NGSOTI - Summary of the action, milestones and deliverables

Restena - Coffee

CIRCL
Computer Incident
Response Center
Luxembourg

CIRCL *TLP:CLEAR*

info@circl.lu

2024-02-08

NGSOTI - Next Generation Security Operator Training Infrastructure] - Objectives

`The action aims at creating an open-source infrastructure for SOC operators practical training regarding network-related alerts.`

- Incident Response $\rightarrow$ best practices
- Log Management and Analysis
- Security Operations Center Management $\rightarrow$ processes
- Communication and Documentation
- Cyber Threat Intelligence
- D4 will be a data source
- The action will make use of low-interaction honeypots
- AIL-project (Analysis Information Leak https://ail-project.org) is a framework used to monitor

NGSOTI - Next Generation Security Operator Training Infrastructure] - Objectives

- Intrusion detection systems $\rightarrow$ suricata, Zeek, vast
- The action will use known open source SIEM technologies
- The action will use the open source tool VAST
- The action will use the ticketing system RTIR
- MISP will be the CTI
- Open source monitoring tools $\rightarrow$ OpenNMS
- MeliCERTes tools will be used $\rightarrow$ Cerebrate

Workpackages

#	Name	Start	End
1	Project management and coordination	1/1/2024	31/12/2026
2	NGSOTI setup and operation	1/1/2024	31/12/2026
3	Training and education	1/1/2024	31/12/2026
4	Dissemination and endorsement	1/1/2024	31/12/2026

Work package 1

Tasks

#	Name
1.1	Project coordination
1.2	Research coordination

Work package 2

Tasks

#	Name
2.1	Technical infrastructure setup
2.2	Providing network connectivity for the infrastructure
2.3	Processing and analysis of the threat detection stream
2.4	Maintenance of NGSOTI
2.5	edu.lu URL checker

Work package 3

Tasks

#	Name
3.1	NGSOTI trainings
3.2	Training on cybersecurity
3.3	Training material publications
3.4	NGSOTI research opportunity evaluation
3.5	Cybersecurity early stage researcher educational plan

Work package 4

Tasks

#	Name
4.1	NGSOTI components blog posts
4.2	Research publications
4.3	Public Lectures / Seminars
4.4	General endorsement of cybersecurity competence in present and future research agenda.

Deliverables 1/3

#	Description	Due date	Resp.
D1.1	NGSOTI deployment status report 1	31/12/2024	LHC
D2.1	Technical requirement analysis report collected	31/12/2024	LHC
D2.2	NGSOTI data key findings report #1	30/11/2024	LHC
D2.3	NGSOTI data key findings repory #2	30/11/2025	LHC
D2.4	NGSOTI sustainability report	30/06/2026	LHC
D3.1	References of training material updates #1	31/03/2025	LHC
D3.2	References of training material updates #2	30/06/2026	LHC

Deliverables 2/3

#	Description	Due date	Resp
D3.3	Reports on NGSOTI training experience and WP3 data set	30/06/2026	uni.lu
D3.4	Reference to lectures given at master courses on cybersecurity and cybersecurity practices	31/12/2026	uni.lu
D3.5	References of training materials	31/12/2026	Restena
D4.1	NGSOTI architecture document	31/03/2024	LHC
D4.2	NGSOTI data collection blog post	30/09/2024	LHC

Deliverables 3/3

D4.3	NGSOTI training experience blog post	30/06/2025	LHC
D4.4	NGSOTI information sharing blog post	31/12/2025	LHC
D4.5	Annual report on seminar and talks	31/12/2026	LHC
D4.6	Research Agenda activity report	30/06/2026	uni.lu
D4.7	Dissemination and exploitation deliverable	29/02/2024	LHC

Milestones

#	Description	Due date
1	Teaching collaboration setup	30/04/2024
2	Hardware tender published	29/02/2024
3	Hardware installed	31/07/2024
4	edu.lu checker implementation	28/02/2026
5	NGSOTI training performance #1	28/02/2025
6	NGSOTI training performance#2	31/08/2025
7	NGSOTI Internship announce	30/06/2024
8	kick-off meeting	30/06/2024
9	Mid-term review meeting	30/06/2025
10	Final review meeting	31/12/2026