Practical Cyber SecurityWorkshop

Workshop Overview

This four-day intermediate workshop introduces practical approaches to cyber defence, incident response, detection, and coordination. The workshop is designed for security practitioners working in network operators, ISPs, CERTs/CSIRTs, SOCs, and related technical teams.

Using realistic scenarios involving ransomware, infostealers, and espionage-style activity, participants will explore how modern attacks unfold and how organisations can improve their ability to prevent, detect, investigate, and respond to cyber incidents.

The workshop will combine lectures, demonstrations, hands-on labs, group discussions, and scenario-based exercises. It will also introduce relevant references such as NIST CSF 2.0, incident response guidance, MITRE ATT&CK, Sigma, and CSIRT service concepts.

Target Audience

This workshop is suitable for:

- Network operator and ISP security teams
- CERT/CSIRT staff
- SOC analysts
- Security analysts
- System and network administrators with security responsibilities
- Incident response team members

Pre-requisites

Participants should have basic knowledge of networking, operating systems, and cybersecurity concepts.

Some experience with Linux/Unix command line, log files, SSH, DNS, IP addressing, and basic incident response concepts will be helpful.

Workshop Format

The workshop will include:

- Instructor-led presentations
- Tool demonstrations
- Hands-on labs
- Group exercises
- Scenario-based discussions
- A final tabletop-style exercise

Workshop Agenda

Day 1 — Rethinking Cyber Defence

Day 1 focuses on the foundations of practical cyber defence. Participants will examine how organisations can understand critical assets, reduce exposure, improve visibility, and prepare for incidents.

Key topics include:

- Current threat landscape: ransomware, infostealers, and espionage-style activity
- Rethinking cyber defence using practical frameworks such as NIST CSF 2.0
- Crown jewels and critical dependencies
- Asset management and external exposure
- Vulnerability management and prioritisation
- Authentication, MFA, SSO, Active Directory, and remote access risks
- DNS filtering and DNS visibility
- Backup and recovery readiness
- EDR, SIEM, logging, supply chain, and policy considerations

Practical activities may include crown jewel mapping, external exposure review, DNS log analysis, and identity risk prioritisation.

Day 2 — Incident Response and Investigation

Day 2 focuses on practical incident response and investigation. Participants will learn how to approach an incident, identify useful evidence, build a timeline, and understand what happened during a compromise.

Key topics include:

- Incident response process and triage
- Evidence sources during ransomware and infostealer investigations
- Endpoint investigation concepts
- Windows event log analysis
- Linux/Unix artefact collection and triage
- DNS, proxy, and network evidence
- Timeline building
- Identifying affected hosts, accounts, and indicators
- Scoping and containment considerations

Possible tools and materials include Hayabusa, UAC, CyberChef, prepared endpoint logs, DNS logs, proxy logs, and simulated incident artefacts.

Day 3 — Detection Engineering and Monitoring

Day 3 focuses on turning investigation findings into repeatable detection and monitoring. Participants will explore how to develop detection ideas, map activity to MITRE ATT&CK, write basic Sigma-style rules, and understand how SIEM and network detection tools support security operations.

Key topics include:

- From incident findings to detection logic
- MITRE ATT&CK for behaviour mapping
- Introduction to Sigma rules
- SIEM concepts and detection lifecycle
- Wazuh or similar open-source SIEM concepts
- Network detection using IDS or network telemetry
- DNS and flow-based detection for network operators
- Honeypots and honeytokens
- False positives, tuning, and detection coverage

Practical activities may include ATT&CK mapping, Sigma rule exercises, SIEM alert review, IDS/network log analysis, and simple deception use cases.

Day 4 — Threat Intelligence Sharing and Response Coordination

Day 4 focuses on operationalising incident response and coordination. Participants will explore how threat intelligence can be shared, how incident cases can be managed, how CSIRT services can be structured, and how organisations coordinate during serious cyber incidents.

Key topics include:

- Threat intelligence concepts for operational teams
- Indicators, context, and actionable intelligence
- Threat intelligence sharing using MISP or similar platforms
- Incident case management using IRIS or similar tools
- CSIRT services and responsibilities
- Coordination with customers, national CERTs, peers, vendors, and other stakeholders
- Incident reporting and communication
- Lessons learned and improvement planning

- Tabletop exercise based on a realistic cyber incident scenario

Practical activities may include reviewing or creating MISP events, working through an incident case, CSIRT service mapping, and a final tabletop-style exercise.

Requirements

Participants will need their own laptop or computer with:

- Internet browser
- SSH client
- PDF/document viewer

Recommended but not mandatory:

- Ability to run Docker or virtual machines, if local labs are used

A remote or pre-prepared lab environment may be provided to reduce setup time. The workshop will use safe simulated datasets, logs, and incident artefacts. Live malware will not be used.