ThIRU Essentials Platform

AI-Enabled SOC Training Curriculum

10-Week Self-Hosted Learning Programme

Modules 1 – 9 | Covering IDAM, EDR, Phishing, DLP, SIRP, Compliance & Capstone Project

ThIRU Labs | 2025

Duration	Delivery Mode	Level
10 Weeks	Self-Hosted / Online	Intermediate–Advanced

Table of Contents

1 Programme Overview & Structure 4
1.1 Programme Design Principles 4
1.2 Programme Structure at a Glance 4
1.3 Time Commitment 5
2 Prerequisites & Platform Access 5
2.1 Learner Prerequisites 5
2.2 Platform Requirements 5
2.3 Session 1.1 — The Modern Cybersecurity Landscape (3 hours) 6
2.4 Session 1.2 — Zero Trust Architecture Deep Dive (3 hours) 6
2.5 Self-Study (2 hours) 7
2.6 Key Topics Covered 7
2.7 Session 2.1 — IDAM Risks & Identity Governance (3 hours) 8
2.8 Session 2.2 — ThIRU IDAM Configuration Lab (4 hours) 8
2.9 Self-Study (3 hours) 9
2.10 Lab Deliverable — Week 2 9
2.11 Session 3.1 — EDR Concepts & Threat Landscape (3 hours) 10
2.12 Session 3.2 — ThIRU EDR Deployment & Operations Lab (4 hours) 10
2.13 Self-Study (1 hour) 11
2.14 Session 4.1 — Phishing Threat Education (3 hours) 12
2.15 Session 4.2 — ThIRU Phishing Lab (3 hours) 12
2.16 Self-Study (2 hours) 13
2.17 Session 5.1 — Endpoint DLP Concepts (2.5 hours) 14
2.18 Session 5.2 — ThIRU Endpoint DLP Lab (4 hours) 14
2.19 Self-Study (1.5 hours) 15
2.20 Session 6.1 — Network & SaaS DLP Risk Landscape (2.5 hours) 16
2.21 Session 6.2 — ThIRU Network DLP Lab (4 hours) 16
2.22 Self-Study (1.5 hours) 17
2.23 Session 7.1 — SIRP & SOC Organisation (3 hours) 18
2.24 Session 7.2 — ThIRU SIRP & SOC Desk Lab (3.5 hours) 18
2.25 Self-Study (1.5 hours) 19
2.26 Session 8.1 — Compliance Frameworks & SOC Evidence (3 hours) 20
2.27 Session 8.2 — ThIRU Dashboard & Compliance Reporting Lab (4 hours) 20
2.28 Self-Study (1 hour) 21
2.29 Week 9 — Build, Configure & Simulate (12 hours) 22

2.30 Week 10 — Report, Present & Assess (8 hours) 22
2.31 Capstone Report Requirements 23
3 Assessment Strategy & Grading Rubric 24
3.1 Assessment Structure 24
3.2 Grading Scale 24
4 Recommended Resources & Reading 25
4.1 Core Platform Documentation 25
4.2 Standards & Frameworks 25
4.3 Regulatory References 25
4.4 Recommended Reading 25
4.5 Online Resources 25

1 Programme Overview & Structure

This 10-week self-hosted curriculum delivers end-to-end training in AI-enabled Security Operations Centre (SOC) capabilities using the ThIRU Essentials Platform. The programme is structured to progressively build competencies from foundational cybersecurity concepts through to advanced hands-on operations, culminating in a real-world capstone project.

1.1 Programme Design Principles

- Theory-first, practice-led: Each week begins with conceptual grounding followed by platform labs
- Cumulative learning: Each module builds on the previous, reinforcing a holistic security posture
- Scenario-based: Real-world threat scenarios are embedded throughout to drive contextual understanding
- AI-augmented: AI analyst capabilities within ThIRU are integrated into every module
- Compliance-aligned: Content maps to ISO 27001, NIST CSF, GDPR, SOC 2, and Zero Trust frameworks

1.2 Programme Structure at a Glance

Session	Duration	Format	Topic / Activity
Week 1	8 hrs	**Lecture + Lab**	Module 1 — Cybersecurity Fundamentals, SOC Monitoring & Zero Trust
Week 2	10 hrs	**Lecture + Lab**	Module 2 — IDAM Risks & ThIRU IDAM Configuration
Week 3	8 hrs	**Lecture + Lab**	Module 3 — Endpoint Detection & Response (EDR)
Week 4	8 hrs	**Lecture + Lab**	Module 4 — Phishing Awareness & ThIRU Phishing Protection
Week 5	8 hrs	**Lecture + Lab**	Module 5 — Endpoint DLP: Application & Execution Controls
Week 6	8 hrs	**Lecture + Lab**	Module 6 — Network & SaaS Data Leakage Prevention
Week 7	8 hrs	**Lecture + Lab**	Module 7 — SIRP, Ticketing & SOC Organisation / DevSecOps
Week 8	8 hrs	**Lecture + Lab**	Module 8 — SOC Dashboards & Multi-Framework Compliance Reporting
Week 9	12 hrs	**Project Lab**	Module 9 — Capstone Project: Setup, Simulation & Operations
Week 10	8 hrs	**Project + Assessment**	Module 9 cont. — Reporting, Presentation & Final Assessment

1.3 Time Commitment

- Total programme hours: approximately 86 hours
- Recommended weekly commitment: 8–12 hours (including self-study)
- Each week: 2 × instructor-led sessions + independent lab time + knowledge checks

2 Prerequisites & Platform Access

2.1 Learner Prerequisites

- Basic understanding of networking concepts (TCP/IP, DNS, HTTP/S)
- Familiarity with Windows and/or Linux operating environments
- Introductory knowledge of information security concepts
- Completion of any vendor-neutral security awareness programme is advantageous

2.2 Platform Requirements

- Active ThIRU Essentials Platform licence (Trainer + Student accounts)
- Access to ThIRU IDAM, ThIRU EDR, ThIRU Phishing, and SOC Dashboard modules
- Lab environment: Minimum 2 test endpoints (Windows 10/11), 1 test server
- Browser: Chrome or Edge (latest), with internet access for cloud-connected labs
- Admin credentials to the ThIRU tenant for organisation setup exercises

Platform Access Note

Each student cohort should be provisioned with a dedicated ThIRU tenant or sandbox environment prior to Week 1. Trainers should complete the 'Organisation Bootstrap' configuration (covered in Module 2) before the first live session to ensure all students can enrol smoothly. Contact ThIRU Labs support for trainer sandbox provisioning.

WEEK 1
Module 1

Cybersecurity, SOC Monitoring & Zero Trust Architecture

This foundational week establishes the conceptual and operational context for the entire programme. Students will understand the SOC as a business function, explore the cyber risk landscape, and examine Zero Trust Architecture as the strategic framework underpinning all subsequent modules.

Learning Outcomes

- ✓ Define the role and mandate of a modern Security Operations Centre (SOC)
- ✓ Identify and classify current cyber threats relevant to enterprise environments
- ✓ Articulate the principles of Zero Trust Architecture and explain why perimeter security is insufficient
- ✓ Navigate the ThIRU Essentials Platform and understand the integrated dashboard
- ✓ Map cybersecurity controls to business risk categories

2.3 Session 1.1 — The Modern Cybersecurity Landscape (3 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	**Lecture**	The evolution of cyber threats: from viruses to APTs and ransomware-as-a-service
0:45–1:15	30 min	**Lecture**	Cyber risk management: threat, vulnerability, likelihood, and impact
1:15–1:45	30 min	**Lecture**	Understanding the SOC: tier structure, SIEM, SOAR, and AI analyst integration
1:45–2:15	30 min	**Discussion**	Case study: anatomy of a real-world breach and how a SOC should have responded
2:15–3:00	45 min	**Lab**	ThIRU Platform orientation — navigating the unified SOC dashboard, alert feeds, geo-map

2.4 Session 1.2 — Zero Trust Architecture Deep Dive (3 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	**Lecture**	Zero Trust principles: verify explicitly, least-privilege access, assume breach
0:45–1:30	45 min	**Lecture**	Zero Trust pillars: identity, devices, networks, applications, data, infrastructure
1:30–2:00	30 min	**Lecture**	NIST SP 800-207 Zero Trust Architecture overview and implementation tenets
2:00–2:30	30 min	**Workshop**	Mapping ThIRU platform modules to Zero Trust pillars (group activity)

Session	Duration	Format	Topic / Activity
2:30–3:00	30 min	**Knowledge Check**	Quiz: Week 1 concepts + reflective journal entry

2.5 Self-Study (2 hours)

- Read: NIST Cybersecurity Framework 2.0 — Executive Summary
- Read: ThIRU Platform User Guide — Chapter 1: SOC Overview
- Complete: ThIRU platform orientation checklist (provided in LMS)
- Watch: CISA Zero Trust Architecture explainer video (linked in LMS)

2.6 Key Topics Covered

- Cyber kill chain and MITRE ATT&CK framework introduction
- CIA Triad (Confidentiality, Integrity, Availability) in operational context
- SOC tiers: L1 Analyst, L2 Responder, L3 Threat Hunter, SOC Manager
- ThIRU AI Analyst: automated alert triage, false positive reduction, threat scoring
- Zero Trust vs traditional perimeter security model

WEEK 2
Module 2

Identity & Access Management (IDAM) Risks & ThIRU IDAM

Identity is the new perimeter. This week provides a comprehensive treatment of IDAM risks and hands-on configuration of ThIRU IDAM — setting up an organisation, defining roles, establishing RBAC, configuring SSO, and generating UEBA reporting.

Learning Outcomes

- ✓ Identify and explain the top IDAM risks including credential theft, privilege escalation, and insider threats
- ✓ Set up a complete organisation within ThIRU IDAM with defined role hierarchies
- ✓ Create and manage employee, contractor, supplier, and customer identity profiles
- ✓ Configure Role-Based Access Control (RBAC) for enterprise applications
- ✓ Set up Single Sign-On (SSO) using SAML 2.0 / OIDC within ThIRU IDAM
- ✓ Generate and interpret UEBA (User and Entity Behaviour Analytics) reports

2.7 Session 2.1 — IDAM Risks & Identity Governance (3 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	**Lecture**	Top IDAM risks: credential stuffing, MFA bypass, lateral movement, over-privileged accounts
0:45–1:15	30 min	**Lecture**	Identity governance: joiner–mover–leaver lifecycle, access reviews, SoD conflicts
1:15–2:00	45 min	**Lecture**	RBAC, ABAC, and PAM: principles, patterns, and pitfalls
2:00–2:30	30 min	**Lecture**	Regulatory obligations: GDPR, ISO 27001 A.9, NIST AC controls
2:30–3:00	30 min	**Discussion**	Case study: SolarWinds and the identity attack vector — lessons learned

2.8 Session 2.2 — ThIRU IDAM Configuration Lab (4 hours)

Session	Duration	Format	Topic / Activity
0:00–0:30	30 min	**Demo**	ThIRU IDAM overview: architecture, connectors, and identity store
0:30–1:30	60 min	**Lab**	Lab 2A: Create organisation, define departments, import 20 users (employees, contractors, suppliers, customers)
1:30–2:30	60 min	**Lab**	Lab 2B: Assign roles and configure RBAC — application-level permissions matrix
2:30–3:15	45 min	**Lab**	Lab 2C: Configure SSO with a test application using SAML 2.0

Session	Duration	Format	Topic / Activity
3:15–4:00	45 min	**Lab**	Lab 2D: Run UEBA baseline report — identify anomalous login behaviour, export findings

2.9 Self-Study (3 hours)

- Read: ThIRU IDAM Administration Guide (Chapters 2–4)
- Practice: Complete RBAC matrix worksheet for a 50-user mock organisation
- Watch: Recorded demo — ThIRU SSO wizard walkthrough
- Research: Compare SAML 2.0 vs OAuth 2.0 / OIDC — document key differences

2.10 Lab Deliverable — Week 2

Assessment Task 2

Students must submit a 2-page IDAM configuration report documenting:

1. Organisation structure and user categories created in ThIRU IDAM
2. RBAC matrix with at least 3 roles, 3 applications, and permission rationale
3. SSO configuration screenshots with verification evidence
4. UEBA report summary highlighting at least 2 anomalies and recommended mitigations

WEEK 3 Module 3 Endpoint Detection & Response (EDR)

Endpoints remain the primary attack surface in enterprise environments. This week covers the full EDR lifecycle — from understanding threats, deploying ThIRU EDR, interpreting telemetry, to active risk management and response.

Learning Outcomes

- ✓ Explain EDR risks including fileless malware, living-off-the-land attacks, and ransomware behaviours
- ✓ Deploy and configure ThIRU EDR agents on Windows endpoints
- ✓ Interpret EDR telemetry data: process trees, network connections, file events, and registry activity
- ✓ Configure automated monitoring rules and response playbooks
- ✓ Classify and manage EDR-originated alerts through the ThIRU SOC dashboard

2.11 Session 3.1 — EDR Concepts & Threat Landscape (3 hours)

Session	Duration	Format	Topic / Activity
0:00–0:50	50 min	**Lecture**	The endpoint threat landscape: malware families, ransomware, fileless attacks, LoLBAS
0:50–1:30	40 min	**Lecture**	EDR vs AV vs XDR: capabilities comparison and when each is appropriate
1:30–2:15	45 min	**Lecture**	EDR telemetry data types: process, network, file, registry, memory — what each reveals
2:15–2:45	30 min	**Demo**	ThIRU EDR: architecture, agent deployment, and alert console walkthrough
2:45–3:00	15 min	**Q&A**	Open discussion: challenges in EDR tuning and reducing false positives

2.12 Session 3.2 — ThIRU EDR Deployment & Operations Lab (4 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	**Lab**	Lab 3A: Deploy ThIRU EDR agent on test endpoint — verify telemetry ingestion
0:45–1:45	60 min	**Lab**	Lab 3B: Configure detection rules — define suspicious process rules, exclusions, and severity mappings
1:45–2:30	45 min	**Lab**	Lab 3C: Simulate a malware execution (benign test payload) — observe and interpret alert data
2:30–3:15	45 min	**Lab**	Lab 3D: Investigate an alert — build process tree, pivot to network connections, document findings

Session	Duration	Format	Topic / Activity
3:15–4:00	45 min	**Lab**	Lab 3E: Create automated response rule — isolate endpoint on detection, notify SOC via SIRP

2.13 Self-Study (1 hour)

- Read: MITRE ATT&CK Enterprise Matrix — review Execution, Persistence, and Defence Evasion tactics
- Complete: ThIRU EDR alert triage exercise (sample alert set provided in LMS)

WEEK 4
Module 4

Phishing Awareness & Protection

Phishing remains the single most prevalent initial access vector. This week delivers both the awareness education component and the technical protection layer using ThIRU Phishing, including simulated attack campaigns and defensive configuration.

Learning Outcomes

- ✓ Recognise the full spectrum of phishing attack types: spear phishing, whaling, vishing, smishing, BEC
- ✓ Explain the psychological manipulation techniques used in phishing attacks
- ✓ Configure and launch a simulated phishing campaign using ThIRU Phishing
- ✓ Interpret phishing campaign results and identify high-risk user segments
- ✓ Deploy technical phishing countermeasures: email filtering, link scanning, DMARC/SPF/DKIM
- ✓ Design and deliver targeted security awareness content based on simulation results

2.14 Session 4.1 — Phishing Threat Education (3 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	**Lecture**	Phishing taxonomy: email, spear, whaling, vishing, smishing, quishing (QR), BEC fraud
0:45–1:30	45 min	**Lecture**	Social engineering psychology: authority, urgency, scarcity, social proof, familiarity
1:30–2:00	30 min	**Workshop**	Phishing email analysis: identify red flags in 10 sample emails (group activity)
2:00–2:30	30 min	**Lecture**	Technical countermeasures: DMARC, SPF, DKIM, email gateway filtering, safe links
2:30–3:00	30 min	**Discussion**	Building a phishing-resilient culture: awareness training cadence and metrics

2.15 Session 4.2 — ThIRU Phishing Lab (3 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	**Lab**	Lab 4A: Configure ThIRU Phishing — set up campaign, choose template, define target user group
0:45–1:30	45 min	**Lab**	Lab 4B: Launch simulated phishing campaign — observe delivery, open rates, link clicks, credential harvests
1:30–2:15	45 min	**Lab**	Lab 4C: Analyse campaign results dashboard — identify at-risk users, departments, time patterns

Session	Duration	Format	Topic / Activity
2:15–3:00	45 min	**Lab**	Lab 4D: Configure phishing protection rules in ThIRU — automated quarantine, alert generation, user notification

2.16 Self-Study (2 hours)

- Read: APWG Phishing Activity Trends Report (latest edition — linked in LMS)
- Practice: ThIRU Phishing template library — create 2 custom templates for your simulated organisation
- Research: Evaluate 3 phishing-resistant MFA options — document pros/cons

WEEK 5
Module 5

Endpoint Data Loss Prevention (DLP)

This module addresses the endpoint layer of data loss prevention — controlling what applications run, what can be installed, what can be executed, and how browsers behave. This is the first of two DLP modules, focusing exclusively on the host-based enforcement plane.

Learning Outcomes

- ✓ Explain the endpoint DLP risk landscape including shadow IT, unauthorised software, and insider data exfiltration
- ✓ Configure application whitelisting and blacklisting policies in ThIRU DLP
- ✓ Block local application execution using process control rules
- ✓ Restrict downloads and software installation on managed endpoints
- ✓ Manage browser extensions and enforce approved browser policies
- ✓ Configure browser management controls: allowed sites, blocked categories, safe browsing enforcement

2.17 Session 5.1 — Endpoint DLP Concepts (2.5 hours)

Session	Duration	Format	Topic / Activity
0:00–0:40	40 min	**Lecture**	Endpoint DLP risk landscape: data exfiltration paths, shadow IT, removable media, unauthorised apps
0:40–1:10	30 min	**Lecture**	Application control strategies: allowlisting vs denylisting — risk/usability tradeoffs
1:10–1:40	30 min	**Lecture**	Browser risk: extensions, plugins, password managers, developer tools, incognito bypass
1:40–2:10	30 min	**Lecture**	Regulatory context: ISO 27001 A.8, GDPR Art.32, NIST PR.DS controls
2:10–2:30	20 min	**Discussion**	Balancing security with user productivity — the cost of over-restriction

2.18 Session 5.2 — ThIRU Endpoint DLP Lab (4 hours)

Session	Duration	Format	Topic / Activity
0:00–0:50	50 min	**Lab**	Lab 5A: Configure application whitelist — define approved apps, hash verification, publisher rules
0:50–1:40	50 min	**Lab**	Lab 5B: Block specific local applications — test enforcement, review alert generation in SOC dashboard
1:40–2:30	50 min	**Lab**	Lab 5C: Block software downloads and installation — configure file-type and source restrictions

Session	Duration	Format	Topic / Activity
2:30–3:20	50 min	**Lab**	Lab 5D: Browser management — block unapproved extensions, enforce safe browsing, restrict developer tools
3:20–4:00	40 min	**Lab**	Lab 5E: Review and interpret ThIRU DLP alert stream — triage and escalate policy violations

2.19 Self-Study (1.5 hours)

- Read: CIS Benchmark for Endpoint Security — Application Control section
- Design: Draft an application allowlist policy for a 50-user financial services company

WEEK 6
Module 6

Data Leakage Prevention — Network & SaaS Layer

This module extends DLP coverage to the network and cloud SaaS layer — addressing the increasingly common exfiltration paths via clipboard operations, web uploads, messaging platforms (WhatsApp), and SaaS applications. This is the operational lynchpin of modern data governance.

Learning Outcomes

- ✓ Identify the primary network and cloud-based data leakage vectors in enterprise environments
- ✓ Configure cut-and-paste blocking policies to prevent clipboard-based exfiltration
- ✓ Control web uploads and downloads via proxy and DLP inspection rules
- ✓ Block or monitor data transfers via WhatsApp Web and other messaging-based SaaS applications
- ✓ Implement upload/download controls for major SaaS platforms (Google Drive, OneDrive, Dropbox)
- ✓ Interpret and respond to DLP alerts from the ThIRU unified dashboard

2.20 Session 6.1 — Network & SaaS DLP Risk Landscape (2.5 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	Lecture	SaaS exfiltration vectors: cloud storage sync, messaging apps, webmail, screen capture
0:45–1:15	30 min	Lecture	Clipboard exfiltration: cut/copy/paste as a covert channel — detection and prevention
1:15–1:50	35 min	Lecture	WhatsApp Web, Telegram, and consumer messaging as enterprise data leak vectors
1:50–2:20	30 min	Lecture	CASB principles and how ThIRU DLP integrates SaaS visibility and control
2:20–2:30	10 min	Q&A	Open Q&A on SaaS risk management in BYOD and hybrid work environments

2.21 Session 6.2 — ThIRU Network DLP Lab (4 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	Lab	Lab 6A: Configure clipboard blocking rules — test block vs monitor mode on sensitive content types
0:45–1:30	45 min	Lab	Lab 6B: Web upload/download control — configure rules for file type, size, destination domain
1:30–2:15	45 min	Lab	Lab 6C: Block WhatsApp Web and Telegram — category-based URL filtering + application signature rules

Session	Duration	Format	Topic / Activity
2:15–3:00	45 min	**Lab**	Lab 6D: SaaS upload monitoring — configure ThIRU for Google Drive and OneDrive upload visibility
3:00–3:45	45 min	**Lab**	Lab 6E: Simulate a data exfiltration scenario — attempt upload to personal cloud; observe and triage alerts
3:45–4:00	15 min	**Review**	Debrief: what the simulation revealed; policy tuning recommendations

2.22 Self-Study (1.5 hours)

- Read: Gartner CASB Market Guide summary (linked in LMS)
- Research: 3 documented case studies of SaaS-based data breaches — summarise for class discussion

WEEK 7
Module 7

Security Incident Reporting & SOC Operations (SIRP)

Effective incident management is the operational heartbeat of a SOC. This week covers the full Security Incident Reporting & Response Platform (SIRP) lifecycle, SOC organisational structure, and the critical DevSecOps function that bridges security and engineering.

Learning Outcomes

- ✓ Describe the end-to-end security incident lifecycle from detection to closure
- ✓ Configure and operate the ThIRU SIRP ticketing system for incident triage and escalation
- ✓ Design a SOC organisational structure with defined roles and responsibilities
- ✓ Explain the role and key responsibilities of a DevSecOps function within an enterprise
- ✓ Apply incident severity classification criteria to real-world scenarios
- ✓ Generate and interpret incident metrics from the ThIRU SIRP dashboard

2.23 Session 7.1 — SIRP & SOC Organisation (3 hours)

Session	Duration	Format	Topic / Activity
0:00–0:50	50 min	**Lecture**	Incident lifecycle: identification, containment, eradication, recovery, lessons learned (NIST SP 800-61)
0:50–1:30	40 min	**Lecture**	SIRP and ticketing: escalation paths, SLA definitions, severity matrix, stakeholder communication
1:30–2:10	40 min	**Lecture**	SOC organisation: roles — L1/L2/L3 analyst, threat hunter, SOC manager, CISO interface
2:10–2:50	40 min	**Lecture**	DevSecOps: definition, responsibilities, shift-left security, CI/CD pipeline security, SAST/DAST
2:50–3:00	10 min	**Discussion**	Where does DevSecOps sit in a SOC org chart? Mapping responsibilities and escalation

2.24 Session 7.2 — ThIRU SIRP & SOC Desk Lab (3.5 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	**Lab**	Lab 7A: Configure ThIRU SIRP — define incident categories, severity levels, and assignment rules
0:45–1:30	45 min	**Lab**	Lab 7B: Create and manage incident tickets — log a simulated phishing incident end-to-end
1:30–2:15	45 min	**Lab**	Lab 7C: Escalation workflow — configure auto-escalation rules, SLA breach notifications
2:15–3:00	45 min	**Lab**	Lab 7D: SOC desk scenario — manage 5 concurrent incidents; prioritise, assign, and close

Session	Duration	Format	Topic / Activity
3:00–3:30	30 min	**Workshop**	Design a SOC org chart for a 200-person organisation using RACI framework

2.25 Self-Study (1.5 hours)

- Read: NIST SP 800-61 Rev.2 — Computer Security Incident Handling Guide (summary)
- Template: Complete the SOC RACI template worksheet for your simulated organisation

WEEK 8
Module 8

Reporting Dashboard & Compliance Frameworks

SOC value must be demonstrated to leadership through clear, evidence-based reporting. This week covers the ThIRU reporting dashboard in depth and maps platform outputs to the five major compliance frameworks: ISO 27001, NIST CSF, GDPR, SOC 2, and controls auditing.

Learning Outcomes

- ✓ Configure and customise the ThIRU SOC reporting dashboard for executive and operational audiences
- ✓ Map ThIRU platform controls and alert data to ISO 27001:2022 Annex A controls
- ✓ Align platform monitoring outputs with NIST CSF 2.0 functions and categories
- ✓ Identify GDPR Article 32 controls evidenced by ThIRU platform operations
- ✓ Produce a SOC 2 Type II audit evidence pack from ThIRU platform data
- ✓ Conduct an internal controls audit using the ThIRU compliance reporting module

2.26 Session 8.1 — Compliance Frameworks & SOC Evidence (3 hours)

Session	Duration	Format	Topic / Activity
0:00–0:45	45 min	**Lecture**	ISO 27001:2022 — Annex A control mapping relevant to SOC operations (A.8, A.9, A.10, A.12, A.16)
0:45–1:20	35 min	**Lecture**	NIST CSF 2.0 — Identify, Protect, Detect, Respond, Recover: SOC contributions to each function
1:20–1:55	35 min	**Lecture**	GDPR Art.32 — Technical and organisational measures: what ThIRU provides as evidence
1:55–2:30	35 min	**Lecture**	SOC 2 Type I & Type II — Trust Service Criteria, audit evidence, control testing
2:30–3:00	30 min	**Workshop**	Control mapping exercise: assign ThIRU platform features to NIST CSF categories (group)

2.27 Session 8.2 — ThIRU Dashboard & Compliance Reporting Lab (4 hours)

Session	Duration	Format	Topic / Activity
0:00–0:50	50 min	**Lab**	Lab 8A: Configure ThIRU dashboard — customise widgets, KPIs, alert trends, geo-map for executive view
0:50–1:40	50 min	**Lab**	Lab 8B: Generate ISO 27001 compliance report — map controls to platform data, identify gaps
1:40–2:20	40 min	**Lab**	Lab 8C: GDPR evidence report — produce data processing log, access control evidence, incident log
2:20–3:00	40 min	**Lab**	Lab 8D: SOC 2 evidence pack — compile access logs, change records, alert dispositions

Session	Duration	Format	Topic / Activity
3:00–4:00	60 min	**Lab**	Lab 8E: Internal controls audit simulation — run ThIRU audit module, score control effectiveness, produce findings report

2.28 Self-Study (1 hour)

- Download and review: ISO 27001:2022 Annex A control list (reference copy in LMS)
- Prepare: Identify 5 controls from your simulated organisation that ThIRU can evidence — document for capstone

WEEK 9–10
Module 9

Capstone Project — ThIRU Essentials Full Platform Deployment

The capstone project integrates all nine modules into a comprehensive real-world simulation. Students will build a complete security programme on ThIRU Essentials from the ground up, simulate live threats, respond through the SOC, and produce a board-quality security report.

Learning Outcomes

- ✓ Deploy a complete ThIRU Essentials environment from scratch — IDAM, EDR, Phishing, DLP, and SIRP
- ✓ Simulate a multi-vector attack scenario: malware execution + phishing campaign simultaneously
- ✓ Operate the SOC dashboard as an analyst — triage, investigate, escalate, and resolve incidents
- ✓ Generate a comprehensive compliance and security posture report from the dashboard
- ✓ Present findings in a structured executive briefing format

2.29 Week 9 — Build, Configure & Simulate (12 hours)

Session	Duration	Format	Topic / Activity
Phase 1	3 hrs	**Lab**	Organisation Setup: Create new ThIRU tenant — IDAM organisation, 30 users across 4 roles, RBAC, SSO
Phase 2	2 hrs	**Lab**	Security Stack Deployment: Deploy EDR on all test endpoints, configure DLP policies, activate Phishing module
Phase 3	2 hrs	**Lab**	SIRP Configuration: Define incident categories, severity matrix, escalation rules, SOC team assignments
Phase 4	2.5 hrs	**Lab**	Malware Simulation: Execute benign test payload on 2 endpoints — monitor, triage, and respond to EDR alerts
Phase 5	2.5 hrs	**Lab**	Phishing Simulation: Launch targeted phishing campaign — observe results, configure protective rules, notify affected users

2.30 Week 10 — Report, Present & Assess (8 hours)

Session	Duration	Format	Topic / Activity
Phase 6	3 hrs	**Lab + Report**	Dashboard Reporting: Configure executive dashboard, generate ISO 27001/NIST/GDPR compliance reports, export evidence
Phase 7	3 hrs	**Written**	Capstone Report: Write comprehensive 15–20 page security posture report (template in LMS)

Session	Duration	Format	Topic / Activity
Phase 8	2 hrs	**Presentation**	Final Presentation: 15-minute executive briefing per student/group + peer Q&A

2.31 Capstone Report Requirements

Capstone Deliverable (35% of Final Grade)

The capstone report must include the following sections:

5. Executive Summary — 1 page overview of security posture and key findings
6. Organisation Profile — IDAM configuration, roles, and user count
7. Threat Simulation Results — EDR alert analysis for malware simulation
8. Phishing Campaign Analysis — Click rates, high-risk users, mitigations applied
9. DLP Controls Summary — Policies configured, alerts generated, data exfiltration prevented
10. Incident Management Log — All SIRP tickets raised, classification, resolution times
11. Compliance Posture — Mapped to ISO 27001, NIST CSF, GDPR with control evidence
12. Risk Register — Top 10 residual risks with likelihood/impact ratings and treatment plans
13. Recommendations — Prioritised action plan for security programme improvement

3 Assessment Strategy & Grading Rubric

3.1 Assessment Structure

Assessment Component	When	Format	Weight
Weekly Knowledge Checks (8 × quizzes, best 6 counted)	Weeks 1–8	Online quiz (20 min each)	**15%**
IDAM Lab Report (Module 2)	End of Week 2	Written report (2 pages)	**10%**
EDR Incident Investigation (Module 3)	End of Week 3	Alert analysis report	**10%**
Phishing Campaign Analysis (Module 4)	End of Week 4	Campaign findings report	**10%**
DLP Policy Design (Modules 5–6)	End of Week 6	Policy documentation	**10%**
SIRP Scenario Exercise (Module 7)	End of Week 7	Practical (observed)	**10%**
Capstone Project Report (Module 9)	End of Week 10	Report (15–20 pages)	**25%**
Capstone Presentation (Module 9)	Week 10	15-min presentation	**10%**

3.2 Grading Scale

Distinction	**Credit**	**Pass**	**Fail**
85–100%	70–84%	50–69%	Below 50%

4 Recommended Resources & Reading

4.1 Core Platform Documentation

- ThIRU Essentials Platform User Guide (v12+) — all modules
- ThIRU IDAM Administration & Configuration Guide
- ThIRU EDR Deployment & Tuning Manual
- ThIRU SOC Dashboard Reference Guide

4.2 Standards & Frameworks

- NIST SP 800-207: Zero Trust Architecture
- NIST SP 800-61 Rev.2: Computer Security Incident Handling Guide
- NIST Cybersecurity Framework 2.0
- ISO/IEC 27001:2022 — Information Security Management Systems
- ISO/IEC 27035: Information Security Incident Management
- MITRE ATT&CK Enterprise Framework (attack.mitre.org)
- CIS Controls v8 — Center for Internet Security

4.3 Regulatory References

- GDPR (EU) 2016/679 — General Data Protection Regulation
- SOC 2 Trust Service Criteria — AICPA
- Australian Privacy Act 1988 and Notifiable Data Breaches scheme

4.4 Recommended Reading

- The Practice of Network Security Monitoring — Richard Bejtlich
- Security Operations Center: Building, Operating, and Maintaining Your SOC — Joseph Muniz et al.
- Zero Trust Networks — Evan Gilman & Doug Barth
- The Web Application Hacker's Handbook (2nd Ed.) — Stuttard & Pinto

4.5 Online Resources

- CISA (Cybersecurity & Infrastructure Security Agency) — cisa.gov
- SANS Internet Stormcast — isc.sans.edu
- Krebs on Security — krebsonsecurity.com
- ACSC (Australian Cyber Security Centre) — cyber.gov.au

ThIRU Labs Pty Ltd

Unit 305, 65 Victor Cr, Narre Warren VIC 3805 | thirulab.com.au