DEFENSIVE

Threat Intelligence Operations

Collection, Analysis, and Operationalising Cyber Threat Intelligence

Practical cyber threat intelligence guide covering the intelligence cycle, OSINT collection, dark web monitoring, IoC management, STIX/TAXII, threat actor profiling, and integrating CTI into SOC and security operations.

HORIZONSHIELD

LEVEL	READ TIME	SERIES
Advanced	40 min	Book 18 of 22

Contents

CHAPTER 01

Threat Intelligence Fundamentals

Threat intelligence transforms raw data about threats into actionable knowledge that drives security decisions. The distinction between data, information, and intelligence is not semantic — it defines whether your security team is reacting to events or anticipating them.

Intelligence Type	Audience	Examples	Lifespan
Strategic	Board, CISO, executives	Threat landscape reports, geopolitica…	Months to years
Operational	Security managers, IR teams	Campaign analysis, actor TTPs	Weeks to months
Tactical	SOC analysts, detection engineers	TTPs, malware behaviour, attack pat…	Days to weeks
Technical	SIEM, firewall, EDR tools	IP addresses, domains, file hashes, …	Hours to days

i The intelligence cycle — Direction, Collection, Processing, Analysis, Dissemination, Feedback — is the structured process that turns raw data into finished intelligence. The most commonly skipped step is Direction: defining specific intelligence requirements. Without clear requirements, CTI teams collect everything and deliver nothing useful.

Most organisations consume threat intelligence as IP blocklists and file hashes — technical-level indicators with lifespans measured in hours. This is the lowest-value intelligence type and the easiest for sophisticated actors to change. The highest-value intelligence describes attacker TTPs (Tactics, Techniques, and Procedures) at the MITRE ATT&CK level — these change slowly, survive infrastructure takedowns, and directly drive detection engineering.

CHAPTER 02

OSINT for Threat Intelligence

This chapter covers osint for threat intelligence — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

Open-source collection techniques for CTI analysts. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 03

Dark Web & Underground Monitoring

This chapter covers dark web & underground monitoring — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

Safely monitoring threat actor forums, markets, and channels. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 04

Indicator of Compromise Management

This chapter covers indicator of compromise management — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

IoC lifecycle, confidence scoring, and expiry management. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 05

STIX / TAXII & Intelligence Sharing

This chapter covers stix / taxii & intelligence sharing — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

Structured threat intelligence exchange and sharing platforms. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 06

Threat Actor Profiling

This chapter covers threat actor profiling — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

TTPs, attribution methodology, and MITRE ATT&CK actor mapping. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

CHAPTER 07

Operationalising CTI in the SOC

This chapter covers operationalising cti in the soc — providing practical guidance, reference tables, and implementation frameworks for security practitioners.

Integrating intelligence into detection, hunting, and response workflows. The techniques and controls described here are drawn from industry standards, real-world engagements, and operational experience. Apply them in the context of your specific environment, risk appetite, and regulatory obligations.

HS

HORIZONSHIELD ORIGINALS

Complete Security Library

Practitioner-written guides for real-world security implementation.

AVAILABLE IN THIS SERIES

01	SMB Cybersecurity Guide	02	Penetration Testing Checklist
03	Incident Response Playbook	04	DORA Compliance Guide
05	Cloud Security Hardening	06	Zero Trust Architecture
07	Threat Hunting & SOC Operations	08	DevSecOps Implementation
09	Web Application Security	10	Network Security Fundamentals
11	Linux & Systems Security	12	Social Engineering & Human Hacking
13	Malware Analysis & Reverse Engineer…	14	Digital Forensics & Incident Respon…
15	Applied Cryptography	16	Compliance Audit & Risk Management
17	Identity & Access Management	18	**Threat Intelligence Operations**
19	Red Team Operations	20	OT & ICS Security
21	Privacy Engineering & Data Protecti…	22	AI Security & LLM Threats

horizonshield.net/library

Download all 22 books · Access hands-on labs · Track your progress

Published Q1 2026 · Updated annually