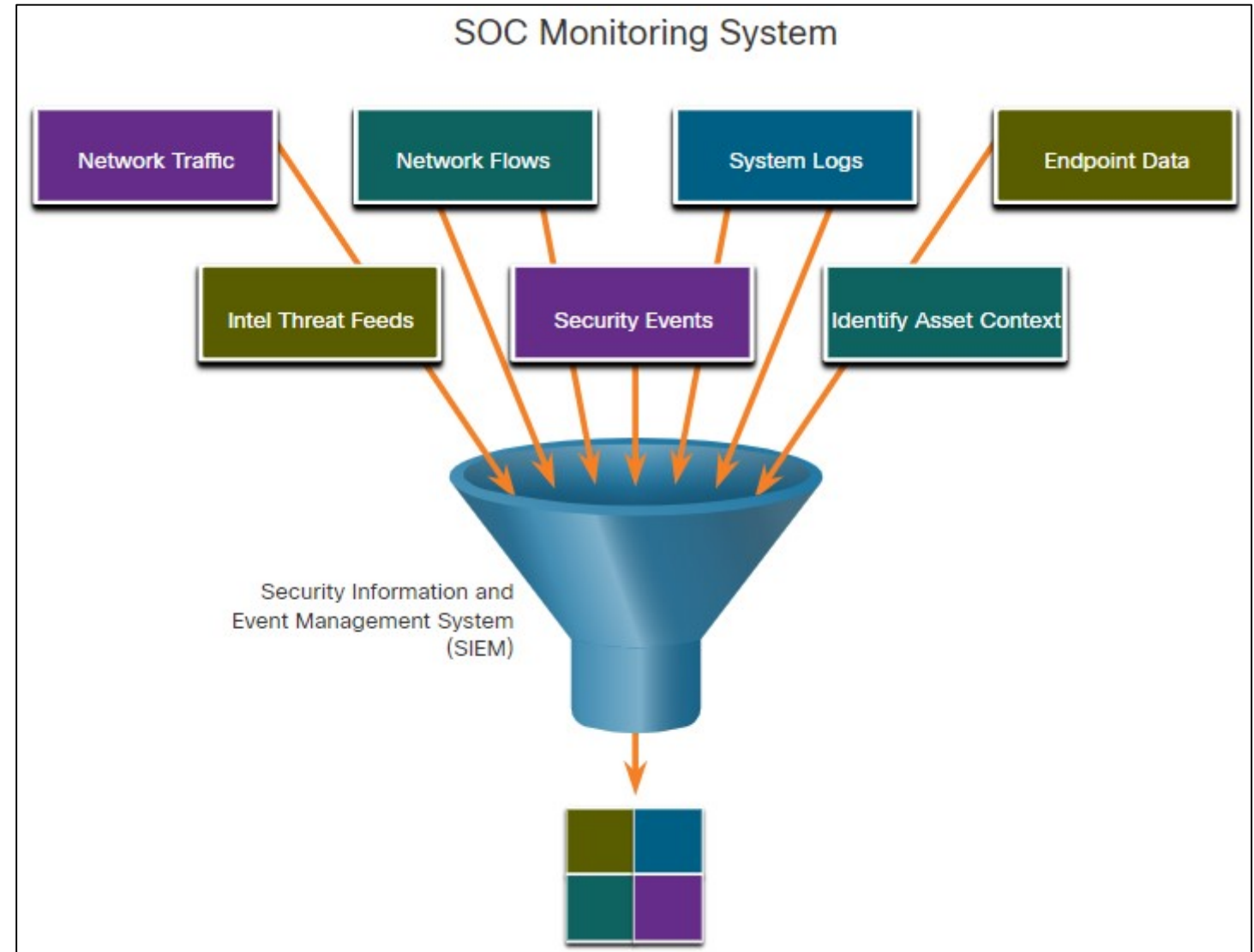


Source: SANS Institute

Fighters in the War Against Cybercrime

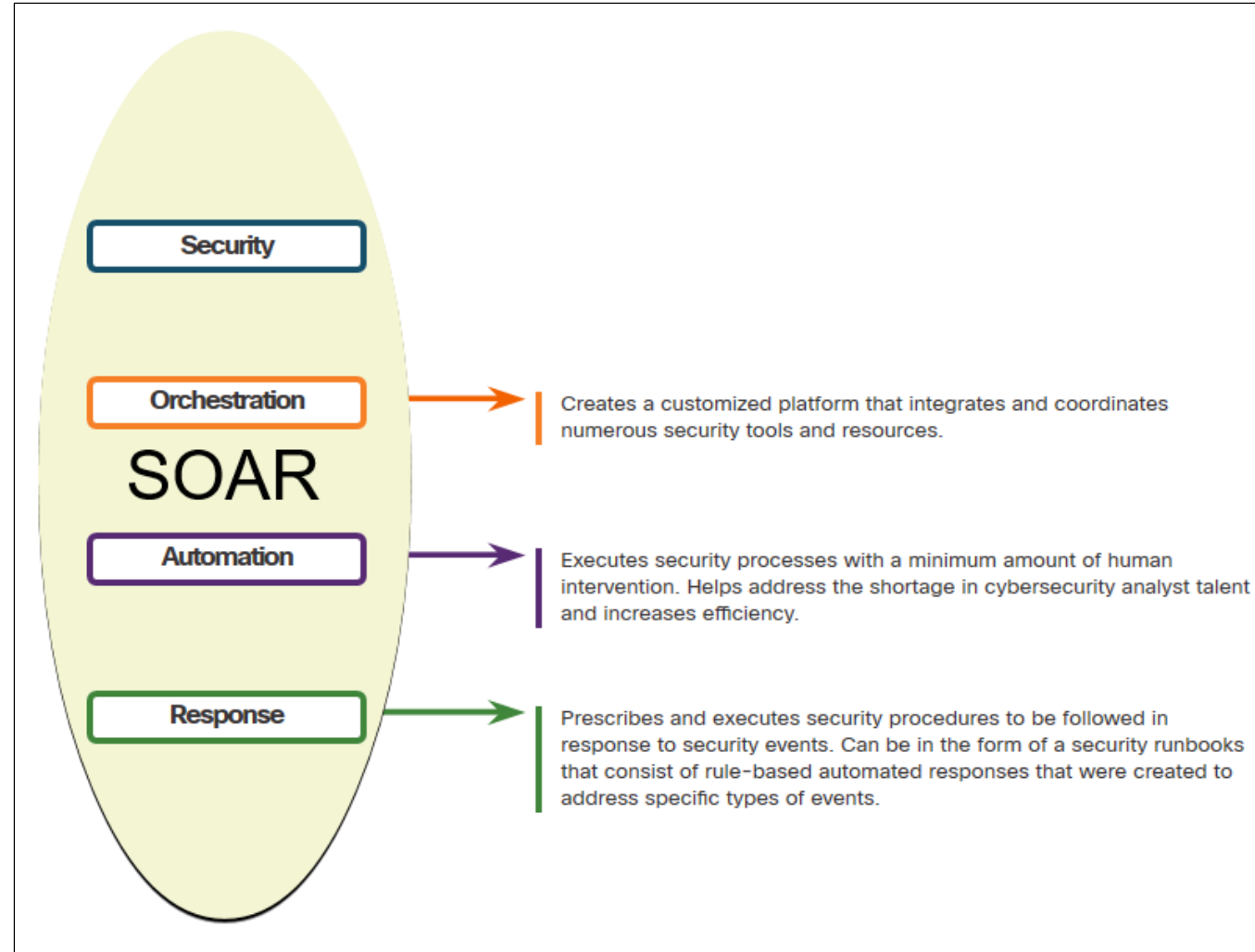
Technologies in the SOC: SIEM

- An SOC needs a Security Information and Event Management (SIEM) system to understand the data that firewalls, network appliances, intrusion detection systems, and other devices generate.
- SIEM systems collect and filter data, and detect, classify, analyze and investigate threats. They may also manage resources to implement preventive measures and address future threats.



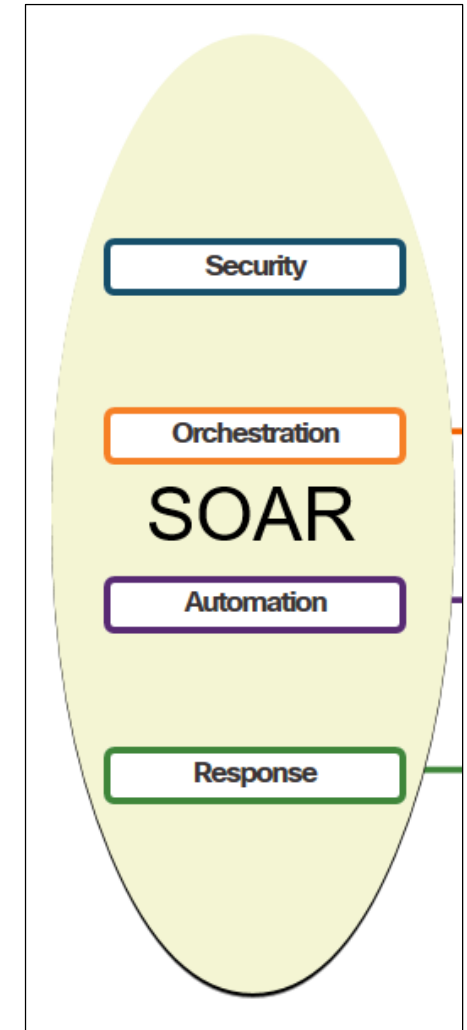
Technologies in the SOC: SOAR

- **SIEM** and Security Orchestration, Automation and Response (**SOAR**) are often paired together as they have capabilities that **complement each other**.
- Large security operations (SecOps) teams use both technologies to optimize their SOC.
- SOAR platforms are similar to SIEMs as they aggregate, correlate, and analyze alerts. In addition, SOAR technology **integrate threat intelligence** and **automate incident investigation** and **response** workflows based on **playbooks** developed by the security team.



Technologies in the SOC: SOAR (Contd.)

- SOAR security platforms:
 - **Gather alarm data** from each component of the system.
 - Provide **tools** that enable cases to be **researched, assessed, and investigated**.
 - Emphasize integration as a means of automating **complex incident response workflows** that enable more rapid response and adaptive defense strategies.
 - Include pre-defined playbooks that enable automatic response to specific threats. **Playbooks** can be **initiated automatically** based on **predefined rules** or may be triggered **by security personnel**.



Fighters in the War Against Cybercrime

SOC Metrics

- Whether internal to an organization or providing services to multiple organizations, it is important to understand how well the SOC is functioning, so that improvements can be made to the people, processes, and technologies that comprise the SOC.
- Many metrics or **Key Performance Indicators (KPI)** can be devised to measure different aspects of **SOC performance**. However, **five metrics are commonly used** as SOC metrics by SOC managers.

Metrics	Definition
Dwell Time	The length of time that threat actors have access to a network before they are detected, and their access is stopped
Mean Time to Detect (MTTD)	The average time that it takes for the SOC personnel to identify valid security incidents have occurred in the network
Mean Time to Respond (MTTR)	The average time it takes to stop and remediate a security incident
Mean Time to Contain (MTTC)	The time required to stop the incident from causing further damage to systems or data
Time to Control	The time required to stop the spread of malware in the network

Enterprise and Managed Security

- For medium and large networks, the organization will benefit from implementing an enterprise-level SOC, which is a complete **in-house solution**.
- Larger organizations may **outsource at least a part of the SOC operations** to a security solutions provider.
- Cisco offers a wide range of incident response, preparedness, and management capabilities including:
 - Cisco Smart Net Total Care Service for Rapid Problem Resolution
 - Cisco Product Security Incident Response Team (PSIRT)
 - Cisco Computer Security Incident Response Team (CSIRT)
 - Cisco Managed Services
 - Cisco Tactical Operations (TacOps)
 - Cisco's Safety and Physical Security Program

Fighters in the War Against Cybercrime

Security vs. Availability

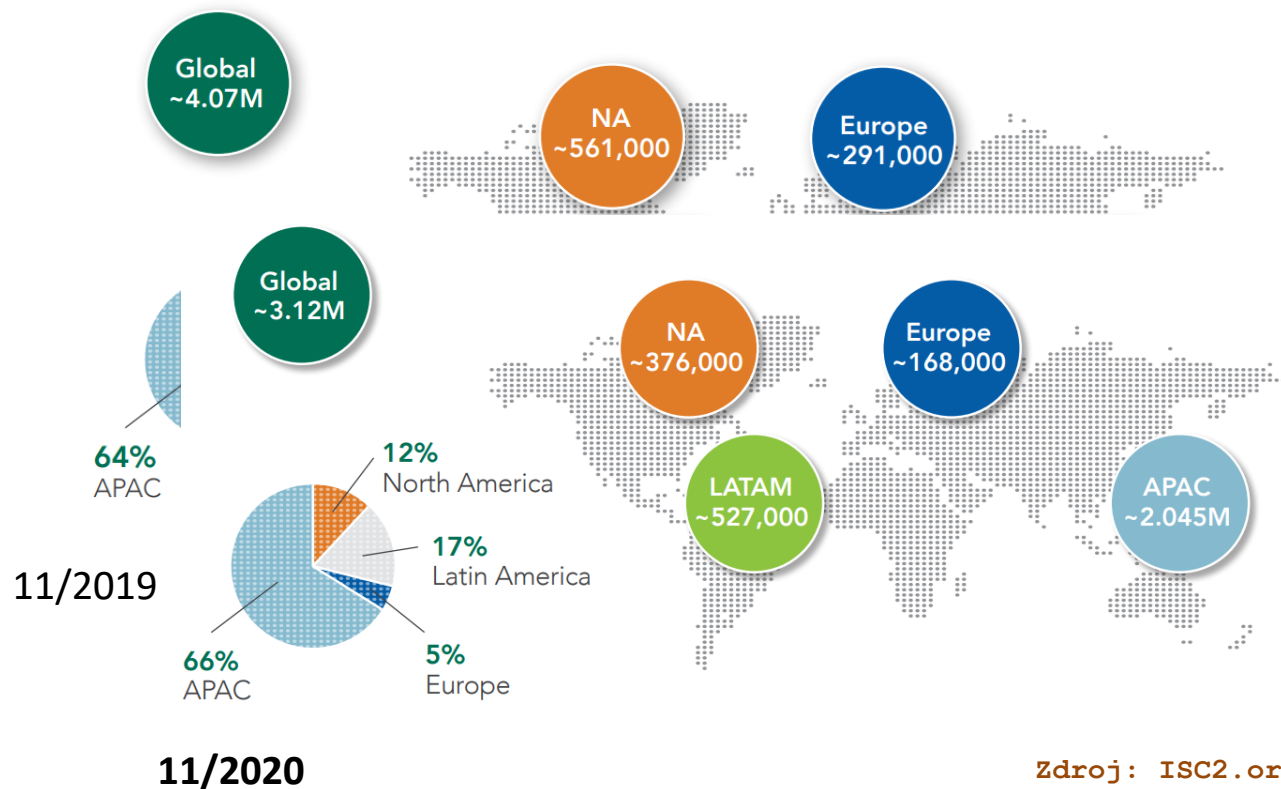
- Security personnel understand that for the organization to accomplish its priorities, network availability must be preserved.
- Each business or industry has a limited tolerance for network downtime. That tolerance is usually based upon a comparison of the cost of the downtime in relation to the cost of ensuring against downtime.
- Security cannot be so strong that it interferes with the needs of employees or business functions. It is always a tradeoff between strong security and permitting efficient business functioning.



2.2 Becoming a Defender

Počty neobsadených miest odborníkov na bezpečnosť

The Cybersecurity Workforce Gap by Region



<https://www.isc2.org/Research/Workforce-Study>

Motivácia ku KB

- Téma KB sa týka **každého**
- Každý je **zodpovedný** za svoje dáta
 - Aj **osobné údaje** sú dáta a treba ich chrániť



Pravdepodobne by sme mohli tento rok vyskúšať iný prístup ku kybernetickej bezpečnosti

Becoming a Defender

Motivácia

The Most Important Qualifications for Cybersecurity Professionals (Non-technical Skills and Attributes)



38%

Strong problem-solving abilities



32%

Curiosity and eagerness to learn



32%

Strong communication skills



23%

Strong strategic thinking skills

Becoming a Defender

Motivácia

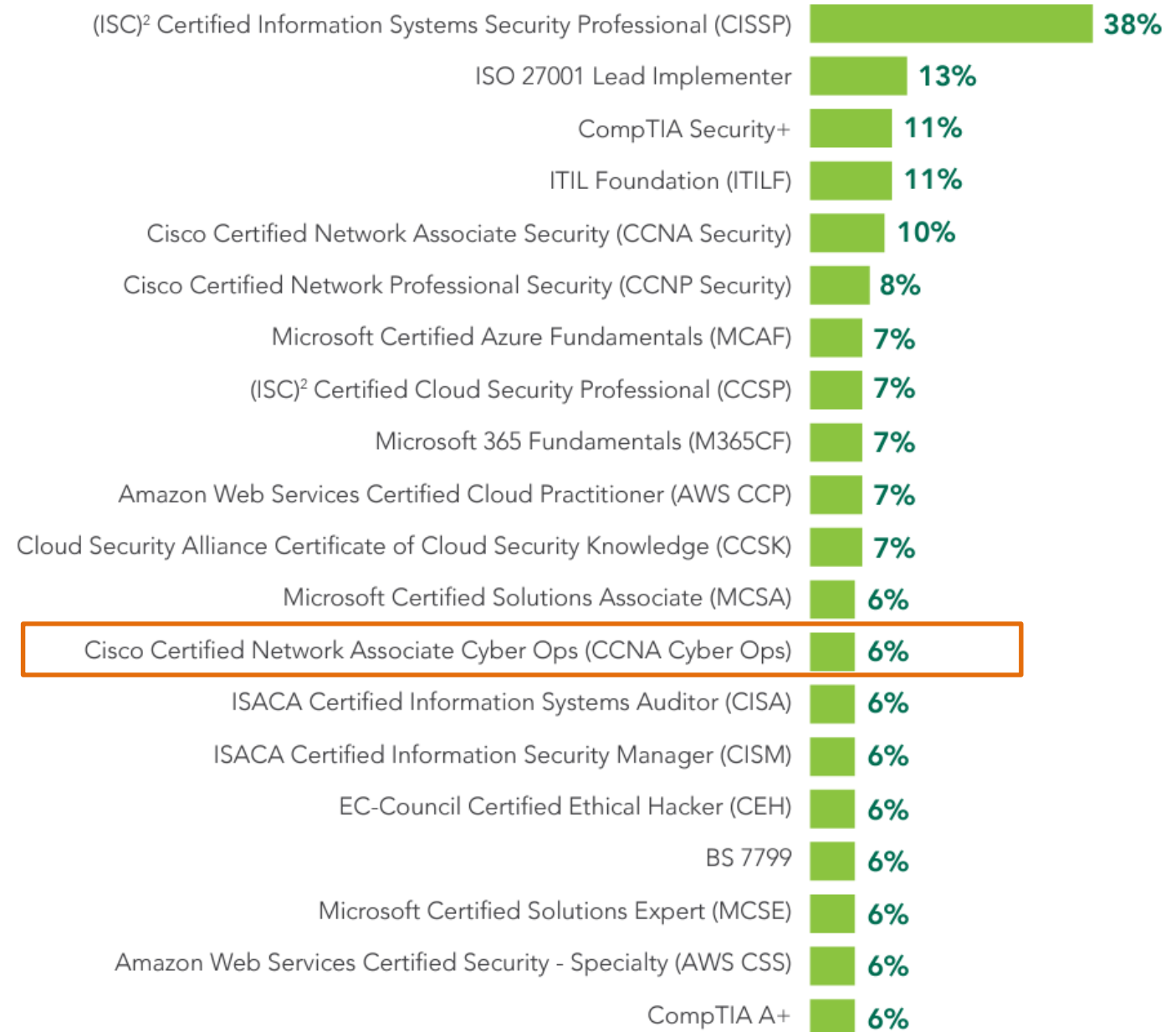
Top Attributes Sought in Cybersecurity Personnel



Becoming a Defender

Motivácia

Most Commonly Held Certifications and Certificates



Becoming a Defender

Certifications

- A variety of cybersecurity certifications that are relevant to careers in SOCs are available:
 - Cisco Certified CyberOps Associate
 - CompTIA Cybersecurity Analyst Certification
 - (ISC)² Information Security Certifications
 - Global Information Assurance Certification (GIAC)
- Search for “cybersecurity certifications” on the Internet to know more about other vendor and vendor-neutral certifications.



Becoming a Defender

Further Education

- **Degrees:** When considering a career in the cybersecurity field, one should seriously consider pursuing a technical degree or bachelor's degree in computer science, electrical engineering, information technology, or information security.
- **Python Programming:** Computer programming is an essential skill for anyone who wishes to pursue a career in cybersecurity. If you have never learned how to program, then Python might be the first language to learn.
- **Linux Skills:** Linux is widely used in SOCs and other networking and security environments. Linux skills are a valuable addition to your skillset as you work to develop a career in cybersecurity.



Becoming a Defender

Sources of Career Information

- A variety of websites and mobile applications advertise information technology jobs. Each site targets a variety of job applicants and provides different tools for candidates to research their ideal job position.
- Many sites are job site aggregators that gather listings from other job boards and company career sites and display them in a single location.
 - Indeed.com
 - CareerBuilder.com
 - USAJobs.gov
 - Glassdoor
 - LinkedIn
 - Profesia.sk



Becoming a Defender

Getting Experience

- **Internships:** Internships are an excellent method for entering the cybersecurity field. Sometimes, internships turn into an offer of full time employment. However, even a temporary internship allows you the opportunity to gain experience in the inner workings of a cybersecurity organization
- **Scholarships and Awards:** To help close the security skills gap, organizations like Cisco and INFOSEC have introduced scholarship and awards programs.
- **Temporary Agencies:** Many organizations use temporary agencies to fill job openings for the first 90 days. If the employee is a good match, the organization may convert the employee to a full-time, permanent position.
- **Your First Job:** If you have no experience in the cybersecurity field, working for a call center or support desk may be your first step into gaining the experience you need to move ahead in your career.



2.3 Fighters in the War Against Cybercrime Summary

Fighters in the War Against Cybercrime Summary

What Did I Learn in this Module?

- Major elements of the SOC include people, processes, and technologies.
- The job roles include a Tier 1 Alert Analyst, a Tier 2 Incident Responder, a Tier 3 Threat hunter, and an SOC Manager.
- A Tier 1 Analyst monitors incidents, open tickets, and performs basic threat mitigation.
- SEIM systems are used for collecting and filtering data, detecting and classifying threats, and analyzing and investigating threats.
- SOAR integrates threat intelligence and automates incident investigation and response workflows based on playbooks developed by the security team.
- KPIs are devised to measure different aspects of SOC performance. Common metrics include Dwell Time, Meant Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Contain (MTTC), and Time to Control.



What Did I Learn in this Module? (Contd.)

- There must be a balance between security and availability of the networks. Security cannot be so strong that it interferes with employees or business functions.
- A variety of cybersecurity certifications that are relevant to careers in SOCs are available from different organizations.





UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Ďakujem za pozornosť

Obsahom boli moduly:

Module 1 The Danger

Module 2 Fighters in the War Against Cybercrime

Vyjadrite spätnú väzbu na prednášku a/alebo cvičenie v anonymnej ankete cez google form: [link](#)

Dorobit' zvyšok z ineho videa...

