



CSIRT and SOC modernization practices

Dr. Vilius Benetis
NRD CIRT

<https://www.linkedin.com/in/viliusbenetis>



Friday, July 1st, 10:15 - 10:50



ABOUT ME



DR. VILIUS BENETIS

Member of NRD CIRT

ABOUT DR. VILIUS BENETIS

Dr. Vilius Benetis specializes in security operations build-out:

- CSIRT/SOCs incident response capability establishment or modernization for nations, regions, sectors and organizations

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 modernization and Oxford's CMM model for national cybersecurity capacity building.

Vilius Benetis graduated from Kaunas University of Technology (KTU), with BSc in Computer Science as well as MSc and PhD in Teletraffic Engineering from Danish Technical University, and currently serves as a cybersecurity industry professor at KTU.

AREAS OF EXPERTISE

- CSIRT/SOC establishment
- Cybersecurity resilience/governance (CII)

CREDENTIALS AND MEMBERSHIPS IN PROFESSIONAL ASSOCIATIONS

- CISA, CRISC, board m. ISACA Lithuania
- ITU-D, GFCE WG-B CIM, NECC
- Certified SIM3 Auditor

YOU?

1. CSIRT/SOC

- 1. Manager
- 2. Incident handler
- 3. Other role

2. Consultant

3. Vendor

4. Other



NRD Cyber Security

We are based in Lithuania

FOCUS

Cybersecurity operations build-out, incident detection and handling, establishment and support of CSIRT / SOC and cyber capacity enhancement / modernization for organizations, sectors and nations

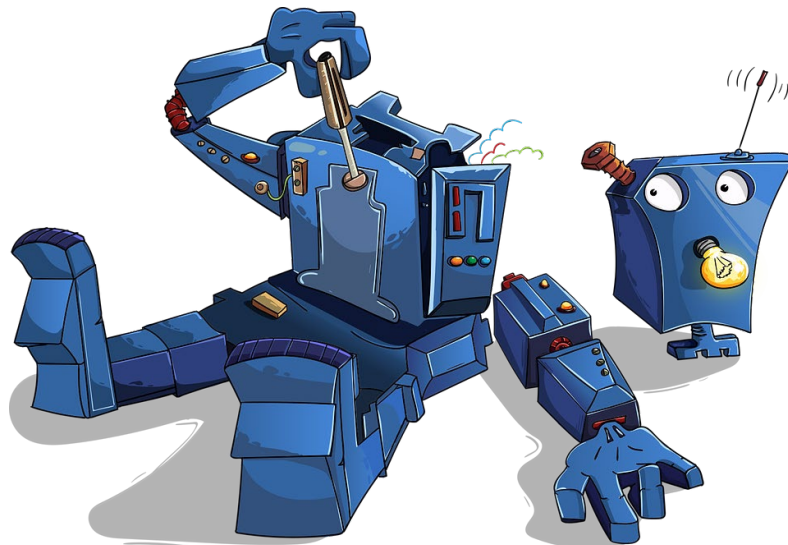
CUSTOMERS

Governments, public and private sector organizations



Modernization of CSIRTs and SOC

- CSIRTs and SOC are increasingly expected to work as professional and effective organizations
 - which can reflect on own performance and improvement.
- Such expectation is not easy to fulfill for many teams around the world.



Learning objectives

1. How to plan annual review and improvement activities, based on examples
2. How to tune mandate -> service model -> processes -> KPIs for effective & balanced outcome
3. How to model competences of CSIRT and SOC teams via service model use
4. Inspiration how to manage the team more effectively



Lifecycle of CSIRT / SOC growth

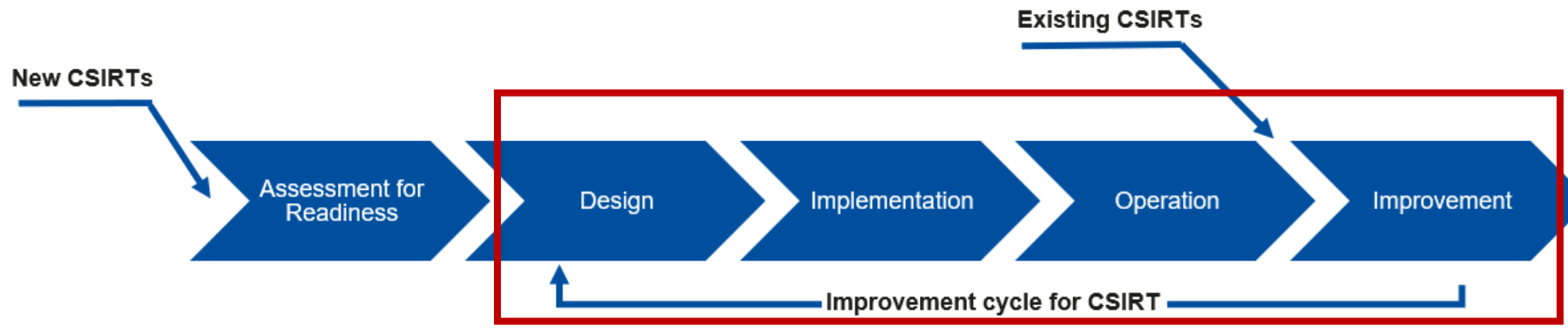


Figure 2 Summary of CSIRT Establishment Outcomes

Assessment for Readiness	Design	Implementation	Operations	Improvement
☐ Preliminary Mandate ☐ Governance Structure ☐ CSIRT hosting organisation ☐ Budget for 1-3 years ☐ Detailed Requirements for Design Stage	☐ Approved Detailed Mandate ☐ CSIRT Services Plan ☐ CSIRT Processes and Workflows Plan ☐ CSIRT Organisation, Skills and Training Structure Plan ☐ CSIRT Facilities Plan ☐ CSIRT Technologies and Processes Automation Plan ☐ CSIRT Cooperation Plan ☐ CSIRT IT and Information Security Management Plan ☐ Detailed Requirements for Implementation Stage	☐ Approved and implemented organisational structure ☐ Hired and appointed people ☐ Executed training plan for the staff roles ☐ Prepared facilities ☐ Developed and Implemented detailed processes and procedures ☐ Implemented technology for automation of processes ☐ Implemented IT and information security management procedures ☐ Trained people for CSIRT Operations ☐ Signed relevant agreements with constituency, stakeholders and partners ☐ CSIRT Services Test Run and Tuning Results ☐ CSIRT Launch Communication and Celebrations	☐ Measured KPIs ☐ Annual Operations Performance Review ☐ Annual Stakeholder Needs Review ☐ Approved Annual Budget ☐ Collected Requirements for Improvement	☐ List of chosen Initiatives for improvement ☐ Detailed Requirements for Improvement for Design Stage ☐ Preliminary Budget for Improvement

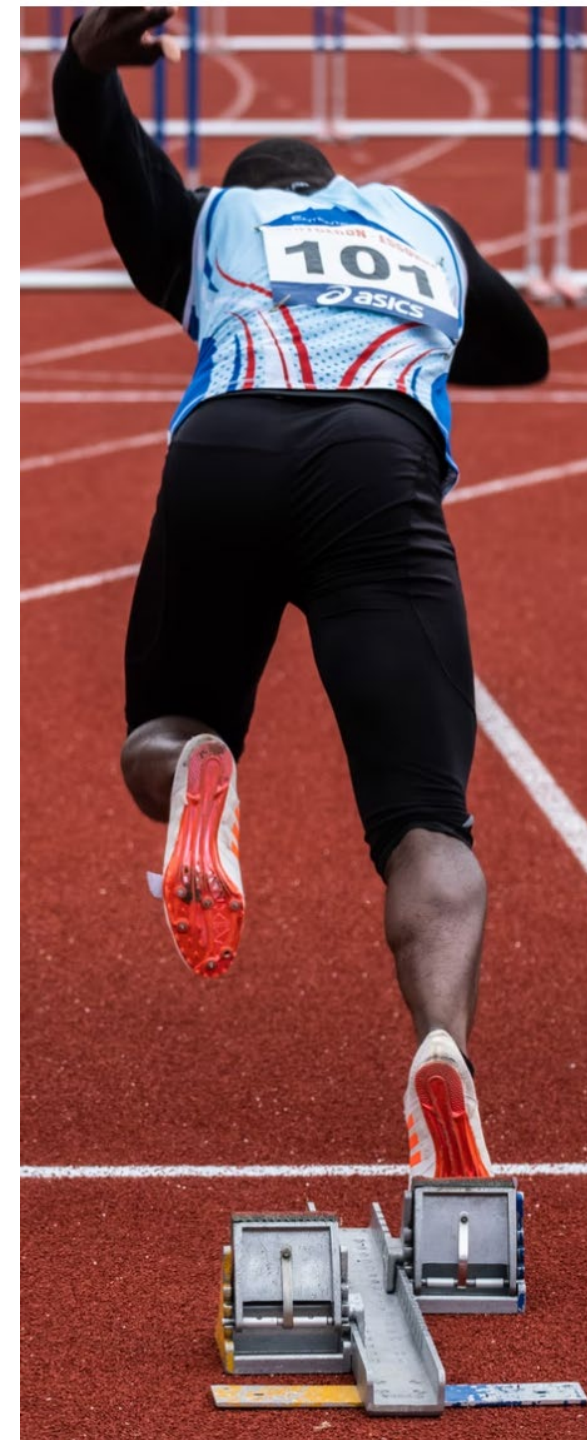


Authored by NRD Cyber Security team

How CSIRT/SOCs mature into well performing teams:

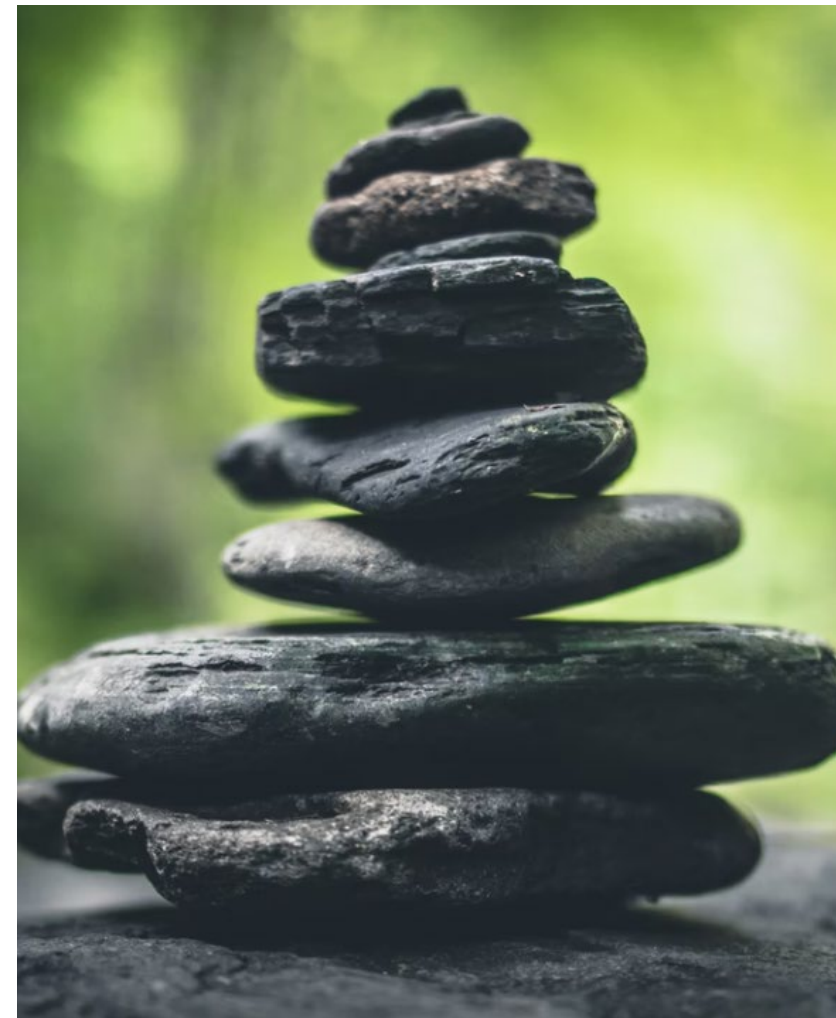
1. Managing **maturity** and preparing the **roadmaps for modernization**:
 1. SIM3 (by OCF, backed by FIRST.org, ENISA, GFCE)
 2. SOC-CMM (by Rob van Os)
2. **Review the mandate and strategy** via assessments of stakeholder needs / resources to adjust direction of operations and focus.
3. **Review CSIRT / SOC services** model (against FIRST.org CSIRT/PSIRT Services Model, SOC-CMM) clarifying priority services, and allocated resources.
4. **Review KPIs model of services** delivery
for improved tracking of CSIRT / SOC operational performance.
Improve the automation of the workflows of services.
5. **Reviewing the skills and competences model** of the organization to improve training plans for the staff positions, based on ENISA, FIRST CSIRT Services Competence model, NIST-NICE, and other work.

to improve training plans for the staff positions (CSIRT Manager training, CSIRT Technical Analyst trainings, ..)
6. ..and more...

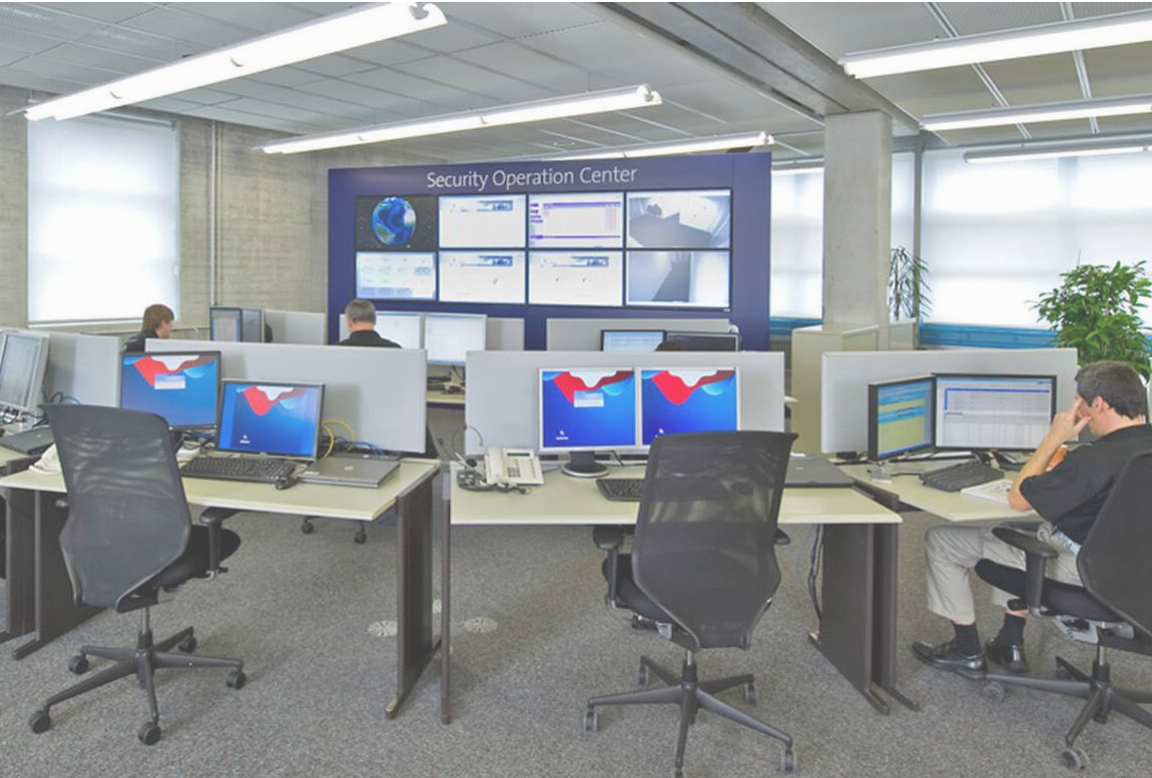


I.e. good practices of CSIRT / SOC

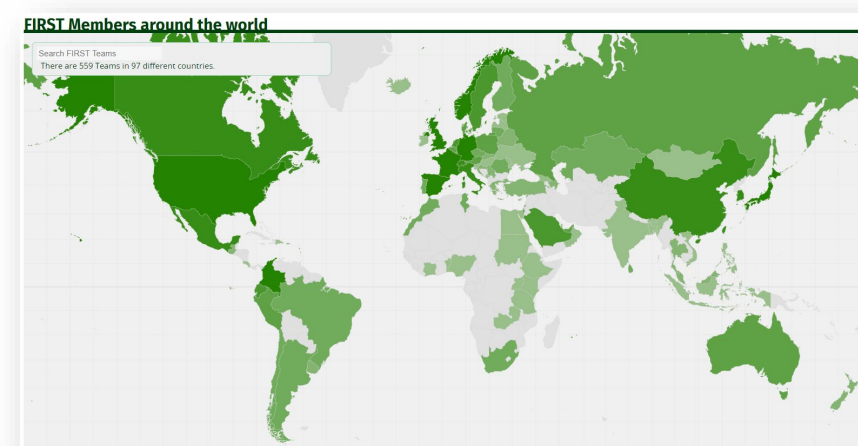
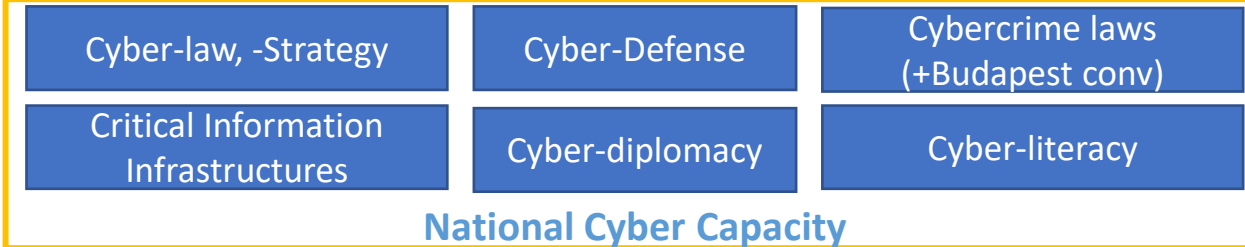
1. **Clear SOC Governance Model:**
Focus on stakeholders needs, clear mandate and CSIRT / SOC services implementation
2. **Extensive use of consolidated knowledge:**
SIM3, FIRST.org services model, SOC-CMM, RSIT taxonomy, setup guides, membership in FIRST.org, TF-CSIRT, ..
3. **Balance resources:**
Processes - People - Technology
4. **Valuable and applicable KPIs:**
KPIs should create actionable value



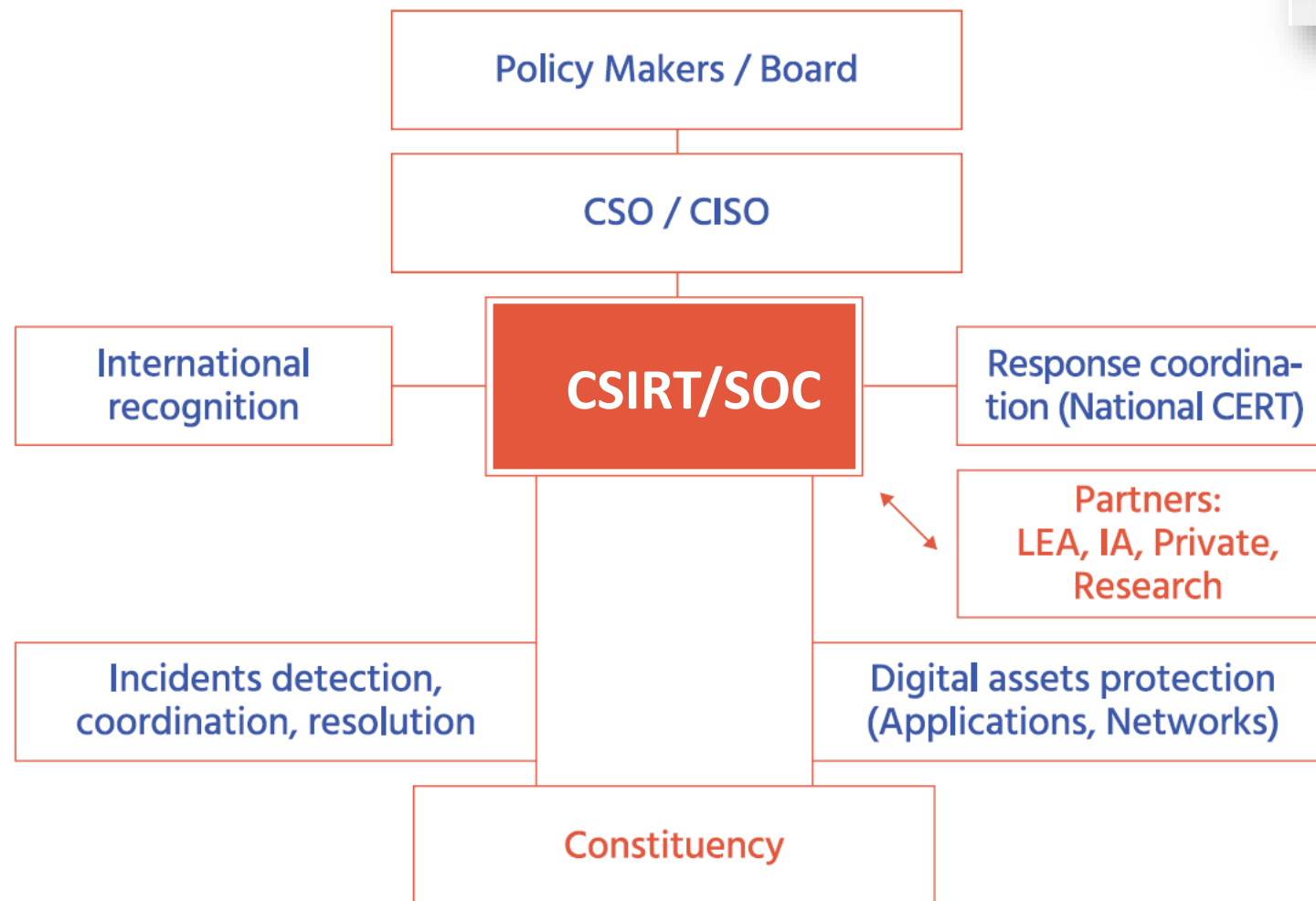
1. Clear SOC Governance Model: stakeholder needs



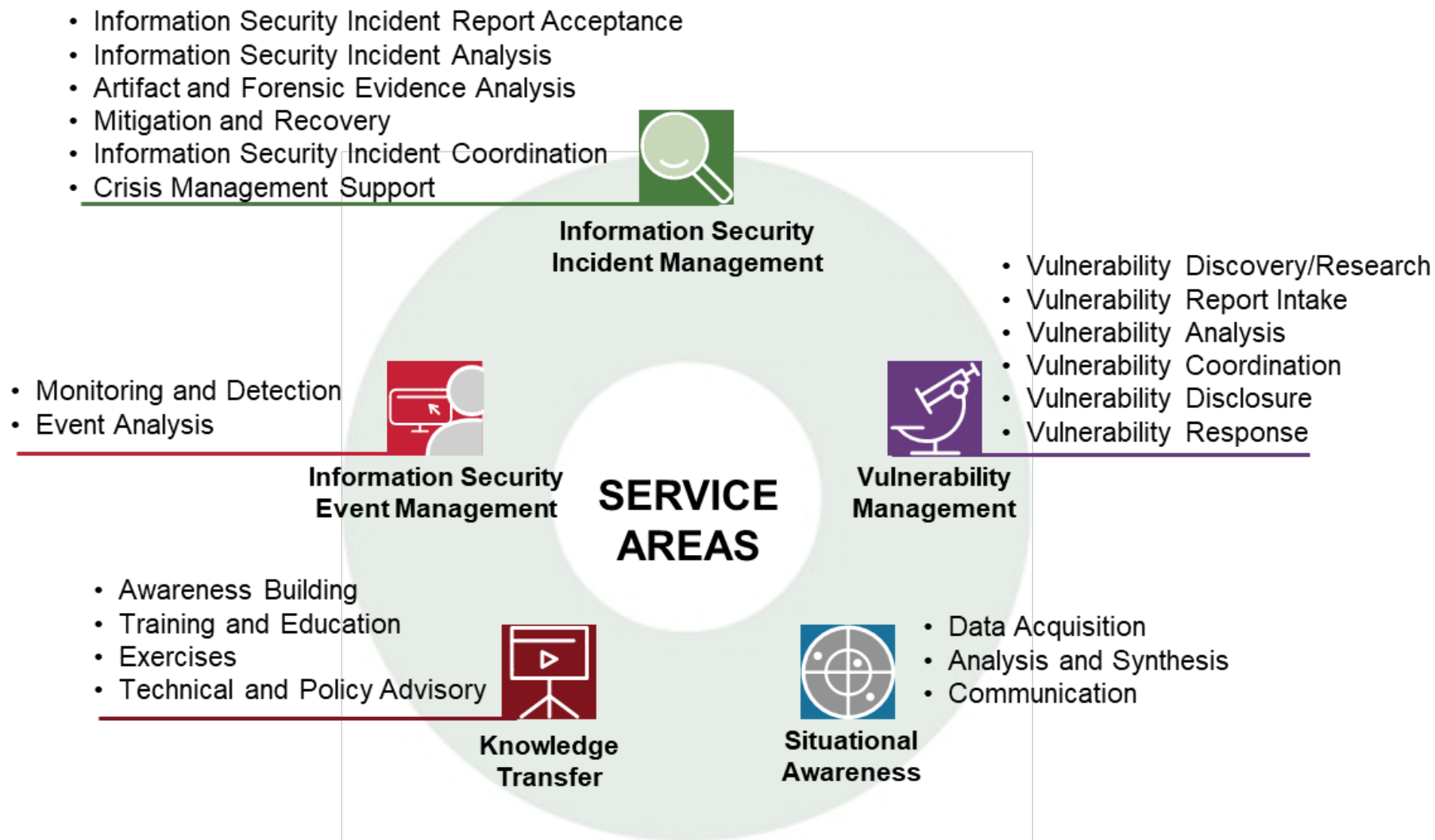
1. How to reduce negative **overall impact** of cyber incidents?
2. When attack hits:
is there a skilled team ready to respond and handle cyber-incidents using well known and **internationally accepted Incident Response method**?
3. Cyber crime is international:
is your team trusted by international community to **provide support** during your investigations?



1. Clear SOC Governance Model: positioning and mandate



1. Clear SOC Governance Model: FIRST.org Services Model Framework



Basic activities for value

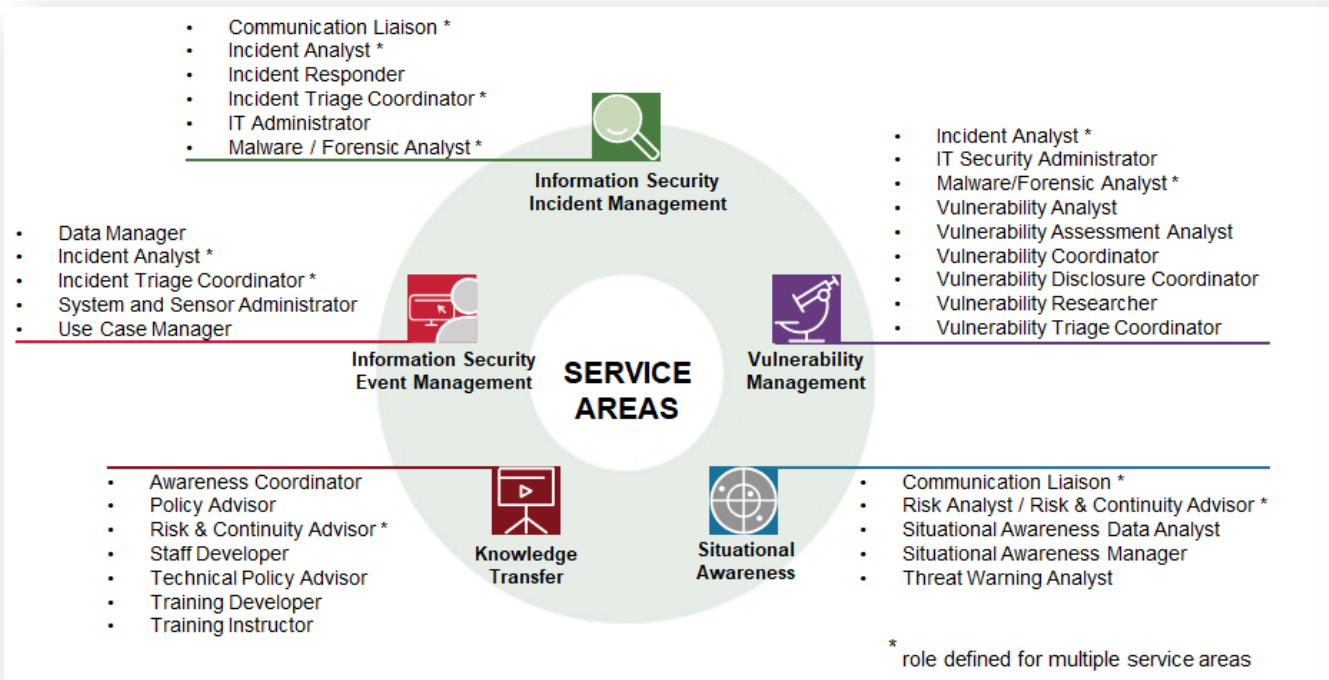
CSIRT



SOC



NEW!: FIRST.org CSIRT Services Roles and Competences v0.9 (CSIRT SIG, 76p report)



5.2.2 General Tasks

- Analyze and understand information security events, potential and confirmed information security incidents
- Assess the potential and actual impacts and damages
- Analyze incidents to identify root cause and impact
- Conduct cross-incidents analysis
- Analyze media and perform surface analysis of artifacts
- Discover incident-related vulnerabilities used by attacks
- Identify and correlate, when appropriate, distinct but possibly related security events and/or incidents to better understand the context of the incident in a bigger picture

5.2.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Event Management
 - Event Analysis
 - Correlation (5.2.1)
- Service Area: Information Security Incident Management
 - Information Security Incident Report Acceptance:
 - Information Security Incident Root Cause Analysis (6.2.4)
 - Cross-Incident Correlation (6.2.5)
 - Artifact and Forensic Evidence Analysis:
 - Media or Surface Analysis (6.3.1)
- Service Area: Vulnerability Management
 - Vulnerability Discovery/Research:
 - Incident Response Vulnerability Discovery (7.1.1)

5.2.4 Generic Competencies

- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
 - Oral Communication (C036)
 - Written Communication (C060)
- Technical
 - Problem Solving (C040)

5.2.5 Role-Specific Competencies

- Operational
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Organizational Awareness (C037)
- Technical
 - Computer Forensics (C005)

Contributors - many usual suspects:

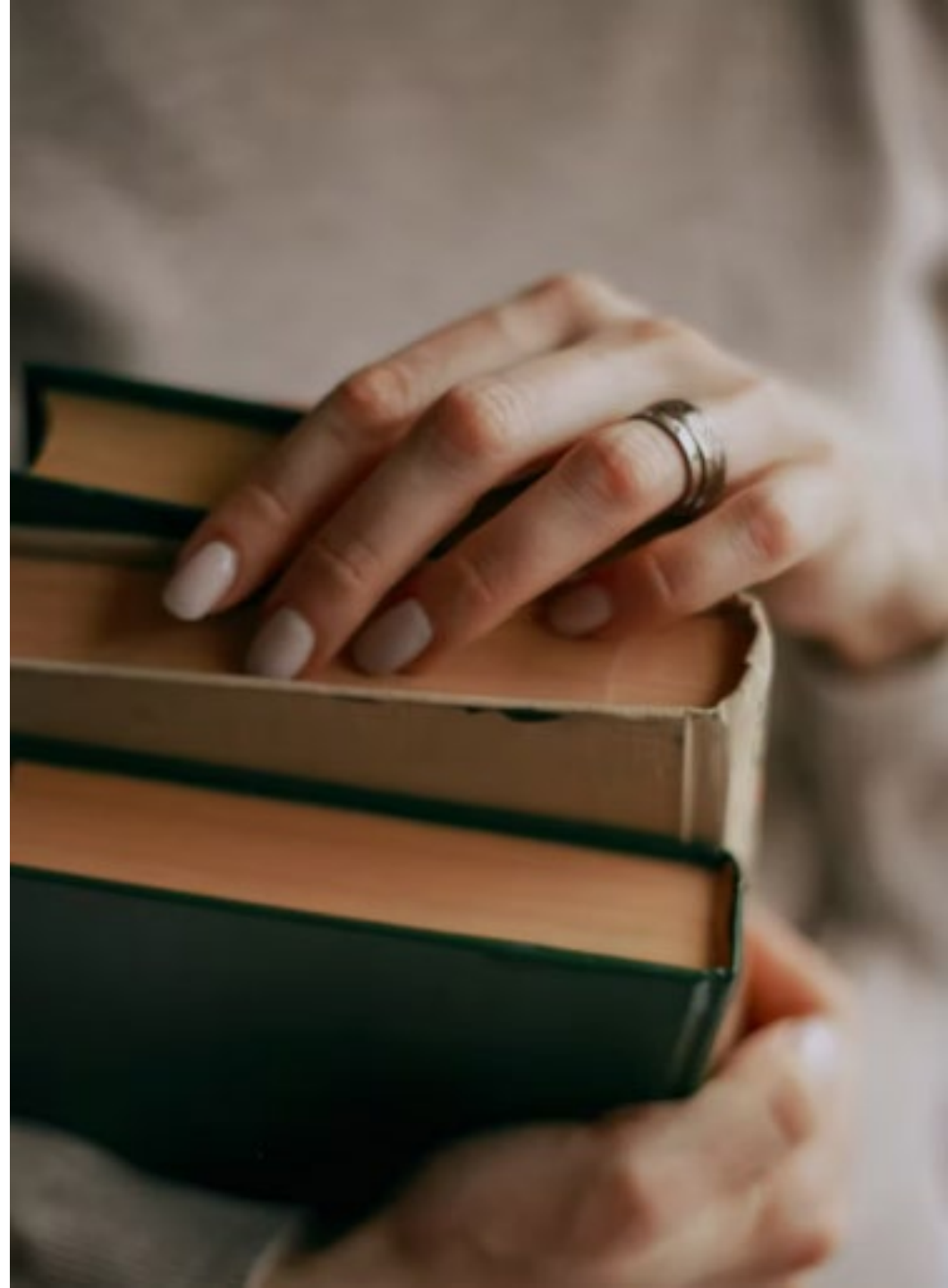
Klaus-Peter, Shin, Olivier, Cristine, Baiba, Franz, Samuel, Louis, Robin, Don, Edgars, Sanita, Mark, Vilius

Location: <https://www.first.org/global/sigs/csirt/>

2. Extensive use of consolidated knowledge

There is plenty of very specific CSIRT / SOC working knowledge.
Are you utilising it?

1. **SIM3**
for maturity of CSIRT / SOC organisation
2. **FIRST.org services model and competences model**
for services construction
3. **RSIT incident taxonomy (available on ENISA's github)**
for classifying cybersecurity incidents
4. **SOC-CMM**
for detail diagnostics and long term operational improvement
5. **ENISA, OAS, Thai-CERT setup guides**
for directing and getting ideas on improvements
6. **Membership in FIRST.org, TF-CSIRT**
for accessing tacit knowledge of peer-experts



3. Balance resources placed into CSIRT / SOC

How do you know that you balance \$\$\$ investment?

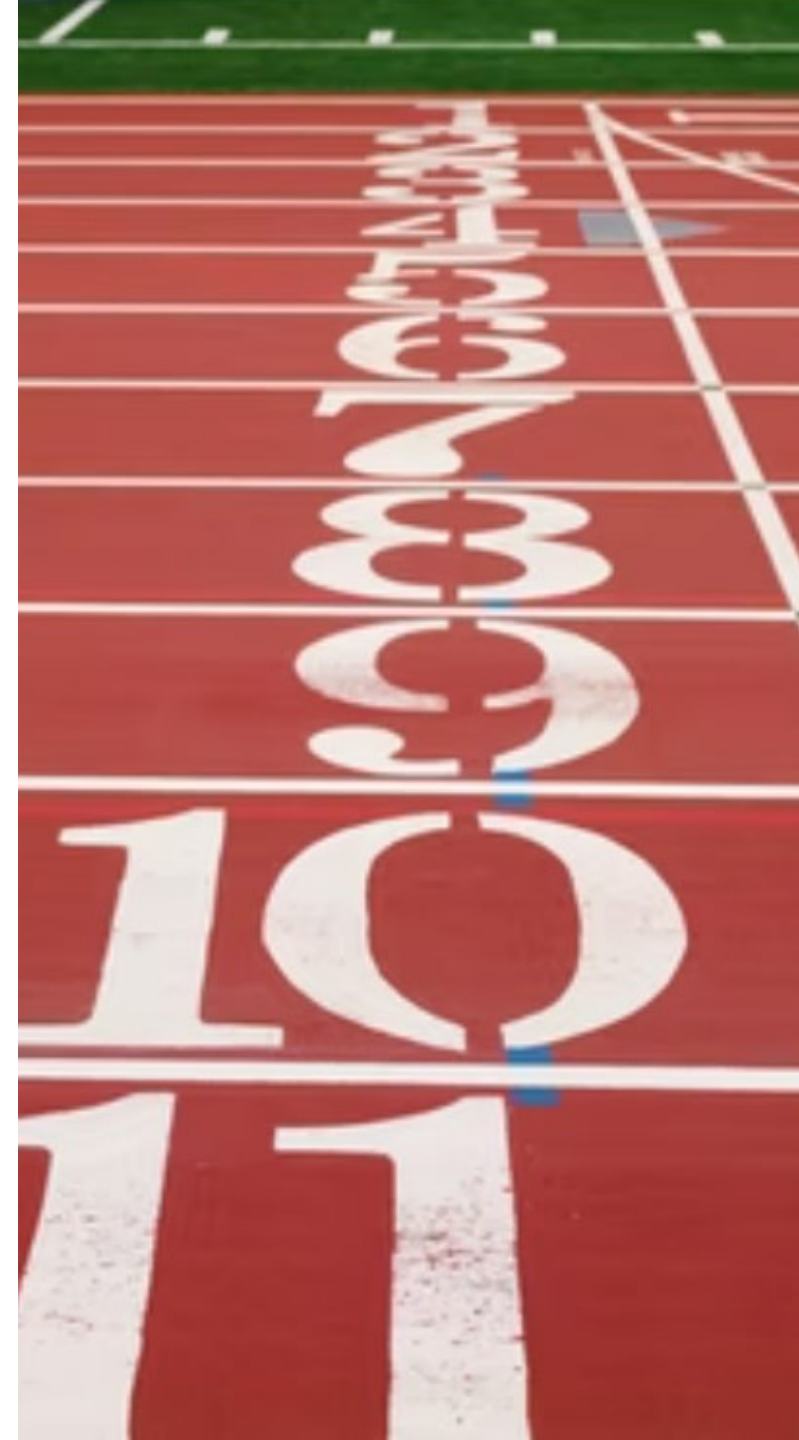
1. **Processes**
Probably - processes are not tuned to optimum
2. **People**
Probably lack of skills and hands
3. **Technology**
Usually not fully utilized what is acquired



4. Valuable and applicable KPIs

Each measured KPI must have short (month) or long (year) **actionable value** - linked to services and mandate.

- **Bad KPIs:**
 - Number of incidents - does not create any value
- **Connected KPIs:**
 - Time-to-respond metric kept under threshold (Response)
 - Errors in use-cases and human analysis are kept under threshold (Detect)
 - Coverage of monitored systems is kept under a threshold (Monitoring scope)
 - ..



KEY PERFORMANCE INDICATORS (KPI) CSIRT SERVICES DASHBOARD

CSIRT Dashboard for the monthly report

For: 2019 _____

Service	KPI	KPI objective	Reported value
Incident handling			
	Number of opened incidents (per priority Px)	Total number more than 0	
	Incidents registered – aggregated from daily reports	statistics aggregated by first working day of next month	Appendix 1.
	Statistics on which Constituency opened tickets	>0, as proper working relationship would record some incidents	
	Total number of outstanding not closed incidents in tracking system	Long term – should not increase	
	Percentage of incidents with breached initial response SLA (per priorities)	<5%	

Service	KPI	KPI objective	Reported value
Incident analysis			
	Number of confirmed complains (internal or external) about the quality, presentation, or professionalism of analysis		
	Quarterly drills conducted for analysts	Should be done in each quarter	
Incident mitigation			
	Percentage of closed tickets with successfully resolved status		
	Number of mitigated critical incidents with breached mitigation action's SLA	zero	
Artifact analysis	Number of artifact analysis which have breached reporting SLA		
Information Sharing and Publication			
	Number of website alerts and news	Not less than 3 in total	
	Unique total and visitors on CSIRT website	Long term should be growing	
	Quarterly report has been published, date	No later than the first week of <u>newQ</u>	
	Yearly report has been published, date	No later than 1st of Feb of new year	
Security awareness rising			
	Total number of events, meetings and trainings with external participation, organized by CSIRT (and number of Internal meetings with constituency)	>0	

DIFFERENT CSIRT/SOC STACKS

	Mini	Basic	Effective	Full Scale
Governance 	• Mandate definition • FIRST.org membership • Roadmap & Strategy	• Mandate definition • FIRST.org membership • Roadmap & Strategy	• Mandate definition • FIRST.org membership • Roadmap & Strategy • Orgchart buildout	• Mandate definition • FIRST.org membership • Roadmap & Strategy • Orgchart buildout
People 	• Featured CSIRT training • Limited remote support	• Relevant CSIRT training • Remote support • SOPs • Study mission tours	• Relevant CSIRT training • Remote support • SOPs • Study mission tours	• Relevant CSIRT training • On-site and remote support • SOPs • Study mission tours
Processes and services 	• Incident handling service • Incident handling process	• Incident handling and outreach • Infrastructure support • Standard reporting	• Incident handling, outreach, digital forensics, vulnerability management • Process automation • Infrastructure support • Standard reporting	• Full scale CSIRT/SOC services • Process automation • Automated custom reporting • Maturity progress assessment • Infrastructure support
Measurements 	• A few KPIs • No SLAs	• Basic KPIs • SLAs for processes	• KPIs system • SLAs for processes • <u>SIM3 successful audit</u>	• KPIs system • SLAs for services and automation • <u>Annual reviews, SOC-CMM L3 C15</u>
Technological Capability 	• Incident registration and handling • PGP	• Incident registration and handling • Outreach and visualization portal • Internal support, PGP • Simple vulnerability assessment	• Incident detection and handling • Outreach and visualization portal • Internal support, PGP • Simple vulnerability assessment • Simple video wall • Simple threat intelligence • Simple digital forensics • Simple integration with ex. tooling • Situational awareness	• Incident detection and handling • Outreach and visualization portal • Internal support, PGP • Vulnerability assessment • Video wall • Threat intelligence • Digital Forensics • Integration with existing tooling • Situational awareness and EWS • Multi-site sensing at CII
Local resources 	2-5 people	5-10 people	7-15 people	15-45 people
Duration 	9 months	12 months	12-24 months	24-36 months

Let's talk!

1. independent CSIRT/SOC assessments

How to identify current state and maturity, and issues & build roadmap, run professional CSIRT/SOC audits

2. Tune mandate, service model, processes, KPIs

3. Prepare your staff, or excel as CSIRT/SOC manager



Dr. Vilius Benetis

vb@nrdcs.lt, +37068755503

NRD Cyber Security

<https://www.linkedin.com/in/viliusbenetis>