

Kako raditi uz kibernetičke napade?

dr.sc. Ante Žigman
Predsjednik Upravnog vijeća

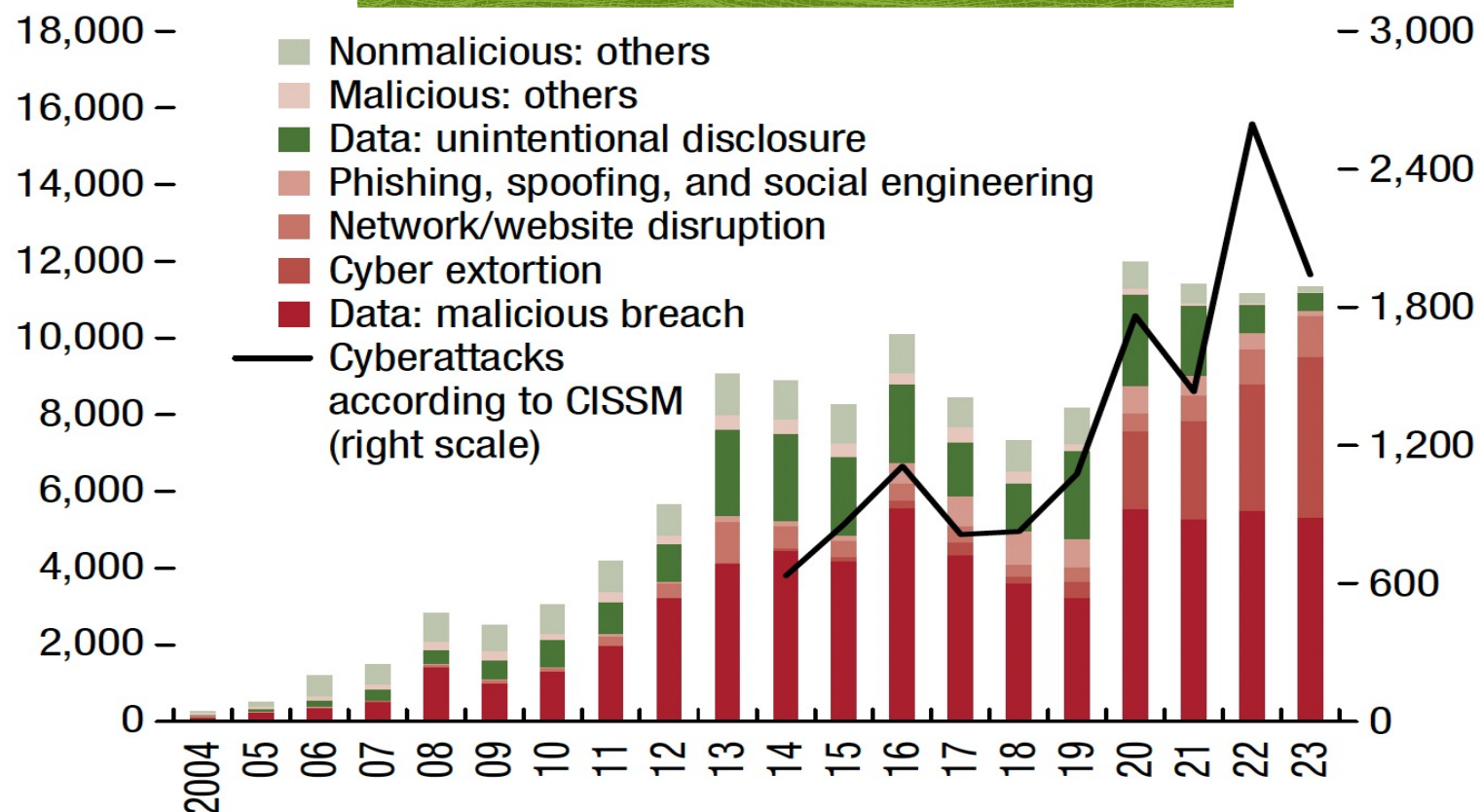
25.11.2024.

BROJ CYBER INCIDENATA GLOBALNO 2004.-2023.

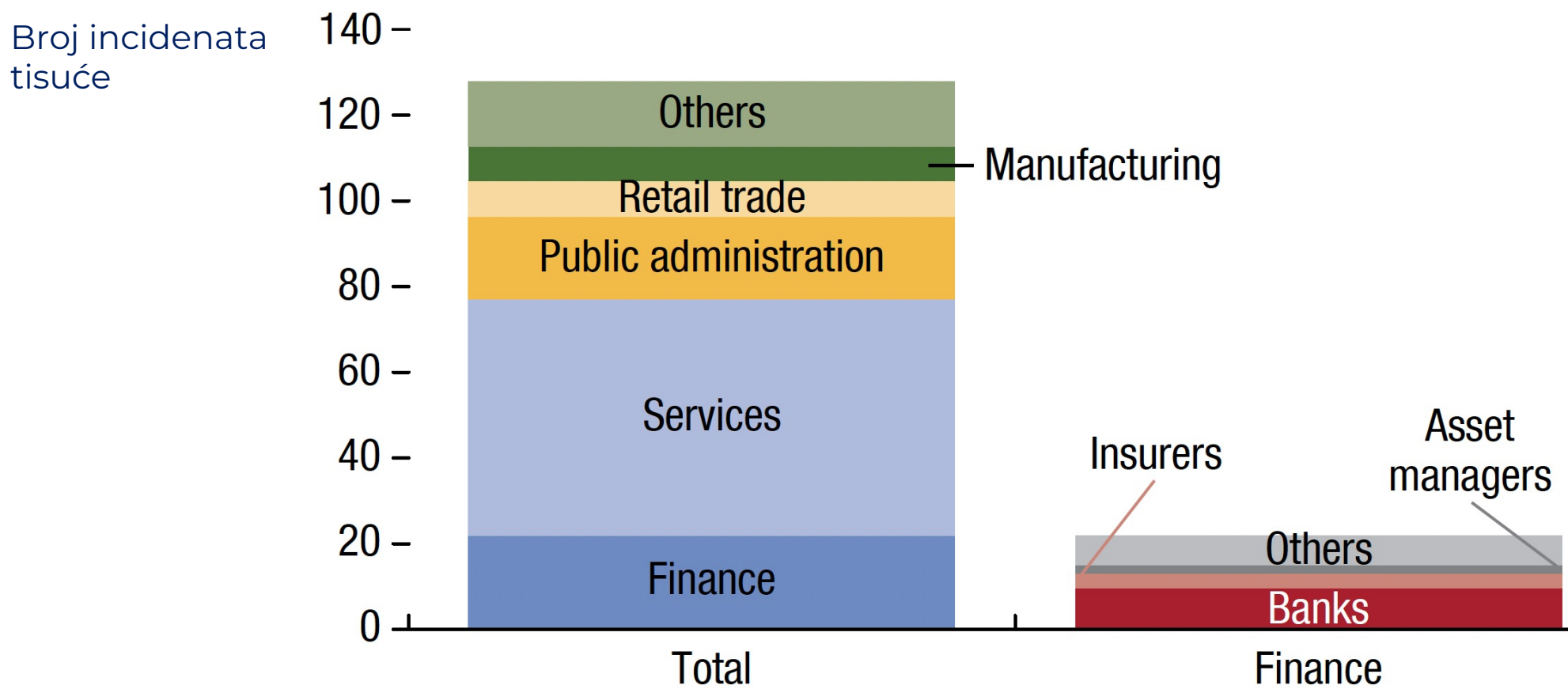
Broj
incidenata



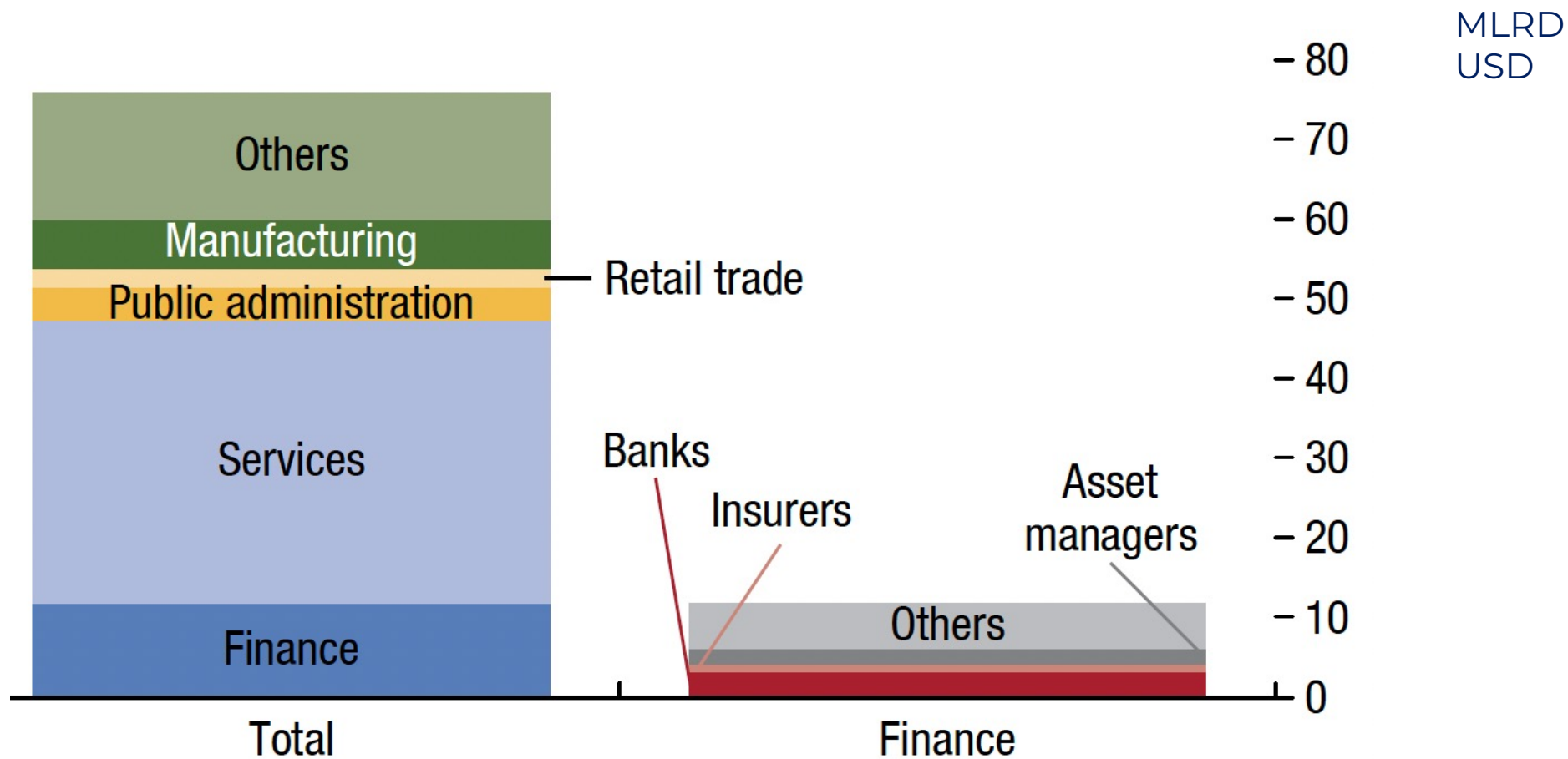
Broj cyber
NAPADA



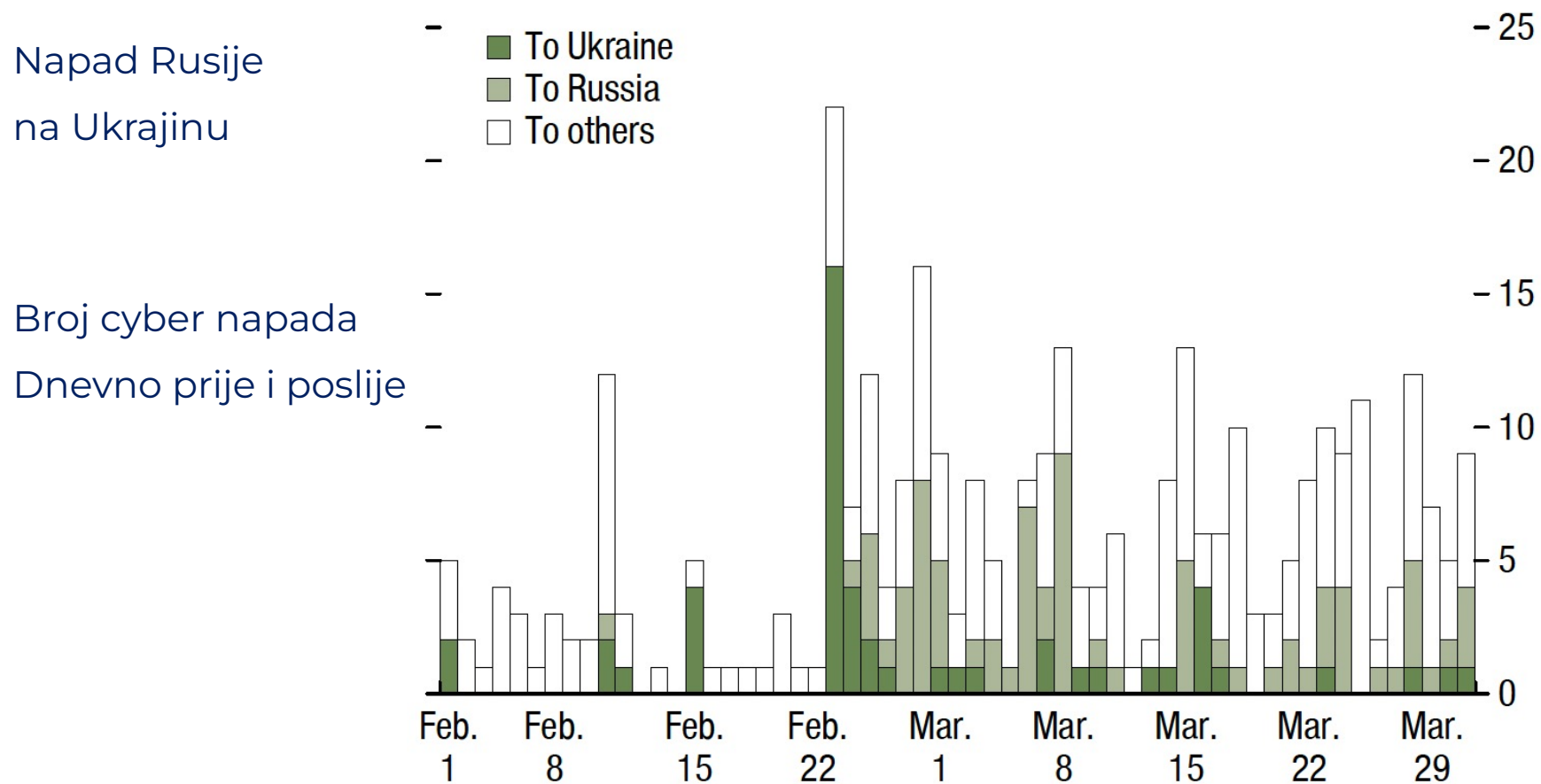
UKUPNO CYBER INCIDENTI GLOBALNO 2004.-2023.



GUBICI – CYBER INCIDENTI GLOBALNO 2004.-2023.



GEOPOLITIČKI ODNOSI I CYBER NAPADI



MMF IZVJEŠĆE, travanj 2024. (poglavlje 3)

- Broj kibernetičkih napada je gotovo dvostruko veći u odnosu na razdoblje prije COVID-19
- Financijski sektor visoko izložen kibernetičkim rizicima – približno 20% svih napada
- Do sada kibernetički incidenti nisu bili systemske razine ali rizik postoji
- Poremećaj u radu kritičnih sustava može dovesti do većeg incidenta zbog visoke razine povezanosti i međuovisnosti
- Nova regulativa EU kao i nacionalne razine (DORA, NIS2) će značajno unaprijediti stabilnost i umanjiti učestalost incidenata



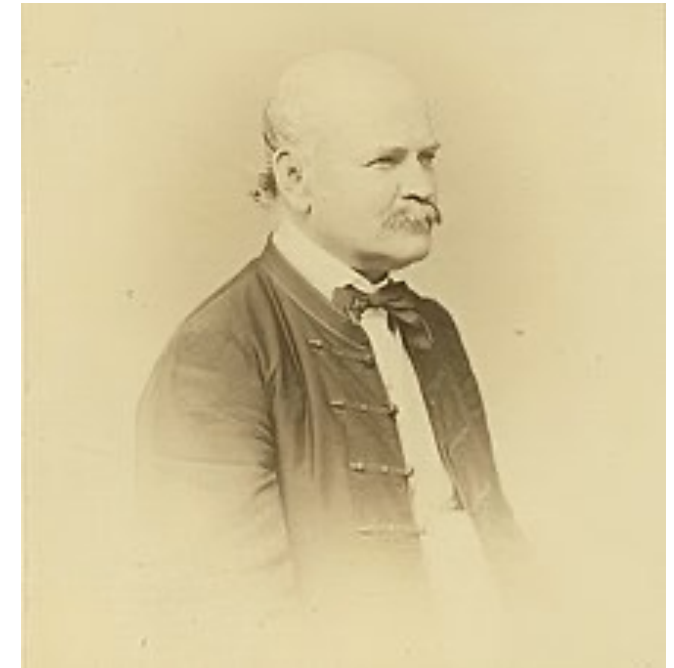
CYBER HIGIJENA – NOVA ETAPA DRUŠTVENOG RAZVOJA

- Liječnik u Općoj bolnici u Beču
- Empirijski otkrio da se infekcije mogu značajno smanjiti mjerama HIGIJENE

pranje ruku otopinom klora i limete

- Smrtnost roditelja na jednom odjelu se smanjila s 18% na 2 %
- Objavio je 1861. knjigu o svojim saznanjima, ali ga je znanstvena javnost odbila
- Louis Pasteur je dokazao teoriju mikroba godinama kasnije i potvrdio teoretski Semmelweisova opažanja i tvrdnje

Ignaz Philipp Semmelweis
(1818 –1865)



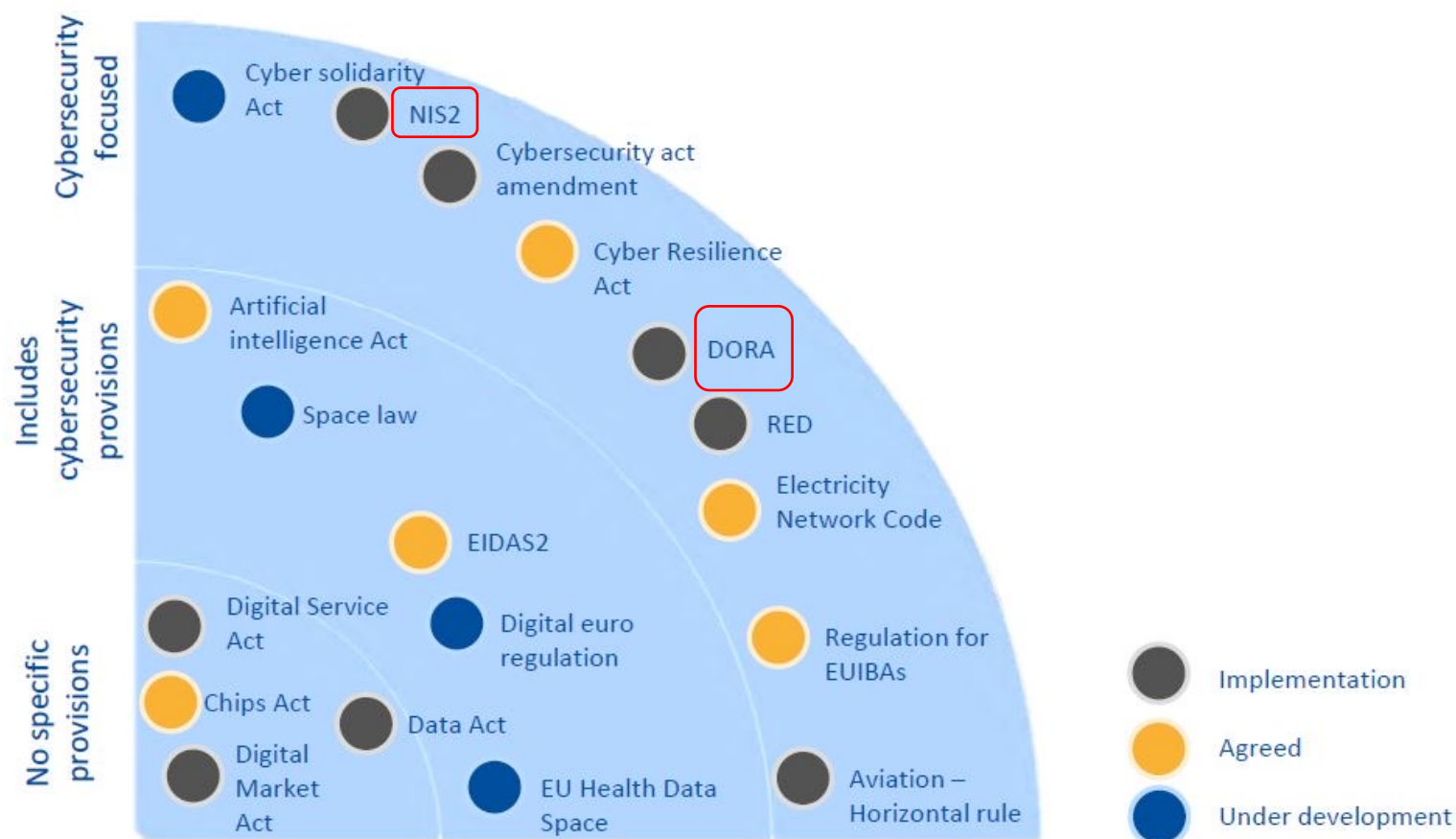
PREPORUKE: CYBER HIGIJENA

- Ne koristiti NA VIŠE MJESTA iste lozinke
- Lozinke: dugačke i složene, slučajni niz
- Pristup – **VIŠESTRUKA PROVJERA** (Multifactor Authentication)
- Provjere – redovne i neovisne: tehničke, procesne i organizacijske
- Ojačavanje – ciljano podešavanje sustava (Security Hardening)
- Threat Intelligence – pratite jeste li aktivna meta (vaša procjena rizika)

TEMELJNI ZAHTJEVI NOVE REGULATIVE: DORA I NIS2/ZKS

- Odgovor na visoku razinu ovisnosti suvremenog društva o digitalnoj tehnologiji i temelj za daljnji razvoj EU
- Organizacijski pristup kontinuitetu upravljanja kibernetičkom sigurnošću i spremnost za daljnji razvoj; Fintech, AI
- Razvoj kulture upravljanja rizikom kibernetičke sigurnosti

EU REGULATIVA – ZNAČAJAN SEGMENT KIBERNETIČKE SIGURNOSTI



* ENISA: WK 10244/2024 INIT, 17. srpnja 2024.

DORA : POČETAK U 2020.

- 24 rujna 2020. Europska komisija objavila je prvi draft Digital Operational Resilience Act (DORA).
- Zakonski tekst nadograđuje postojeće zahtjeve upravljanja IKT rizicima koje su već razvile pojedine EU institucije i povezuje niz inicijativa u jednu Uredbu
- DORA u 2025. uspostavlja znatno čvršću osnovu za EU nadzorna i regulatorna tijela, omogućuje proširenje fokusa nadzora financijskih institucija
- Do sada: financijska stabilnost i zaštita potrošača
- **Od 2025 : podizanje sposobnosti financijskih institucija da održe visoku razinu otpornosti u poslovanju uslijed cyber napada**

NIS2 : ISTODOBNO ZA DRUGE SEKTORE

POVIJEST ANALIZE SIGURNOSTI I DRUŠTVENI ODGOVOR

- 1995. dva programera objavila su alat za provjeru sigurnosti S.A.T.A.N.
- Alat je objavljen u časopisu PC Magazine i bio je BESPLATAN
- Ministarstvo pravosuđa SAD je zaprijetilo da povuku alat iz distribucije
- Razlog : alat se može koristiti za napade na mreže i sustave



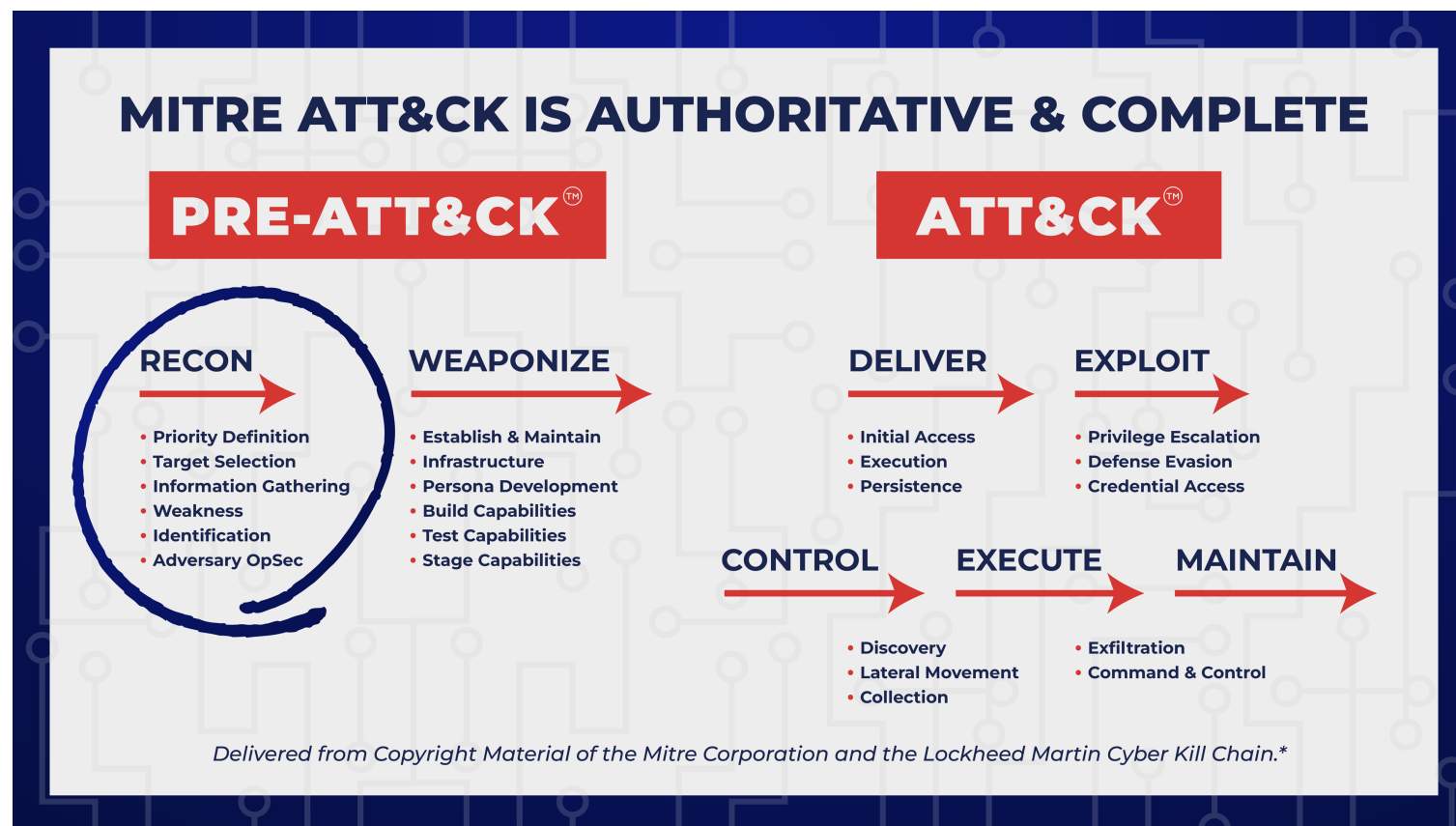
(Security Administrator Tool for Analyzing Networks)

ALATI DANAS – SUSTAVNO DOSTUPNI

MITRE ATT&CK®													
Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog 🔗 Search 🔍													
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Data Manipulation (3)	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Financial Theft
Search Open Websites/Domains (3)	Trusted Relationship	Valid Accounts (4)	Serverless Execution	Event Triggered Execution (17)	Escape to Host	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (5)	Hide Infrastructure	Exfiltration Over Web Service (4)	Firmware Corruption
Search Victim-Owned Websites	Valid Accounts (4)	Shared Modules	Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Inhibit System Recovery
	System Services (2)	Hijack Execution Flow (13)	System Services (2)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Hide Artifacts (12)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Resource Hijacking (4)
	User Execution (3)	Implant Internal Image	User Execution (3)	Implant Internal Image	Hijack Execution Flow (13)	Hijack Execution Flow (13)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol	System Shutdown/Reboot	Service Stop
	Windows Management Instrumentation	Modify Authentication Process (9)	Windows Management Instrumentation	Modify Authentication Process (9)	Process Injection (12)	Impersonation	Steal Application Access Token	Group Policy Discovery		Data from Removable Media	Non-Standard Port		System Shutdown/Reboot
		Office Application Startup (6)	Office Application Startup (6)	Office Application Startup (6)	Scheduled Task/Job (5)	Indicator Removal (10)	Steal or Forge Authentication Certificates	Log Enumeration		Data from Removable Media	Protocol Tunneling		
		Power Settings	Power Settings	Power Settings	Valid Accounts (4)	Indirect Command Execution	Steal or Forge Kerberos Tickets (5)	Log Enumeration		Data from Removable Media	Proxys (4)		
		Pre-OS Boot (5)	Pre-OS Boot (5)	Pre-OS Boot (5)	Valid Accounts (4)	Masquerading (10)	Steal Web Session Cookie	Log Enumeration		Data from Removable Media	Remote Access Software		
		Scheduled Task/Job (5)	Scheduled Task/Job (5)	Scheduled Task/Job (5)	Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media	Traffic Signaling (2)		
		Server Software Component (5)	Server Software Component (5)	Server Software Component (5)	Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media	Web Service (3)		
		Traffic Signaling (2)	Traffic Signaling (2)	Traffic Signaling (2)	Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts (4)	Masquerading (10)	Unsecured Credentials (8)	Log Enumeration		Data from Removable Media			
					Valid Accounts								

ANALIZA - JASNO SE RAZLIKUJU FAZE NAPADA

Lockheed Martin postavio je analizu koja se danas koristi u MITRE ATT&CK* okviru



Napad uvijek počinje **izviđanjem**

kako izgledate na mreži kakve **ranjivosti** imate

gdje mjere nedostaju

IZVIĐANJE (JOŠ PRIMJERA)

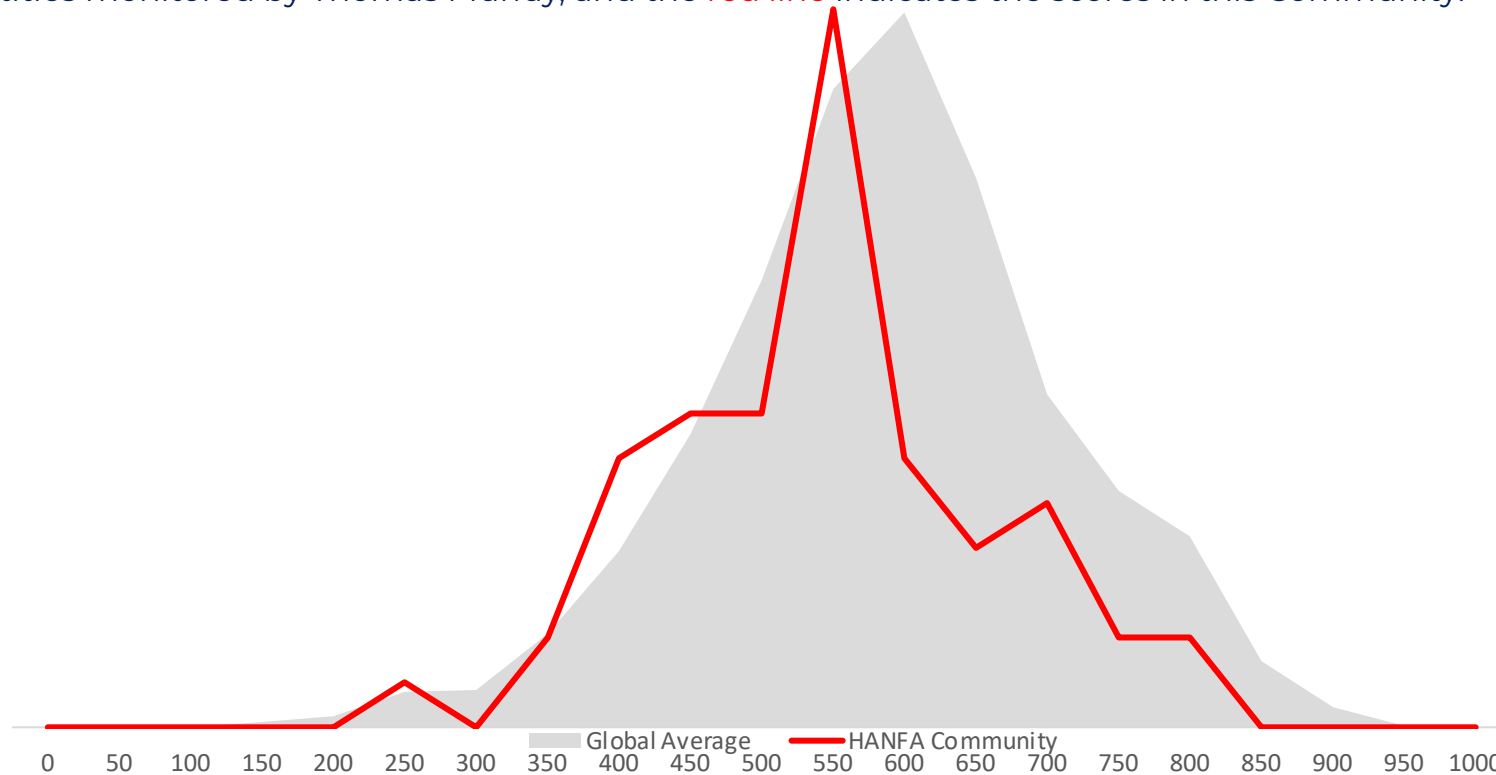
HANFA je angažirala „etičke hakere” da obave izviđanje

Thomas Murray Cyber(UK) obavio je izviđanje SVIH subjekata nadzora Hanfe

- Neinvazivno skeniranje dostupnih sustava na internetu
- Analiza otkrivenih slabosti, ranjivosti koje omogućuju prodor
- Provjera dostupnih informacija na „dark webu”
- Usporedba ukupnog profila rizičnosti s drugim subjektima
- Ne objavljujemo podatke tvrtki
- Pojedinačni podaci su dostupni za daljnju analizu

SCAN: OCTOBER SECURITY SCORES

The distribution shows the number of companies at each Orbit Risk score level. The **filled area** represents the Global distribution of scores across all entities monitored by Thomas Murray, and the **red line** indicates the scores in this Community.



Key takeaways:

- Some entities in the HANFA community fall below a score of 500.
- A few entities score less than 400.

HANFA Average	566
Global average	611

HIGH RISK ISSUES

XX

Open Service

Services likely to not be purposely exposed

XX

Vulnerable Service

Services out of date and may require patching

XX

Compromised Server

Servers may be port-scanning or part of a botnet – **Further investigation required**

XX

Stolen Credentials

Stolen credentials may highlight password re-use and could be used for initial access

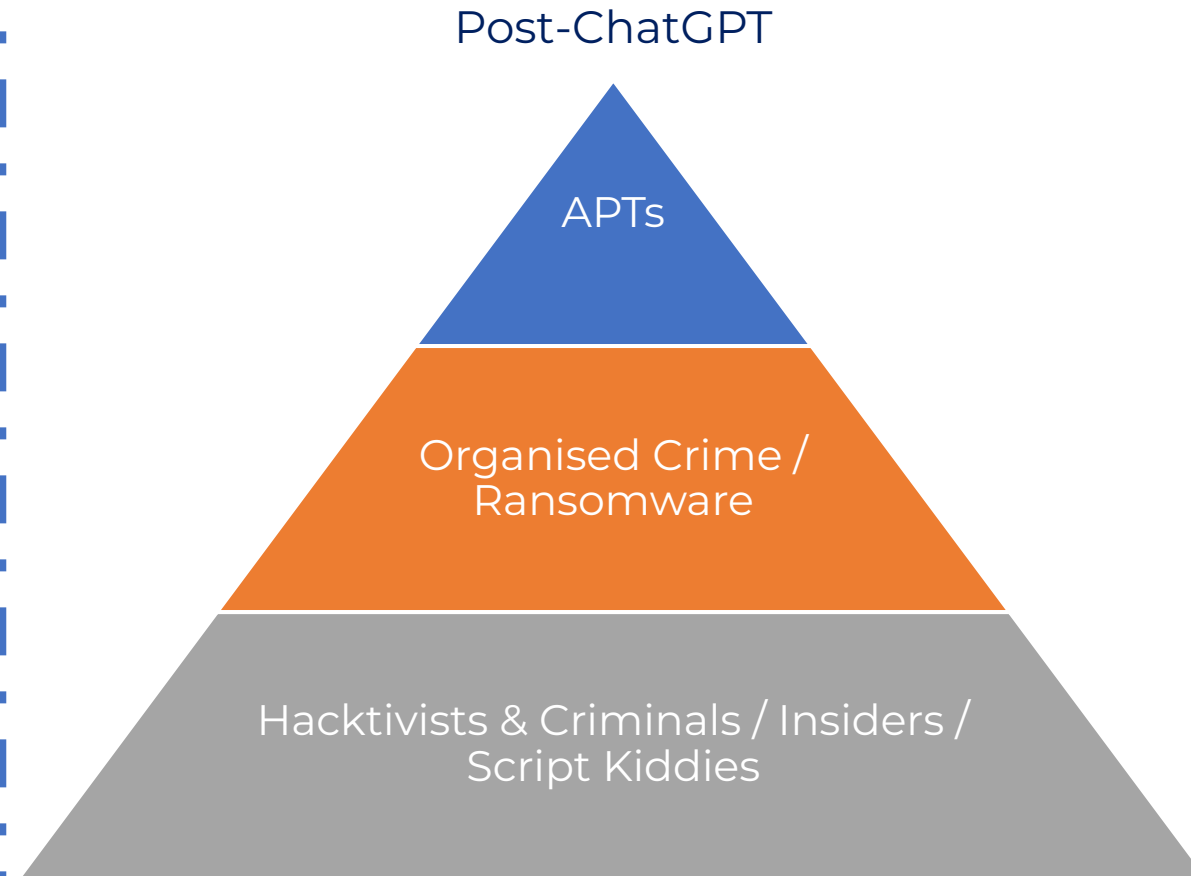
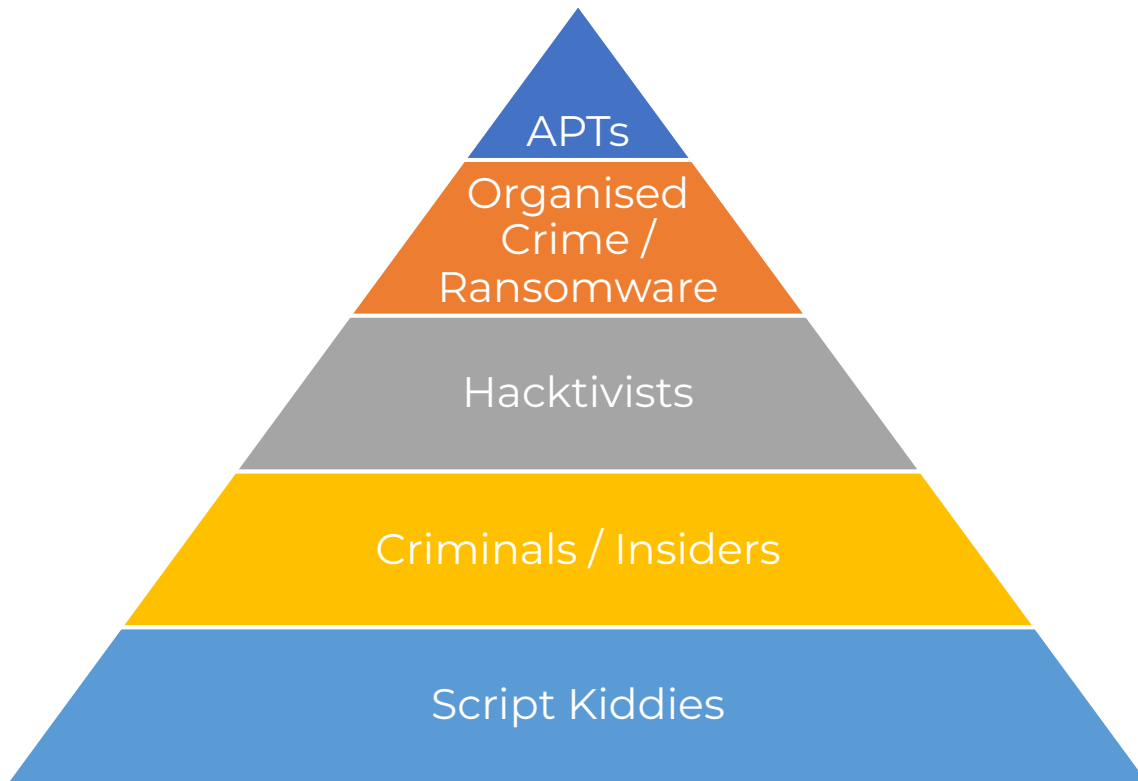
XX

Breached Emails

Emails identified in data dumps

Orbit Security Analysis

NAPADAČI PO VRSTAMA



KAKO BITI SIGURAN I POSLOVATI

- Učinimo sve što je moguće
- Dosegnimo sigurnost!



NAŠ NOVI MINDSET – *ASSUME BREACH*

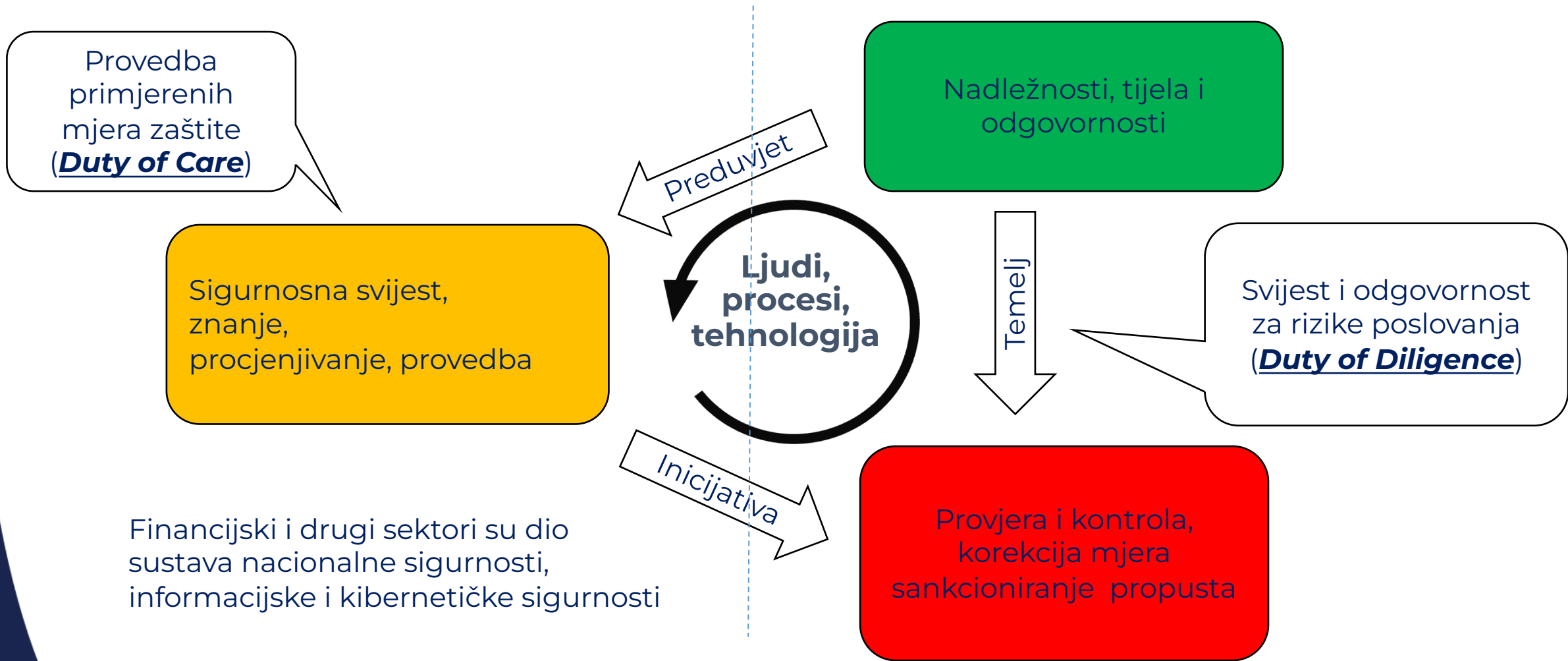
Analize i iskustvo nas uči da se incidenti ne mogu izbjeći

Jedino što nam preostaje je priprema, jer tada upravljamo incidentima

Hanfa je u listopadu 2024. provela vježbu odgovora na kibernetičke incidente s 11 društava te izvijestila tržište

Incidenti će se događati – potrebno je pripremiti se da utjecaj bude manji

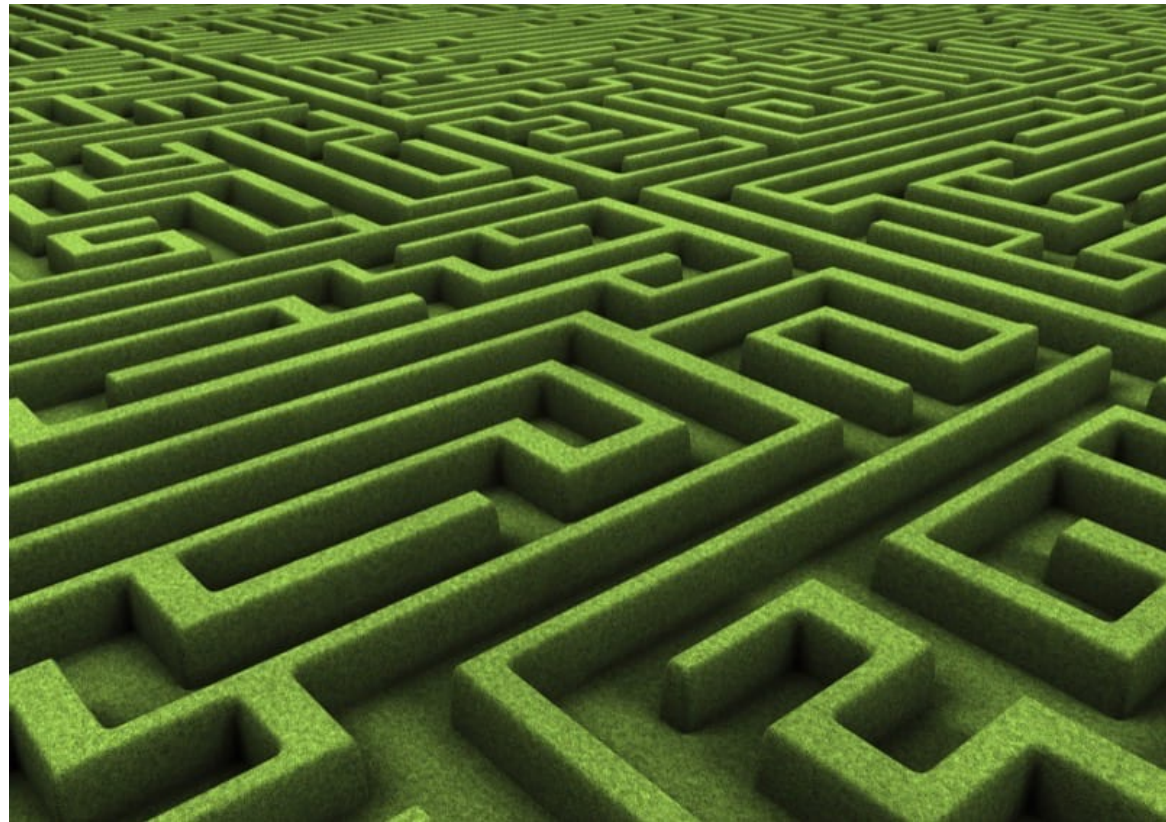
KAKO NAM KORISTI REGULATIVA*



* SOA; Sk@ut konferencija 2024.

KAKO RADITI...

- Koliko prepreka imate?
- Jesu li složene i zahtjevne?
- Običan napadač će uvijek izabrati lakši put
- Šansa je da će umjesto vas napasti nekog drugog





HVALA NA POZORNOSTI!