NGSOTI - Next Generation Security Operator Training Infrastructure

DGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS - CYSSME.eu

event 18/03/2024

CIRCL
Computer Incident
Response Center
Luxembourg

CIRCL *TLP:CLEAR*

info@circl.lu

2024-03-18

NGSOTI - Consortium

- Luxembourg House of Cybersecurity (LHC) coordinator
- Computer Incident Response Center Luxembourg
- Fondation Restena
- University of Luxembourg (Interdisciplinary Research Group in Socio-technical Cybersecurity)
- Tenzir






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 the 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

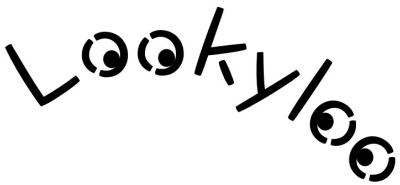
- Intrusion detection systems $\rightarrow$ suricata, Zeek, vast
- The action will use known open source SIEM technologies
- The action will use the open source tool VAST
- The action will use the ticketing system RTIR
- MISP will be the CTI
- Open source monitoring tools $\rightarrow$ OpenNMS
- MeliCERTes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

NGSOTI - Cybersecurity solution pillars

Focus on open source solutions



NGSOTI - Cybersecurity solution pillars

Focus on open source solutions

- MISP `https://www.misp-project.org/`
- Tenzir Open source data pipelines for security teams `https://tenzir.com/`
- Distributed denial of service detection (d4-project.org) `https://d4-project.org/`
- AIL - project `https://ail-project.org/`
- Lookyloo `https://github.com/Lookyloo`
- Pandora `https://github.com/pandora-analysis`

Trainings

With a focus on the cybersecurity solutions pillars

- Hybrid training in Luxembourg / video conference
- 3 training during the next project
- Next events
  - Monday, April 15th 2024 at FIRST CTI 2024 (Berlin) - MISP API and Automation Workshop (14:00-18:00)
  - Wednesday, April 18th 2024 at FIRST CTI 2024 (Berlin) - Sharing Information and Intelligence without Disclosing It - Private Search Set (PSS)
  - Hack.lu and CTI summit 22-25 October 2024

Target audience

- Threat Analysts
- Bachelor / Master students
- Open Source Enthusiasts
- Engineering Students
- Security Professionals and SOC operators

NGSOTI is looking for contributors

- Github `Issues` creation and `Pull Requests` are welcome
- NGSOTI project outcomes are open-source
  `https://github.com/ngsoti/ngsoti/`
- Extension of open source training material
  - `https://github.com/MISP/misp-training`
  - `https://github.com/ail-project/ail-training`
  - `https://github.com/D4-project/architecture`
- Contributions on the software are also welcome