NRD Cyber Security

CyberAgent Workshop 4

Protecting SME Critical Infrastructure

European Cybersecurity Month Workshop

Sept 23. 10:10–10:35 | Attacks on Critical Infrastructures (SME): Reasonable Cybersecurity

Speaker: Dr. Vilius Benetis,
Director at NRD Cyber Security,
Lithuania

NRDCS.EU

Focus

- Cybersecurity operations build-out
- Incident detection and handling
- Establishment and support of Computer Security Incident Response Teams (CSIRTs) and Security Operation Centres (SOCs)
- Cyber capacity building for organisations, sectors, and nations

Customers

Governments, public, and private sector organisations.

We are based in
Lithuania

Project geography

NRD Cyber Security

Dr. Vilius Benetis
Director

About

- Dr. Vilius Benetis specialises in security operations build-out: CSIRT/SOCs incident response capability establishment or modernisation for nations, regions, sectors, and organisations.
- Dr. Benetis is also a researcher and contributor to FIRST.Org's CSIRT Services Framework and CIS Controls. He advocates SIM3 and SOC-CMM models for CSIRT/SOC modernisation and Oxford's CMM model for national cybersecurity capacity building.
- A graduate of Kaunas University of Technology (KTU), with a BSc in Computer Science as well as a MSc and PhD in Teletraffic Engineering from the Danish Technical University.

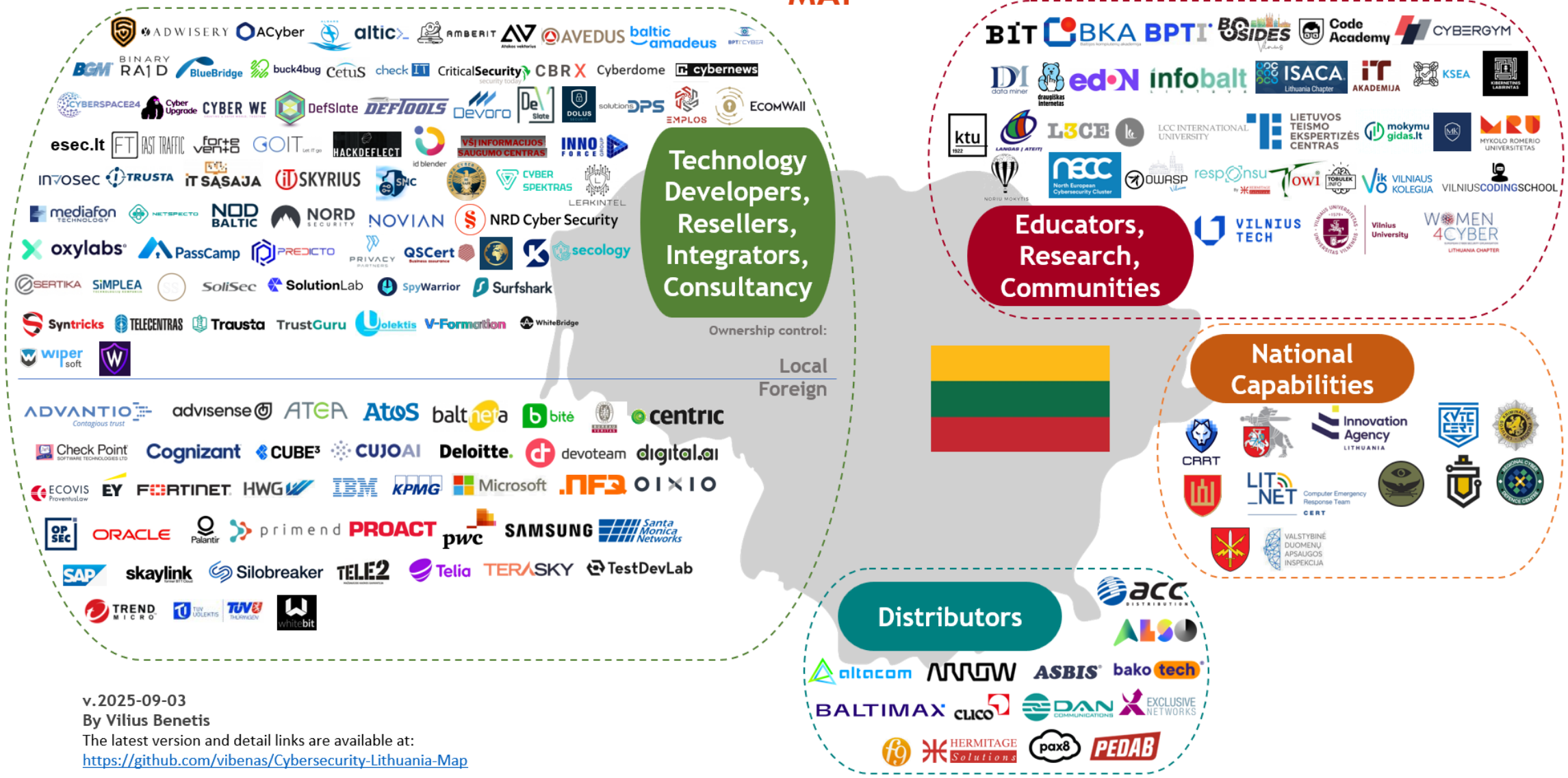
Areas of expertise

- CSIRT/SOC establishment
- Cybersecurity resilience and governance

Credentials and memberships in professional associations

CISA I CRISC I ITU-D I GFCE B I CIS I Certified SIM3 and SOC-CMM Auditor

CYBERSECURITY@LITHUANIA MAP



v.2025-09-03
By Vilius Benetis
The latest version and detail links are available at:
https://github.com/vibenas/Cybersecurity-Lithuania-Map

Protecting the critical infrastructure of SMEs from cyber-attacks

Were you **negligent** or were you just **victim**?

If you are SME and negligent, how much you should to be punished?

- You are punished by criminals
- Should you be punished by law as well?

Depends on the rules/culture/laws

- What are cybersecurity culture? Does it draw line what is good-enough cybersecurity?

- IS there anything what means REASONABLE CYBERSECURITY ???
- Typical Attacks on SMEs:
  - Ransomware via vulnerable infrastructure
  - Email or Websites Phishing (BEC, credential harvesting via infostealers, ..)
  - Hacked infrastructure for reuse of other attacks (supply chain, C&C, malware distribution)

Reasonable Cybersecurity: CIS Controls 8.1 Implementation Group 1

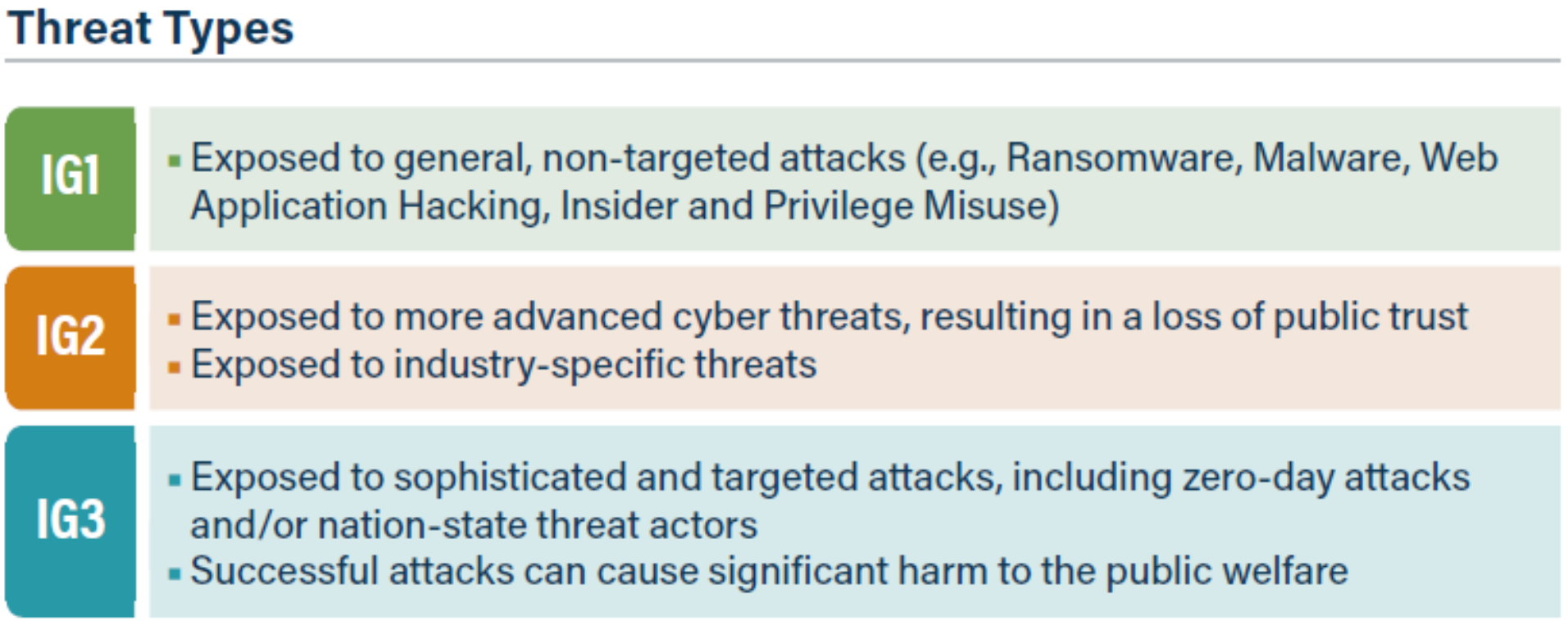
Factors Affecting Implementation

	Size and/or Complexity	Data Types	Resources and Technology	Threat Types	Risk
	CHARACTERISTICS				
IG1 ESSENTIAL CYBER HYGIENE	▪ Small and medium-sized enterprises ▪ Starting point for all enterprises	▪ Data is low sensitivity ▪ Stores unregulated employee and company financial information ▪ No regulatory or compliance oversight	▪ Limited cybersecurity expertise, may outsource IT/cybersecurity needs ▪ Uses existing and/or cost-effective technology and processes ▪ Uses Commercial off-the-Shelf (COTS) products	▪ Exposed to general, non-targeted attacks (e.g., Ransomware, Malware, Web Application Hacking, Insider and Privilege Misuse)	▪ Limited tolerance for downtime ▪ Focus is to keep business operational
IG2	▪ Enterprises managing IT infrastructure spanning multiple departments with differing risk profiles ▪ Increased operational complexity	▪ Stores and processes sensitive client or enterprise information ▪ Pockets of regulatory or compliance oversight	▪ Implements enterprise-grade technology ▪ Has specialized expertise to install and properly configure software ▪ Use COTS products, and may be using proprietary/ in-house software	▪ Exposed to more advanced cyber threats, resulting in a loss of public trust ▪ Exposed to industry-specific threats	▪ Faces an increased risk exposure (probability x potential losses) ▪ Can withstand short interruptions of service ▪ Concern is loss of public trust if a breach occurs
IG3	▪ Large enterprises that are operationally complex ▪ Increased risk profile across the enterprise	▪ Stores and processes sensitive and confidential data ▪ Subject to regulatory and compliance oversight	▪ Employs security experts that specialize in various areas of cybersecurity ▪ Likely using software designed in-house or proprietary to the enterprise, in addition to COTS products ▪ Ability to purchase dedicated cybersecurity software for specific tasks	▪ Exposed to sophisticated and targeted attacks, including zero-day attacks and/or nation-state threat actors ▪ Successful attacks can cause significant harm to the public welfare	▪ Faces the highest risk exposure ▪ Cannot withstand interruptions of service

CIS Controls 8.1

Logic on CIS IG1:

Figure 6 | Threat Type factors impacting IG selection



More resources:

- https://www.cisecurity.org/controls
- https://www.cisecurity.org/controls/cis-controls-list
- https://www.cisecurity.org/controls/cis-controls-navigator

NRD Cyber Security

Let's cooperate on securing the digital environment!

www.nrdcs.eu

Phone: +370 5 219 1919

E-mail: info@nrdcs.lt

Gynėjų str. 14, Vilnius

LT-01109, Lithuania