TW

TERNARY WARD

SECURITY OPERATIONS / CLOUD DEFENCE / PRACTICAL PROOF

Capability-led security practice. Identity minimised. Evidence retained.

Security practitioner focused on security operations, incident investigation, vulnerability assessment, and remediation. Owns assigned security tickets from investigation through resolution and conducts third-party vulnerability assessments. This public brief intentionally omits personal contact details, employer history, precise location, and unsupported performance metrics.

OPERATING MODEL

01
Investigate
Validate signal, context, and evidence.

02
Assess
Evaluate exposure, impact, and control gaps.

03
Remediate
Own assigned work through verified resolution.

04
Improve
Turn findings into repeatable prevention.

SELECTED EVIDENCE

COMPLETED
Segmented blue-team lab
Proxmox, pfSense, Active Directory, domain-joined endpoints, realistic structure, and rollback snapshots.

COMPLETED
Wazuh SIEM deployment
Endpoint and network telemetry with Sysmon, file-integrity monitoring, pfSense events, and vulnerability coverage.

IN PROGRESS
Attack-to-detection workflow
ATT&CK-aligned; technique execution, telemetry validation, detection authoring, and coverage mapping.

WORKING TOOLKIT

Security operations
Microsoft Sentinel, Defender XDR, KQL, incident triage, phishing investigation

Vulnerability management
Tenable Nessus, assessment scoping, remediation tracking, validation

Cloud and identity
Microsoft Azure, Entra ID, Conditional Access, Intune

Lab and automation
Proxmox, pfSense, Wazuh, Sysmon, PowerShell, Git, Docker, Terraform

CREDENTIALS

CEH v12
ISC2 Certified in Cybersecurity
Microsoft SC-900
AWS Cloud Practitioner
CompTIA Network+
ITIL 4 Foundation

PRIVACY-RESPECTING CONTACT

Use the trusted application or introduction channel through which this portfolio was shared.

No direct PII / No tracking / No unsupported metrics