
eset
SECURITY
DAYS
headtechnology
it · security · distribution · services
YOUR TRUSTED
DISTRIBUTOR OF IT SECURITY
SOLUTIONS & SERVICES

headtechnology
it · security · distribution · services

Speaker – Andris Soroka

20+ years in IT, 15+ years in IT Security

Founder of largest vendor independent conferences in Baltics (Digital Era, DSS ITSEC)

Speaker in many international conferences

Member of ECSO, ENISA Awareness Raising Community, Latvian IT Association etc.

Worked as vendor, integrator, reseller, distributo

Organized Latvia's 1st external export / trade mission with national expo stand at Infosecurity Europe

headtechnology
it · security · distribution · services

Latest events

Infosecurity Europe 2022 (London, UK)

Cybersecurity Forum 2022 (Katowice, Poland)

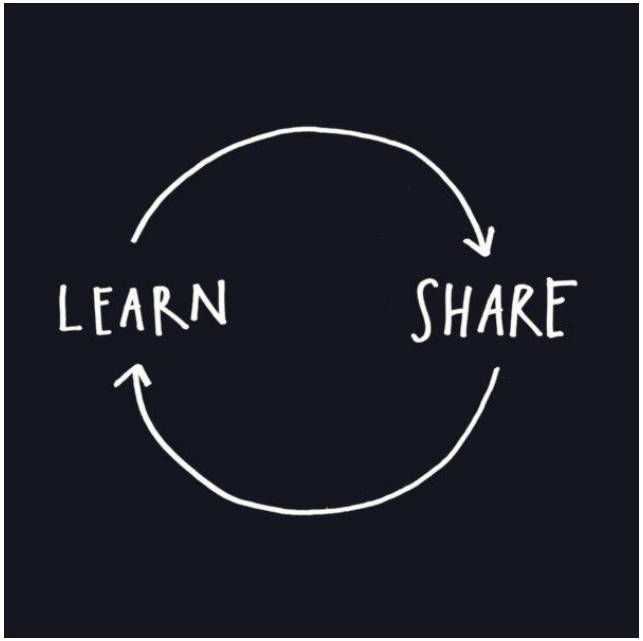
Moldova road to EU conference 2022 (virtual)

Ukraine CSO&CISO forum 2022 (October, Kiiv)

RSA Conference 2023 (San Francisco, USA)

ThinkIn 2023 (Copenhagen, Denmark)

PenteraCon 2023 (Munich, Germany)



LV ES Digitālā nedēļa 2023 & many more partner events accross EU

CyberWeek 2023 (TelAviv, Israel)

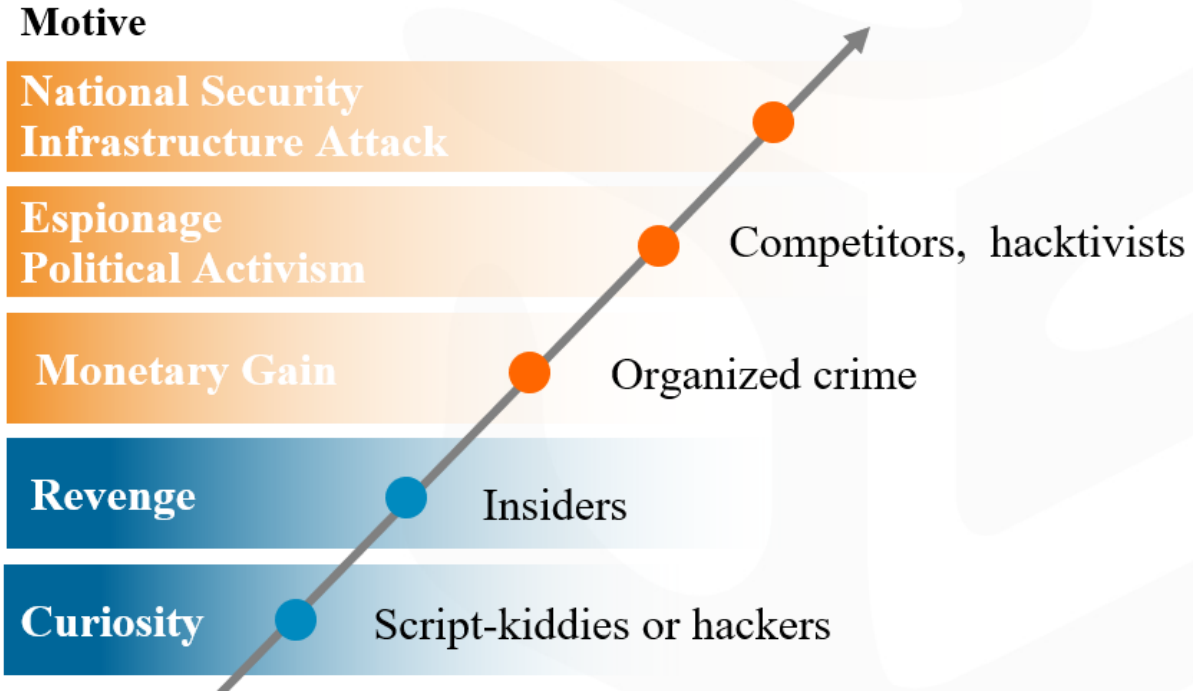
headtechnology
it · security · distribution · services

Where are we now?

We are up against 3 sophisticated adversaries

More than 90% of attacks are financially motivated

Source: Verizon DBIR 2021



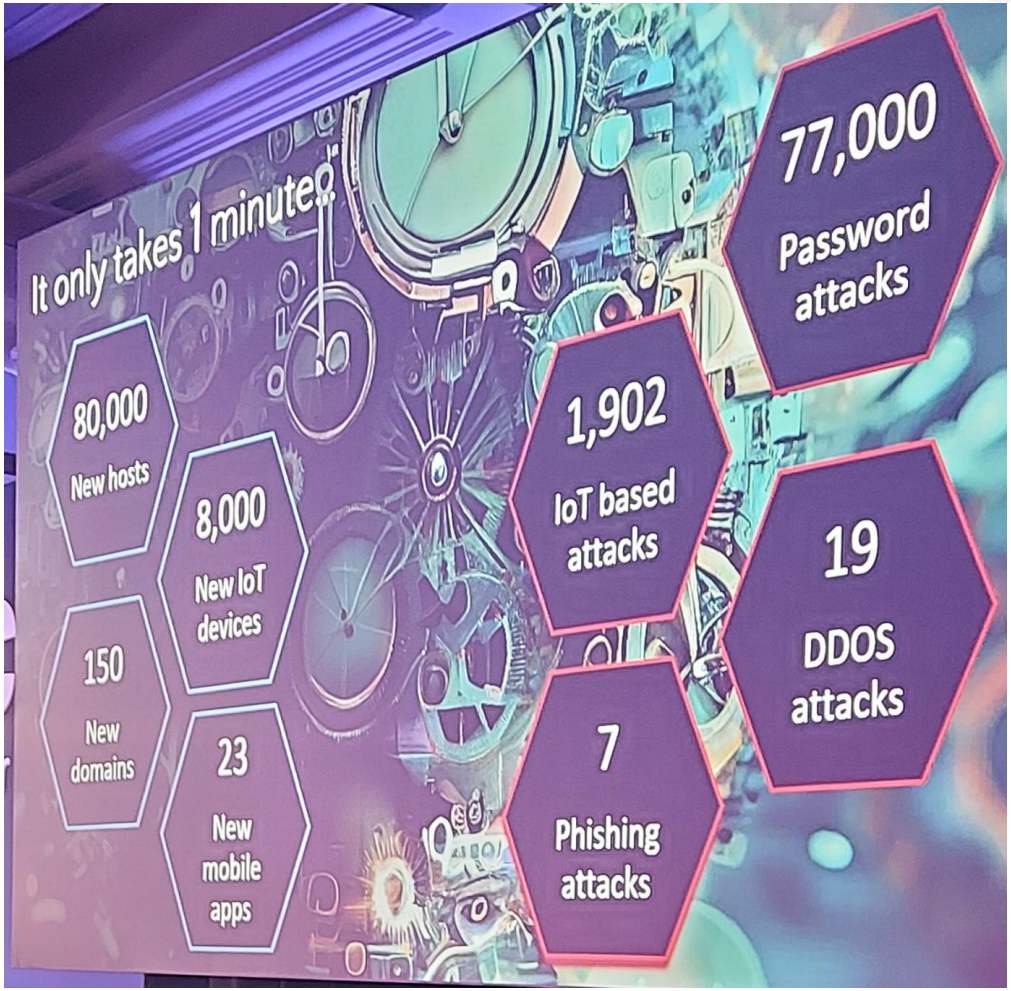
headtechnology
it · security · distribution · services

Reality check

- 90%+ are automated attacks
- 8 trillions total economy «worth» (G7 top3)
- 85%+ of incidents involve human factor
- 61% of attacks involved valid credentials
- Microsoft reports that 80% of Azure users havent activated MFA..
- 65%+ victims notified by external parties

- More than a half of incidents are detected days, weeks, months, years after event...

- IF DETECTED AT ALL!

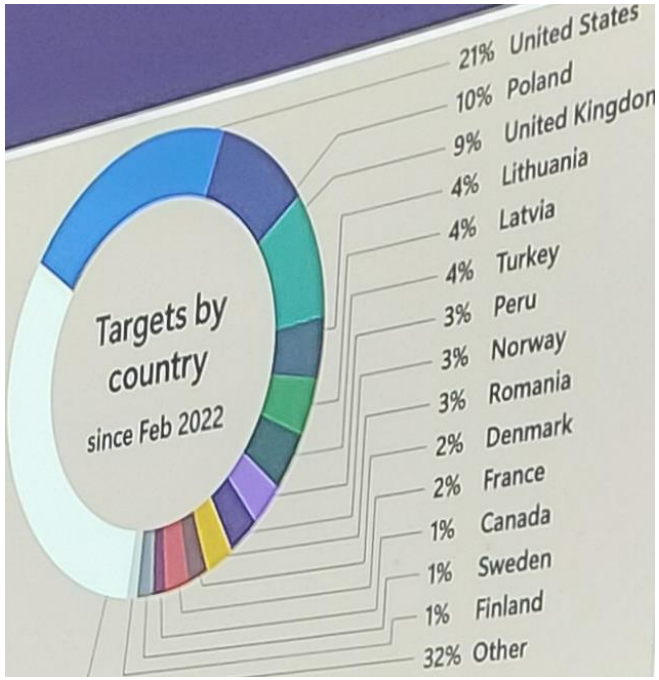


headtechnology
it · security · distribution · services

Reality check ..

- Continous cyberwar (Ukraine and geopolitics)
- Cybercrime as a Service (financial motivation) & Darknet/Deepweb business (KPI's, sales, marketing etc.)
- Business Email compromise - phishing, fraud, scam, spam (payroll, invoice, attachements etc., ~156000 per day, 1h 12minutes to become a victim..)
- Denial of Service Attacks (push bombing too)
- Sophisticated targeted attacks (kill chain etc.)
- Botnets, bots, zombies
- AI (80%+ of all attacks are AI driven)
- IoT/OT (in)security & attacks on everything «smart»
- Critical infrastructure
- Intelectual Property Theft
- Personal (any) data issues & reputation attacks

This had got nothing to do with size of country,region, enterprise, private or public person, organization, industry.



headtechnology
it · security · distribution · services

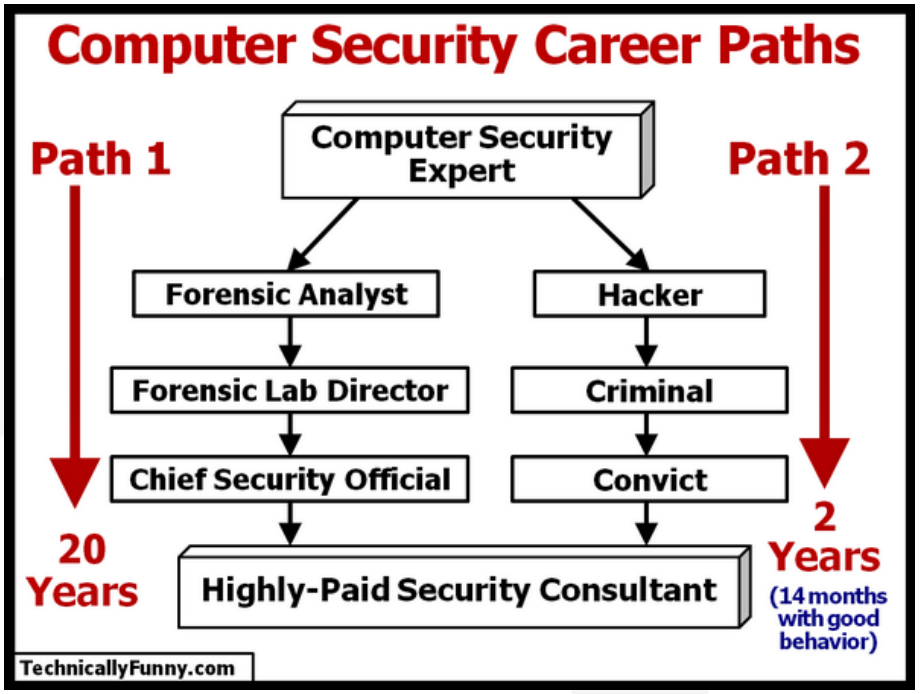
corporate
presentation

headtechnology
it · security · distribution · services

Goal and measures

- We don’t want to be vulnerable, we dont want to be at risk.
- How do we measure that today? How often?
- First is the drive, motivation, curiousity, penalty?
- IT Audit (own, external?)
- Compliance standards audit and certification
- Vulnerability management
- Compliances (industry, country, GOV, regulator, internal, frameworks?)
- Pentests (how often, how wide/deep, costs)
- Own red, blue, purple, white, LGBT team
- Managing own security stack (AV, FW, VPN, antiSpam..)
- Outsourced and maybe even insured (SOC, MSSP etc.)
- Acknowledge risks.. (have faith and other voodoo stuff..)

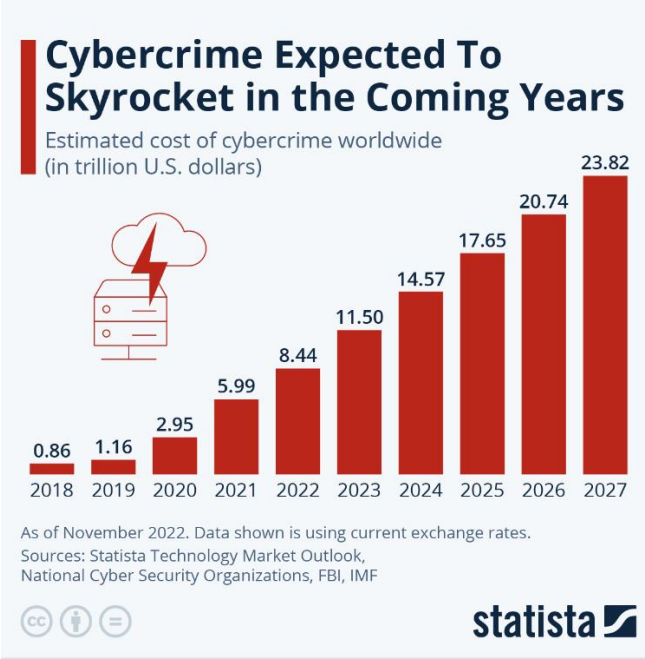
Some constraints



headtechnology
it · security · distribution · services

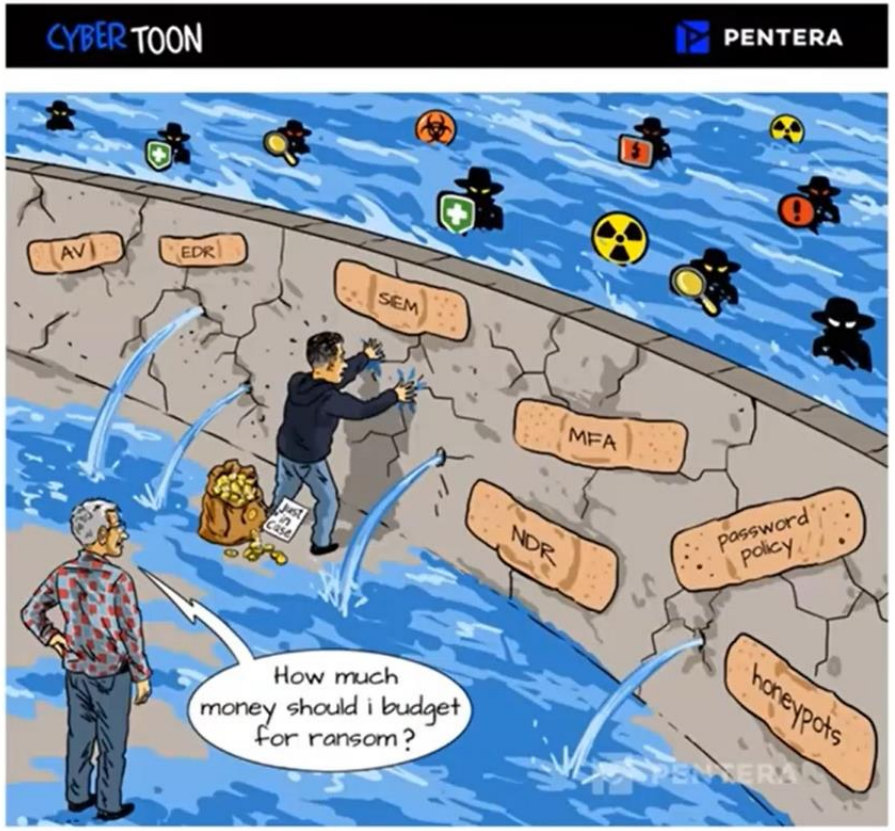
Few more constraints

- Too many standards, everything is changing too fast.
- Standards are outdated.
- Too many technologies and marketing attacks are sophisticated.
- Lack of HR. They burn out, change, are headhunted. Decide to work as dealers.
- Integrators stick to few vendors and push only them.
- Too much information or too much trust.
- Geopolitical issues.
- Economic issues. Expensive. Everything.
- Lack of political drive.
- Bad experience. Lack of trust.
- No knowledge and experience to restructure spending.
- Bureaucracy.
- No chance to control what is happening.
- Vendors buy each other.
- Crazy employees..



Technology advantages

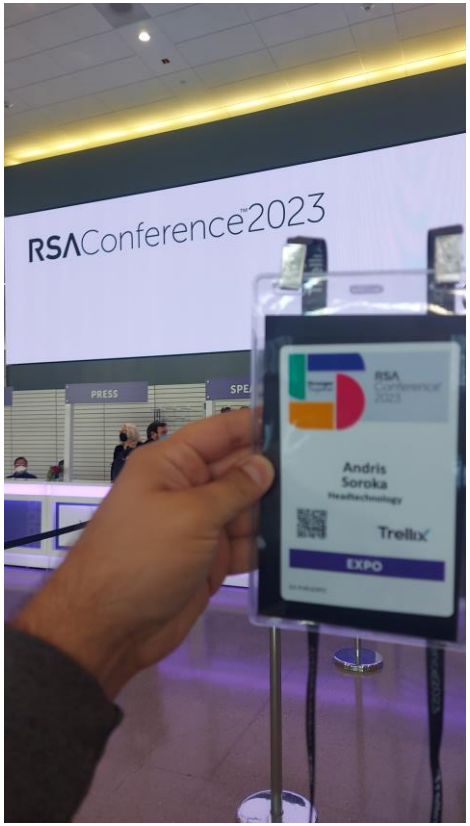
- **Cybersecurity made in Europe. ECSO/ENISA stuff.**
- **Certifications of technologies. EAL/CC etc.**
- **Price / performance. Restructure budgets.**
- **Prevention/proactive vs Reactive/IR**
- **AI / ML / DL empowered.**
- **Game changer.**
- **Trust but take back the control.**
- **Market analysts. Threat Frameworks.**
- **Innovative!**



headtechnology
it · security · distribution · services

Some sources..

- **ENISA CYBERSECURITY MARKET ANALYSIS FRAMEWORK V2.0 (March 2023)**
- **Hype Cycle for Security Operations (July 2023)**
- **MITRE ATT&CK® Matrix for Enterprise (ongoing)**
- **NIST ZERO TRUST Architecture Technology Partners/Collaborators (ongoing)**
- **A Deep Dive Into The Forrester Wave™: Zero Trust Edge Solutions, Q3 2023**
- **ISACA, SANS Institute, Ponemon etc.**
- **Largest industry events – RSA, Defcon, Blackhat, B-Sides, Infosecurity etc.**



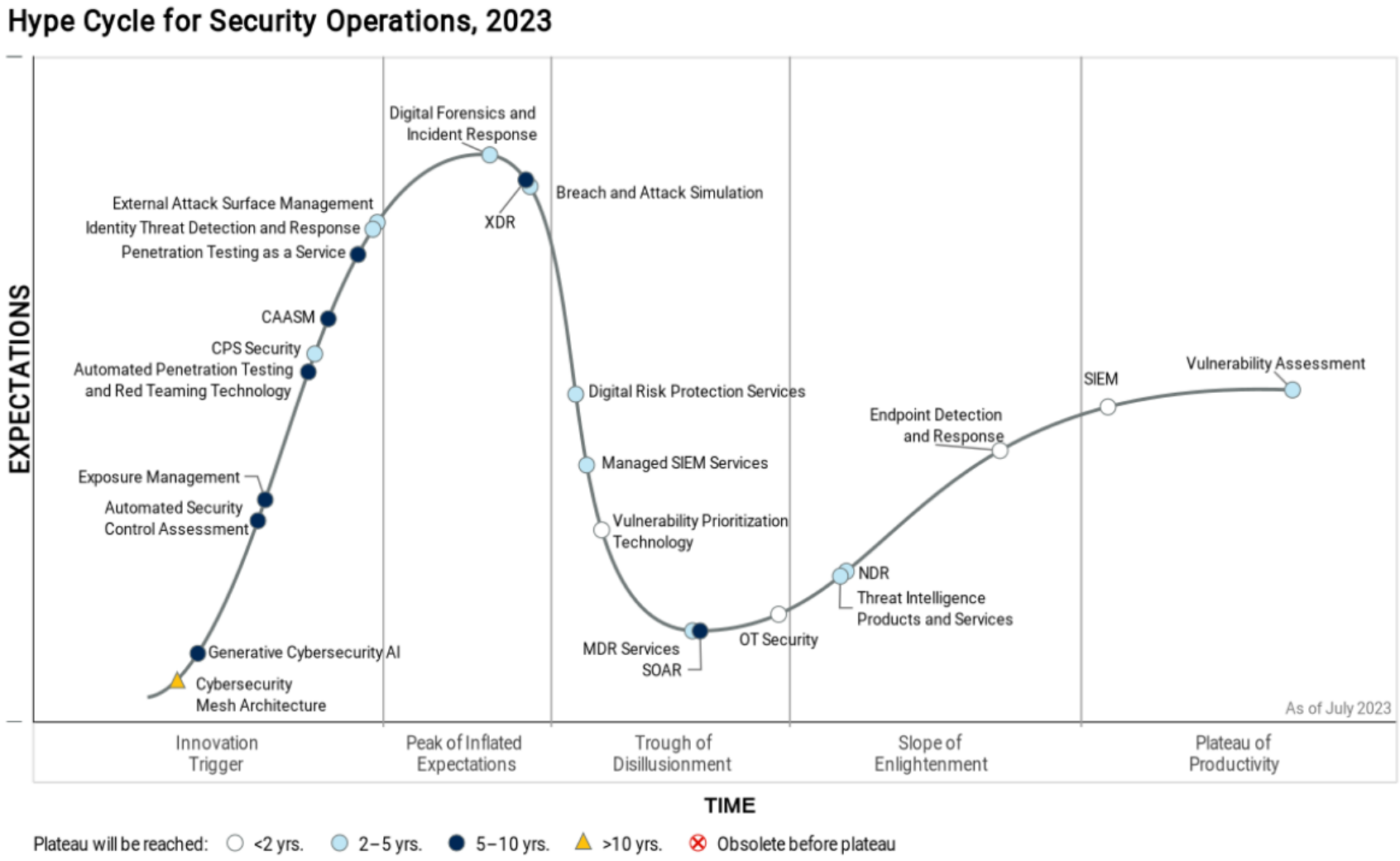
headtechnology
it · security · distribution · services

Some innovations&trends

- **Automated Cybersecurity Validation Platform – PENTERA**
- **ZERO Trust (SDP/ZTNA)**
- **(Multi-) Cloud Security**
- **Supply Chain Security (API as well)**
- **Reputation checkups (various)**
- **Quantum anything**
- **IoT/OT/Smart security (including medical and specific)**
- **Deep-Learning (DNA of malware)**
- **Various browsers, biometrics, behavioral solutions.**

headtechnology
it · security · distribution · services

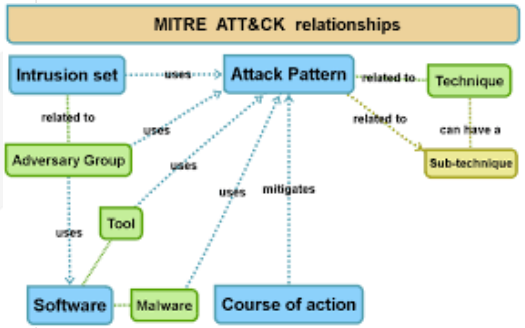
SecOps Tech Hype 2023



headtechnology
it · security · distribution · services

MITRE Framework

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	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
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Direct Volume Access	Modify Authentication Process (5)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process (5)	Valid Accounts (4)	Hide Artifacts (10)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Hijack Execution Flow (12)	Steal or Forge Kerberos Tickets (4)	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Impair Defenses (9)	Steal Web Session Cookie	Network Sniffing		Input Capture (4)	Traffic Signaling (1)		
				Scheduled Task/Job (5)		Indirect Command Execution	Unsecured Credentials (7)	Password Policy Discovery		Screen Capture	Web Service (3)		
				Server Software Component (5)		Masquerading (7)		Peripheral Device Discovery		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (5)		Permission Groups Discovery (3)					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image (2)		Remote System Discovery					
						Network Boundary Bridging (1)		Software Discovery (1)					
						Obfuscated Files or Information (6)		System Information Discovery					
						Plist File Modification		System Location Discovery (1)					
						Pre-OS Boot (5)		System Network Configuration Discovery (1)					
						Process Injection (12)							



headtechnology
it · security · distribution · services

Please visit and register!

ATTA Centre, Riga, Latvia

Annual Conference, Expo & Workshops

OCTOBER 26, 2023

BROUGT BY

DIGITAL FUTURE EVENTS

PLATINUM PARTNERS

headtechnology · FORESCOUT · LOGPOINT · deepinstinct

SPONSORING AND SUPPORTING AUTHORITIES

IT-Harvest · PENTERA · GTB Technologies · STELLAR CYBER · appgate · (Veriato) · OneSpan · eset · radware · RISEBA · Latvijas Kiberpsiholoģijas Asociācija · DATI GROUP · CERT.LV · ITEKSPERTS · VIDZEME UNIVERSITY OF APPLIED SCIENCES

CyberCommando's Meetup 2023 partners and participants

CCM RIGA·2023

TOPICS

4+ parallel sessions and workshops

- Proactive Cybersecurity based on Ai & Deep Learning
- DDoS, botnets and cyberwar
- CyberPsychology and hacker's mentality
- Zero Trust Principle and ZTNA
- SIEMs/SOARs/XDR's
- Cyber Security Technocentric Market
- EU NIS2 meets EU GDPR
- Data Classification and Data Leakage Prevention
- Automated Cybersecurity of Internet of Everything
- Continous Cybersecurity Validation
- Whitebox/Blackbox and Greybox hacking

SPEAKERS


Franck Bernard
Logpoint


Mathias Widler
DeepInstinct


Michael Soukonnik
Radware


Steve Smith
Pentera


Arnis Puksts
GDPR


Andris Soroka
HeadTechnology


Andrejs Konstantinovs
caurumi.lv


Egils Rupenheits
ESET


Richard Stenthon
IT Harvest


Valērijs Dombrovskis
RISEBA

CCM RIGA·2023

corporate presentation

Thank You For Your Attention!

headtechnology
it · security · distribution · services

Andris Soroka
Director CEE & Baltics
Headtechnology Group

Mob: +371 2 9162784

Andris.Soroka@headtechnology.com