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

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
1. CSIRT/SOC
   1. Manager
   2. Incident handler
   3. Other role
2. Consultant
3. Vendor
4. Other
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 SOCs

• CSIRTs and SOCs 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

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

- List of chosen initiatives for improvement
- Detailed Requirements for Improvement for Design Stage
- Preliminary Budget for Improvement

Author: 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

Policy Makers / Board

CSO / CISO

CSIRT/SOC

Response coordination (National CERT)

Partners: LEA, IA, Private, Research

Digital assets protection (Applications, Networks)

Incidents detection, coordination, resolution

Constituency

National Cyber Capacity
1. Clear SOC Governance Model: FIRST.org Services Model Framework

- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support

Information Security Incident Management
- Vulnerability Discovery/Research
- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Coordination
- Vulnerability Disclosure
- Vulnerability Response

Vulnerability Management
- Data Acquisition
- Analysis and Synthesis
- Communication

SERVICE AREAS
- Monitoring and Detection
- Event Analysis
- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

Knowledge Transfer

Situational Awareness

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
Basic activities for value

CSIRT
- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support
- Monitoring and Detection
- Event Analysis

SOC
- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support
- Monitoring and Detection
- Event Analysis

Service Areas
- Vulnerability Discovery/Research
- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Disclosure
- Vulnerability Coordination
- Vulnerability Response
- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory
- Data Acquisition
- Analysis and Synthesis
- Communication

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

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/

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 (C025)
  - 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)
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-CISRT**
   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 ________

<table>
<thead>
<tr>
<th>Service</th>
<th>KPI</th>
<th>KPI objective</th>
<th>Reported value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident handling</td>
<td>Number of opened incidents (per priority Px)</td>
<td>Total number more than 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incidents registered – aggregated from daily reports</td>
<td>statistics aggregated by first working day of next month</td>
<td>Appendix 1.</td>
</tr>
<tr>
<td>Statistics on which Constituency opened tickets</td>
<td>&gt;0, as proper working relationship would record some incidents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total number of outstanding not closed incidents in tracking system</td>
<td>Long term – should not increase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of incidents with breached initial response SLA (per priorities)</td>
<td>&lt;5%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>KPI</td>
<td>KPI objective</td>
<td>Reported value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Incident analysis</td>
<td>Number of confirmed complains (internal or external) about the quality, presentation, or professionalism of analysis</td>
<td>Quarterly drills conducted for analysts</td>
<td>Should be done in each quarter</td>
</tr>
<tr>
<td>Incident mitigation</td>
<td>Percentage of closed tickets with successfully resolved status</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of mitigated critical incidents with breached mitigation action’s SLA</td>
<td></td>
<td>zero</td>
</tr>
<tr>
<td>Artifact analysis</td>
<td>Number of artifact analysis which have breached reporting SLA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Sharing and</td>
<td>Number of website alerts and news</td>
<td>Not less than 3 in total</td>
<td></td>
</tr>
<tr>
<td>Publication</td>
<td>Unique total and visitors on CSIRT website</td>
<td>Long term should be growing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quarterly report has been published, date</td>
<td>No later than the first week of newQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yearly report has been published, date</td>
<td>No later than 1st of Feb of new year</td>
<td></td>
</tr>
<tr>
<td>Security awareness rising</td>
<td>Total number of events, meetings and trainings with external participation, organized by CSIRT (and number of internal meetings with constituency)</td>
<td></td>
<td>&gt;0</td>
</tr>
</tbody>
</table>
# DIFFERENT CSIRT/SOC STACKS

<table>
<thead>
<tr>
<th></th>
<th>Mini</th>
<th>Basic</th>
<th>Effective</th>
<th>Full Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>- Mandate definition</td>
<td>- Mandate definition</td>
<td>- Mandate definition</td>
<td>- Mandate definition</td>
</tr>
<tr>
<td></td>
<td>- FIRST.org membership</td>
<td>- FIRST.org membership</td>
<td>- FIRST.org membership</td>
<td>- FIRST.org membership</td>
</tr>
<tr>
<td>People</td>
<td>- Featured CSIRT training</td>
<td>- Relevant CSIRT training</td>
<td>- Relevant CSIRT training</td>
<td>- Relevant CSIRT training</td>
</tr>
<tr>
<td></td>
<td>- Limited remote support</td>
<td>- Remote support: SOPs, SGPs</td>
<td>- Remote support: SOPs, SGPs</td>
<td>- Remote support: SOPs, SGPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Study mission tours</td>
<td>- Study mission tours</td>
<td>- Study mission tours</td>
</tr>
<tr>
<td>Processes and</td>
<td>- Incident handling service</td>
<td>- Incident handling and</td>
<td>- Incident handling, outreach, digital</td>
<td>- Full scale CSIRT/SOC services</td>
</tr>
<tr>
<td>services</td>
<td>- Incident handling</td>
<td>outreach, infrastructure</td>
<td>forensics, vulnerability management</td>
<td>- Process automation</td>
</tr>
<tr>
<td></td>
<td>process</td>
<td>- Infrastructure support</td>
<td>- Infrastructure support</td>
<td>- Automated custom reporting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Standard reporting</td>
<td>- Standard reporting</td>
<td>- Maturity progress assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Infrastructure support</td>
</tr>
<tr>
<td>Measurements</td>
<td>- A few KPIs</td>
<td>- Basic KPIs</td>
<td>- KPIs system</td>
<td>- KPIs system</td>
</tr>
<tr>
<td></td>
<td>- No SLAs</td>
<td>- SLAs for processes</td>
<td>- SLAs for processes</td>
<td>- SLAs for services and automation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- NISB successful audit</td>
<td>- Annual reviews, SOC-CMM L3 C15</td>
</tr>
<tr>
<td>Technological</td>
<td>- Incident registration</td>
<td>- Incident registration and</td>
<td>- Incident detection and handling</td>
<td>- Incident detection and handling</td>
</tr>
<tr>
<td>Capability</td>
<td>and handling</td>
<td>and handling</td>
<td>- Outreach and visualization portal</td>
<td>- Outreach and visualization portal</td>
</tr>
<tr>
<td></td>
<td>- PGP</td>
<td>- Internal support, PGP</td>
<td>- Internal support, PGP</td>
<td>- Internal support, PGP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Simple vulnerability</td>
<td>- Simple vulnerability assessment</td>
<td>- Vulnerability assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>assessment</td>
<td></td>
<td>- Simple video wall</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Simple threat intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Simple digital forensics</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Simple integration with ex. tooling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Situational awareness</td>
</tr>
<tr>
<td>Local resources</td>
<td>2-5 people</td>
<td>5-10 people</td>
<td>7-15 people</td>
<td>15-45 people</td>
</tr>
<tr>
<td>Duration</td>
<td>9 months</td>
<td>12 months</td>
<td>12-24 months</td>
<td>24-36 months</td>
</tr>
</tbody>
</table>
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

Let’s talk!

Dr. Vilius Benetis
vb@nrds.lt, +37068755503
NRD Cyber Security
https://www.linkedin.com/in/viliusbenetis