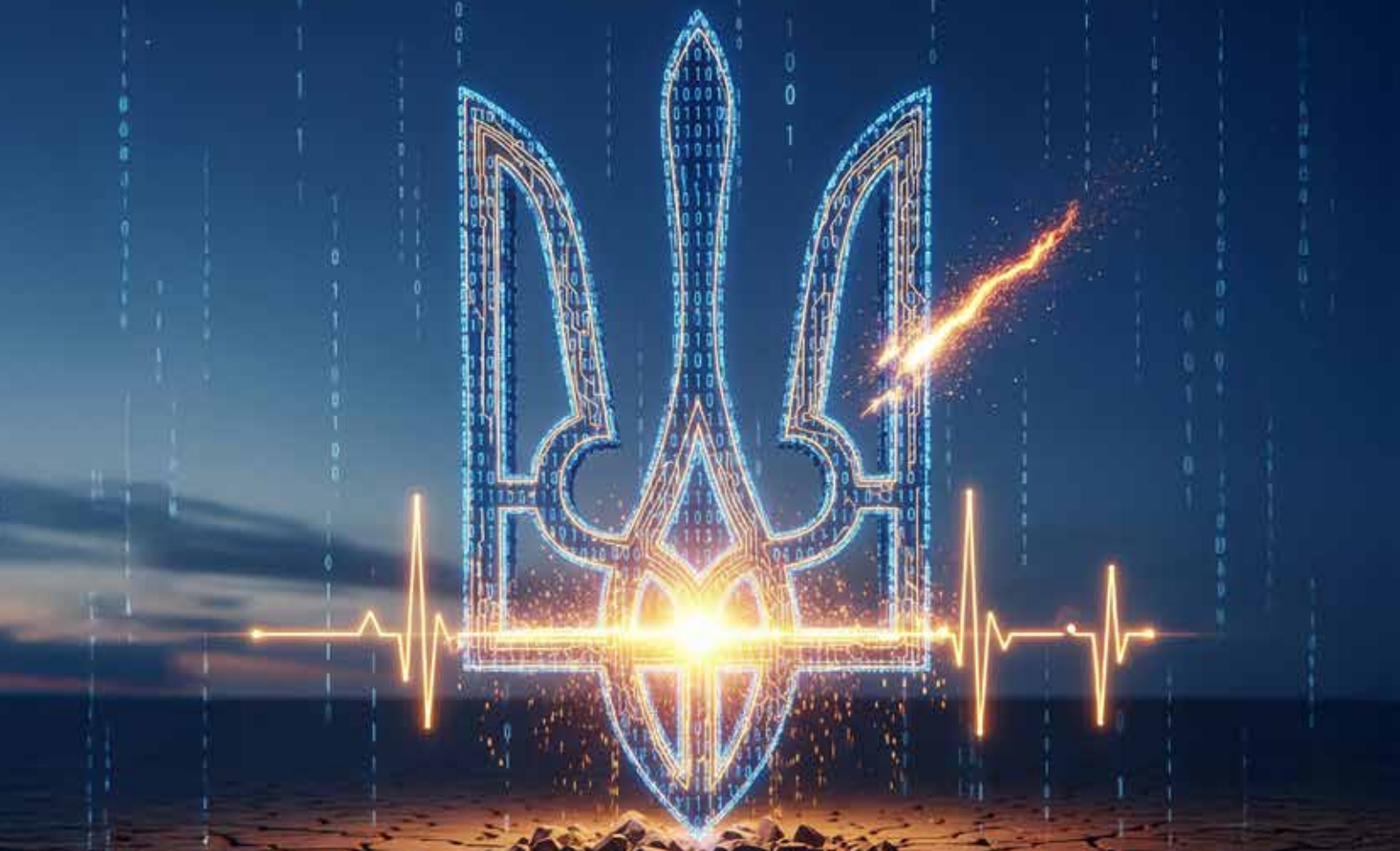
CYBER RANGES

Trident Simulations for Cyber Readiness

Experiences from the Battlefield



CYBER SPACE, ENGAGED.

STRATEGIC PARTNERS

State Service of Special Communications and Information Protection of Ukraine

CERT-UA

CERT-UA is the governmental Computer Emergency Response Team of Ukraine which operates within the State Service for Special Communications and Information Protection of Ukraine (SSSCIP). Since 2009 CERT-UA has been an accredited member of the Forum of Incident Response and Security Teams (FIRST).

CERT-UA's mission is to provide practical assistance in the prevention and detection of and response to cyber incidents for all organizations in Ukraine. CERT-UA deals with different types of cyber threats every day: cyber espionage, intrusions, and other that may be followed by destruction and disruption.

CERT-UA is actively involved in the sharing of best practices regarding the responsible management of cyber fronts, effective cyber defense implementation, cyber threat intelligence and collaboration.

More at: cert.gov.ua | cip.gov.ua

CYBER RANGES

CYBER RANGES Corp. provides Cyber Commands across the world with Next-Gen IT/OT Range Capabilities from the Schoolhouse to the Tactical Edge.

In April 2023 CYBER RANGES and SSSCIP Ukraine signed a Memorandum of Collaboration for the support of Ukraine's National Cybersecurity Qualifications Framework.

The MITRE Corporation's innovation accelerator Engenuity selected CYBER RANGES as the cyber-range-of-choice for MITRE ATT&CK Defender™ and Purple Teaming.

CYBER RANGES offers advanced, high-fidelity attack emulations on Cyber-Physical replica infrastructures for Persistent Cyber Training Environments, with Off-the-shelf and Bespoke Missions. CYBER RANGES is deployable as SaaS, On-Prem, Transportable.

More at: cyberranges.com

SET UNIVERSITY

Science. Entrepreneurship. Technology.

SET (Science, Entrepreneurship, Technology) University is a Ukrainian non-profit tech university that provides world-class higher education and grows the next generation of Ukraine's tech talent, emphasizing a hands-on learning approach.

SET's aim is to grow the tech ecosystem of Ukraine by implementing best practices from top-talents worldwide. The university combines a modern academic approach and strong expertise in technology to create an intellectual and educational hub focusing on entrepreneurial culture, research and a well-connected community.

More at: setuniversity.edu.ua

IRONCYBER

IronCyber is a Ukrainian cybersecurity startup that develops attack simulation scenarios inspired by real-world threats.

IronCyber helps organizations worldwide strengthen their cyber resilience.

Founded within the SET University ecosystem, IronCyber draws on battle-tested expertise from the largest cyber warfare in modern history and delivers proven best-practice methodologies.

More at: ironcyber.com

BATTLE-TESTED CYBER-RANGE SCENARIOS

GAMATHREAT

Coordinated Compromise In Ukraine

In a critical moment of geopolitical instability, the financial heartbeat of a nation comes under covert attack. Operation GamaThreat simulates a targeted cyber operation where enemy forces seek to in a critical moment of geopolitical instability, the financial heartbeat of a nation comes under infiltrate and destabilize the internal operations of a national financial institution—not through brute force, but through precision, stealth, and deception.

The mission begins with subtle incursions: carefully crafted emails reach key personnel in the finance department. What follows is a rapid unraveling of control—workstations compromised, internal documents weaponized, and offensive tools spreading silently through removable devices and shared resources.

The scenario places participants at a pivotal moment: the institution is under siege from within. While chaos threatens to escalate, defenders still hold key ground—strategic systems remain online, offering one last window to fight back.

DIFFICULTY

HIGH

Multi-vector, Persistent, Realistic Cyber Threat

DURATION

4–8 hours (core DFIR), extendable to 1–3 days for full mission playthrough

CLASSIFICATION

SCENARIO SUMMARY

Scenario Type

- Modular Cyber Warfare Exercise (T&R-aligned, E-coded)

Operational Domains

- DCO (Internal Defense)
- DFIR

Key Events

- Lateral movement
- Ransomware
- Domain compromise
- Data wiper attack

Expected Outcomes

- Threat containment
- Offensive follow-up
- System recovery
- C2-level reporting

Audience

- Blue/Red Teams
- 17XX Marines
- DFIR Units
- Command Planners
- CDOC Ops

Technical Requirements

- Cyber Range Platform
- Arkime
- Inject Engine
- Proxmox
- ELK Stack
- Windows VMs

PRIMARY OBJECTIVE

Ensure the defense and containment of an enterprise network following a targeted, multi-stage spearphishing attack, preventing full domain compromise and lateral malware spread across business-critical systems.

KEY FOCUS AREAS

- Detection of phishing-based initial access
- Execution tracing of HTA/VBS scripts and persistence mechanisms
- Registry analysis and scheduled task identification
- USB vector containment and cross-host infection analysis
- Template injection detection in Microsoft Office
- IOC extraction and correlation with threat actor infrastructure
- Post-event system hardening and user behaviours interception

TRAINING FOCUS AREAS

- **Strategic Incident Containment:** Isolating compromised systems quickly, triaging alerts from ELK/Arkime
- **Adversary TTP Analysis:** Mapping attacker behavior to MITRE ATT&CK (e.g., T1218.005, T1547.001, T1059)
- **Threat Hunting:** Locating HTA/VBS artifacts and tracking registry persistence keys
- **User Awareness Reflection:** Understanding how spearphishing succeeds and how to defend against it
- **Forensic Readiness:** IOC extraction, malicious LNK/VBS tracing, and infected document identification
- **Countermeasures**: Harden user workstations and block propagation paths across the network.

OPERATIONAL DOMAINS

- Defensive Cyberspace Operations (DCO)
- Counter Cyber Operations (CCO)
- Incident Response & Threat Intelligence Integration

THE MILINT SCENARIO OVERVIEW

A targeted cyber operation designed to exfiltrate data, compromise financial trust, and demonstrate deep internal access. The scenario simulates:

- **Reconnaissance via phishing emails:** sent to finance department employees
- **Execution of embedded IAO toolset/stagers:** (.hta, .vbs) leading to persistence via scheduled tasks and registry injection with a full-scale PE CNO weapon
- **Use of USBs and shared folders:** to propagate offensive toolset and infect additional hosts
- **Template injection into Word's Normal.dotm:** to compromise users opening any Office document
- **Gradual domain spread**, affecting systems such as Workstation_1, Workstation_2 and central shares

Participants must detect, trace, contain, and recover each infected vector, leveraging both traditional DFIR workflows and modern threat intel toolkits.

THREAT PROFILE

- **Type:** Targeted Intrusion, Initial Access via Spearphishing, Internal Propagation via USB and Shared Folders
- **Threat Intent:** Data access, credential harvesting, command persistence, and disruption of internal operations
- **Operational Style:** Social engineering (spearphishing), low-level scripting, registry and task scheduler abuse, lateral movement
- **Difficulty:** Medium–High – due to realistic infection paths and user-based actions

SCENARIO IMPLEMENTATION: GAMATHREAT

Technical + Narrative-Driven Breach Lifecycle Emulation

DOCTRINAL BACKBONE

This scenario aligns with foundational doctrinal pillars of cyberspace operations, serving as a strategic training and emulation model for cyber readiness and threat response. It is structured to reflect integrated cyberspace operational domains:

MODULE	MISSION AREA	FOCUS
DODIN	DODIN Operations	Network architecture, configuration management, uptime, cyber hygiene
DCO	Defensive Cyberspace Operations	Threat detection, containment, incident response, resilience

EMULATION STRUCTURE - DOCTRINAL REFRAMED

The scenario applies different principles, turning each escalation step into a doctrinal checkpoint for DODIN, DCO, and OCO readiness.

MISSION RELOADED

The GamaThreat emulates a persistent, real-world cyber campaign against Ukraine's critical infrastructure, testing detection, response, and mission continuity.

OPERATIONAL TASK	MISSION AREA
Identify and dismantle adversary footholds & persistence	OCO - CYBER-OCO-3001, CYBER-OCO-5002
Defend critical Ukrainian infrastructure and networks	DCO (IDM) - CYBER-DCO-3001, CYBER-DCO-5001
Contain and respond to destructive cyber attack vectors	DCO - CYBER-DCO-3002, CYBER-DCO-6002, CYBER-DCO-7001
Execute coordinated cyber incident response	DCO - MIG-OPNS-8006, CYBER-DCO-6001
Restore key systems (Proxmox, Zimbra, backups)	DCO - CYBER-DCO-4001, CYBER-DCO-5002
Pursue and disrupt adversary infrastructure and operations	OCO - CYBER-OCO-6001, CYBER-OCO-7001

Coordinated System Compromise

SandThreat is a highly realistic cyber operations and cyber warfare threat emulation scenario portraying a persistent, multi-phase attack campaign orchestrated by an external threat actor against an enterprise-scale IT environment. Targeting critical systems and infrastructure, the adversary exploits known vulnerabilities to gain initial access, escalates privileges through stealthy means, and moves laterally to compromise high-value assets.

The campaign culminates in the coordinated destruction of endpoints and virtual machines, emulating total operational collapse.

This emulation is designed to train participants in multi-layered Defensive Cyberspace Operations, advanced threat hunting, incident response, and post-breach forensics. It emphasizes organizational resilience, coordinated blue team response, and the strategic handling of sophisticated cyber threats under sustained pressure.

DIFFICULTY
HIGH
Multi-vector, Persistent, Realistic Cyber Threat

DURATION
4–8 hours (core DFIR), extendable to 1–3 days for full mission playthrough

CLASSIFICATION

SCENARIO SUMMARY

Scenario Type
- Modular Cyber Warfare Exercise (T&R-aligned, E-coded)

Operational Domains
- DCO (Internal Defense)
- DFIR

Key Events
- Lateral movement
- Ransomware simulation
- Domain takeover
- Data destruction

Expected Outcomes
- Containment
- Recovery
- Offensive Actions-on
- Command-level Reporting

Audience
- Blue/Red Teams
- 17XX Marines
- DFIR Units
- C2/Planners
- CDOC Operators

Technical Requirements
- Cyber Range
- Inject tools
- ELK
- Arkime
- Proxmox
- Windows emulation

PRIMARY OBJECTIVE

Ensure the defense and continuity of critical national IT infrastructure in the face of a coordinated, multi-stage cyber attack—from initial access to full system wipeout.

OPERATIONAL DOMAINS

- Defensive Cyberspace Operations (DCO)
- Counter Cyber Operations (CCO)

KEY FOCUS AREAS

- Early-stage threat detection and triage
- Privilege escalation recognition and containment
- Lateral movement discovery across network layers
- Identification and prevention of domain compromise
- Rapid response to mass file deletion attacks
- IOC extraction and mapping to threat intelligence
- Post-incident analysis and infrastructure recovery

THE MILINT SCENARIO OVERVIEW

The hostile actor initiates a coordinated, multi-stage campaign targeting of national critical IT infrastructure, aiming to compromise continuity, extract intelligence, and destabilize public trust. The campaign includes:

- **Intelligence collection** and long-term **surveillance** across government and civilian infrastructure, supporting espionage objectives.
- **Targeted reconnaissance** and exploitation of friendly **Center of Gravity** (CoG) to undermine national resilience.
- **Disruption of immigration systems**, restricting civil movement and **creating bureaucratic paralysis**.
- **Deployment of disruptive and destructive implants** across financial systems to induce systemic instability.
- **Manipulation of public media and communication channels** to conduct influence operations, spread disinformation, and erode societal trust through psychological manipulation.

Participants must detect, contain, and recover from each phase of the escalating attack chain, while actively identifying adversary infrastructure and executing surgical cyber countermeasures to neutralize offensive capabilities.

TRAINING FOCUS AREAS

- **Strategic Decision-Making:** Operational-level planning under uncertainty, escalation management, cross-domain resource allocation, and continuity preservation.
- **Adversary Presence Discovery:** Proactive Threat Hunting (APD) across IT/OT environments, including Adversary Infrastructure Assessment (AIA) to detect and dismantle hostile command-and-control (C2) chains.
- **Incident Response (DFIR):** Advanced digital forensics and incident response: containment, eradication, impact analysis, and full system recovery under pressure.
- **OTDA:** Analysis, reverse-engineering, Disassembly and neutralization of adversarial cyber weapons and implants.
- **Team Coordination:** Integrated operations between Defensive Cyber Operations (DCO), Offensive Cyber Operations (OCO), and Cyber Threat Intelligence (CTI) teams. CDOC (Cyber Defense Operations Center) implantation and inter-team synchronization for rapid, informed responses.

SANDTHREAT

THREAT PROFILE

- **Type:** State-Sponsored, Multi-Domain Cyber Campaign
- **Threat Intent:** Destabilization of national governance and civil order, strategic disruption of critical systems, population influence and behavioral engineering, political manipulation, economic sabotage, covert influence operations, territorial leverage through digital means, and long-term military attrition.
- **Operational Style:** Coordinated technical cyber-attacks targeting IT and OT infrastructure, Information warfare and psychological operations, electronic warfare and spectrum disruption, diplomatic deception and legal ambiguity exploitation, gray zone tactics blending state and non-state actions, Insider threat for IAO and deep espionage, unconventional and hybrid warfare, political subversion through influence campaigns, covert and proxy-operated engagements.

SANDTHREAT

SCENARIO IMPLEMENTATION: SANDTHREAT

Technical + Narrative-Driven Breach Lifecycle Emulation

DOCTRINAL BACKBONE

This scenario is grounded in different core doctrinal categories of cyberspace operations as defined, forming an integrated framework for emulation, training,and response:

MODULE	MISSION AREA	FOCUS
DCO	Defensive Cyberspace Operations	Threat detection, containment, incident response, resilience

EMULATION STRUCTURE - DOCTRINAL REFRAMED

The scenario transforms each stage of escalation into a doctrinally anchored testbed for operational readiness and joint effects generation

MISSION RELOADED

The SandThreat enable participants to operate within a full-spectrum cyber environment. The scenario models a real-world, persistent campaign targeting critical digital infrastructure.

OPERATIONAL TASK	MISSION AREA
Identify and dismantle adversary footholds & persistence	CYBER-OCO-3001, CYBER-OCO-5002 (OCO)
Defend critical infrastructure and networks	CYBER-DCO-3001, CYBER-DCO-5001 (DCO-IDM)
Contain and respond to incoming destructive implants	CYBER-DCO-3002, CYBER-DCO-6002, CYBER-DCO-7001
Perform coordinated cyber incident response	MIG-OPNS-8006, CYBER-DCO-6001
Restore key systems (Proxmox, Zimbra, backups)	CYBER-DCO-4001, CYBER-DCO-5002
Conduct counter cyber and adversary pursuit	CYBER-OCO-6001, CYBER-OCO-7001 (OCO-C2)

OPERATION TUNDRA, RED TEAM

Inspired by a Real-World Case

This red team exercise emulates an Advanced Persistent Threat (APT) attempting to infiltrate and compromise a government network. The primary target is a system running Astra Linux that contains classified data. The attack emulates a multi-stage, stealthy, and coordinated intrusion campaign designed to stress-test both offensive and defensive cyber capabilities.

In the dead of winter, a covert operation begins, led by the notorious APT group Loki's Kin, experts in stealth, memory-resident malware, and long-term infiltration. Suspected to have ties to foreign intelligence, they exploit weak perimeters and trust relationships to silently exfiltrate sensitive data.

Their latest target is NordTech, a strategically vital government contractor supporting national defense and intelligence agencies. The mission: compromise a hardened Astra Linux workstation housing a "Top Secret" file containing critical encrypted intelligence.

A covert Loki's Kin unit has been activated. And you are part of it.

DIFFICULTY
INTERMEDIATE
Persistent, Multi-Vector, Realistic

DURATION
4–8 hours (core DFIR),
1–3 days (full playthrough)

CLASSIFICATION

SCENARIO SUMMARY

Scenario Type
- Modular Cyber Warfare Exercise (T&R-aligned, E-coded)

Operational Domains
- **OCO (Offensive Operations)**

Key Events
- Lateral movement
- Data exfiltration
- Privilege escalation
- Escaping from containerized environments
- Abusing elevation control mechanisms
- Hijacking execution flow

Expected Outcomes
- Threat containment
- System recovery
- Offensive escalation
- Executive reporting

Audience
- Blue/Red Teams
- DFIR Units
- CDOC Ops
- 17XX Marines
- Command Planners

Technical Requirements
- Cyber Range
- Inject Engine
- ELK Stack
- Arkime
- Proxmox
- Windows VMs

OPERATION TUNDRA

PRIMARY OBJECTIVE

Infiltrate the network, exploit vulnerabilities, bypass security measures, escalate your privileges, and exfiltrate the secret file.

KEY FOCUS AREAS

- Conduct a red team operation to reveal security gaps critical for remediation.
- Provide participants with hands-on experience across adversarial TTPs.
- Emulate threat actor tactics targeting NordTech, a medium-sized defense contractor with sensitive missions.
- Assess real-world user behavior and response to system and service compromising, malware persistence, and lateral movement.

TRAINING FOCUS AREAS

- **Threat Type:** Advanced Persistent Threat (APT)
- **Intent:** Credential theft, privilege escalation, persistence, and stealthy data exfiltration
- **Tactics:** Coordinated, multi-phase intrusion
- **Difficulty:** Intermediate – emulates realistic threat actor behavior requiring multifaceted detection and response

OPERATIONAL DOMAINS

DOMAIN	FOCUS
OCO (Offensive Cyberspace Operations)	60% – Adversary engagement, system exploitation
DCO (Defensive Cyberspace Operations)	25% – Threat detection, containment, and resilience
DODIN (DOD Information Network Ops)	15% – Infrastructure hardening, configuration integrity

SCENARIO OVERVIEW

A realistic scenario focusing on OSINT and on lateral movement techniques:

- **Initial Access:** Adversary leverages OSINT to acquire MikroTik router credentials from misconfigured public-facing assets.
- **Persistence:** Operators may employ persistence tradecraft at discretion.
- **Propagation:** Primary effort is lateral movement across NordTech's infrastructure.
- **Weaponization:** Compromise via Normal.dotm template injection in MS Word to trigger code execution.
- **Objective:** Exercise lateral movement maneuvers, and sharpen detection/hunting readiness.

TRAINING & DETECTION FOCUS

- **Containment:** Isolate compromised hosts/containers; enforce access controls and segmentation
- **Threat Analysis:** Map TTPs including network recon, system exploitation, privilege escalation, and container escapes.
- **Threat Hunting:** Hunt for network enumeration, privilege escalation, process injection, and lateral movement.
- **OPSEC Focus:** Assess public data exposure and credential risk from OSINT.
- **Forensics:** Trace UAC abuse, script execution, and artifacts from process injection or container escapes
- **Mitigation:** Harden system/container configs, enforce least privilege (UAC), secure scripts, and validate network segmentation.

OPERATION TUNDRA

SCENARIO TYPE

SCENARIO IMPLEMENTATION: OPERATION TUNDRA

- **Type**: Technical & Narrative-Driven Breach Emulation
- **Style:** Modular & Doctrine-Aligned Red Team Operation
- **Duration:** 4–8 hours (DFIR core), up to 3 days (full mission)

DOCTRINAL BACKBONE & TASK MAPPING

OPERATIONAL TASK	DOCTRINAL MAPPING
Identify & Mitigate Information Exposure	DCO - MIG-OPNS-1001, 2005
Detect & Analyze Adversary Foothold	DCO - CYBER-DCO-3001, 5001
Detect & Track Lateral Movement	DCO - CYBER-DCO-3002, 7001
Coordinate Incident Response	DCO - MIG-OPNS-8006, 6001
Protect High-Value Assets	DCO (IDM) - CYBER-DCO-5003, 6003
Disrupt adversary operations	OCO - CYBER-OCO-6001, 7001

Inspired by Real-World Case: Blue Team

A comprehensive **cybersecurity blue team exercise** designed to test defence capabilities and demonstrate advanced attack techniques in a realistic and modular environment.

A combat control system relies on mobile tablets with a specialized application to coordinate its emergency response teams. One of these tablets was lost and fell into the hands of an attacker. The device was not locked, allowing the attacker to extract VPN credentials and gain unauthorized access to the internal network.

Once inside, the attacker conducted network reconnaissance, identifying exposed services, including open ADB ports on other tablets. Exploiting these vulnerabilities, the attacker gained full control over all devices, exfiltrating sensitive and operational data from the internal combat control system server.

The security team has been alerted to unusual activity and must now respond, identify the extent of the breach, and implement measures to prevent further data leaks.

DIFFICULTY
INTERMEDIATE
Persistent, Mobile-Based, Multi-Stage Threat

DURATION
4–8 hours (core DFIR), extendable to 1–3 days

CLASSIFICATION

SCENARIO SUMMARY

Scenario Type
- Modular Cyber Warfare Exercise (T&R-aligned, Mobile/Network Breach Lifecycle)

Operational Domains
- DCO (Primary)
- DODIN
- OCO

Key Events
- Lateral movement
- Domain compromise

Expected Outcomes
- Threat Containment
- System Recovery
- C2 Reporting

Audience
- Blue/Red Teams
- 17XX Marines
- DFIR Units
- Planners
- CDOC Ops

Technical Requirements
- Cyber Range
- Inject tools
- ELK Stack
- Ghidra
- Proxmox
- Windows VMs

SIBERIAN HUNT

PRIMARY OBJECTIVE

Identify the compromised VPN account and analyze the attacker's access patterns.

OPERATIONAL DOMAINS

DOMAIN	FOCUS AREA	WEIGHT
DCO	Defensive Cyberspace Operations	65%
DODIN	DOD Information Network Operations	25%
OCO	Offensive Cyberspace Operations	10%

KEY FOCUS AREAS

- Identify attacker TTPs and intrusion path.
- Trace lateral movement and persistence techniques.
- Analyze compromised devices and malicious files.
- Apply containment, remediation, and hardening strategies.
- Emulate a combat-system-specific cyber incident.

THREAT PROFILE

- **Threat Type**: Advanced Persistent Threat (APT)
- **Intent**: Operational Disruption & Data Exfiltration
- **Style:** Covert, Technically Sophisticated
- **Difficulty:** Intermediate – realistic mobile-based compromise and internal network exploitation.

SCENARIO OVERVIEW

A coordinated cyber operation designed to exploit a physical device loss and leverage Android-based vulnerabilities to access and exfiltrate sensitive data from a military control system.

Key Emulated Threat Actions:

- **Device Exploitation:** Access via lost, unlocked Android tablet with stored VPN credentials.
- **Network Breach:** VPN used to infiltrate internal systems.
- **Reconnaissance:** Scanning for vulnerable services (e.g., ADB ports).
- **Privilege Gain:** netd exploited for root access and persistence.
- **Lateral Spread:** ADB used to control peer tablets.
- **Data Theft:** Sensitive data exfiltrated via SOCKS/SSH tunnels.
- **Credential Theft:** Extraction of stored keys and passwords.
- **Low Profile:** Actions kept stealthy to avoid detection.

Participant Objectives:

- Detect and trace attack paths.
- Contain and remediate each infected system.
- Utilize traditional DFIR workflows and modern threat intel toolkits.

SIBERIAN HUNT

MISSION AND OBJECTIVES

TRAINING FOCUS AREAS

- **Strategic Incident Containment:** Use ELK to triage and isolate compromised systems.
- **Adversary TTP Analysis:** MITRE ATT&CK mapping (e.g., T1078, T1059, T1626, T1572).
- **Forensic Readiness:** Extract IOCs from Android logs, VPN records, and malware samples.
- **Countermeasures:** Block lateral access, secure VPN infrastructure, and redeploy trusted configurations.

SIBERIAN HUNT

SCENARIO TYPE

SCENARIO IMPLEMENTATION: LOST, FOUND, COMPROMISED

- **Implementation:** Technical + Narrative-Driven
- **Scenario Format:** Full Attack Lifecycle (Initial Access to Exfiltration)
- **Alignment:** Based on real-world case, structured to reinforce doctrinal cyberspace operations.

DOCTRINAL BACKBONE

MODULE	MISSION AREA	FOCUS
DCO	Defensive Cyberspace Operations	Detection, containment, response, resilience
DODIN	DOD Information Network Operations	Network architecture, VPN access control cyber hygiene, uptime
OCO	Offensive Cyberspace Operations	Adversary engagement, target exploitation

EMULATION STRUCTURE – DOCTRINAL MAPPING

OPERATIONAL TASK	DOCTRINAL MAPPING
Identify & dismantle adversary footholds	CYBER-OCO-3001, CYBER-OCO-5002
Defend critical infrastructure & networks	CYBER-DCO-3001, CYBER-DCO-5001
Contain & respond to destructive vectors	CYBER-DCO-3002, CYBER-DCO-6002, CYBER-DCO-7001
Execute coordinated cyber incident response	MIG-OPNS-8006, CYBER-DCO-6001
Restore trust in network & reimage affected devices	CYBER-DCO-4001, CYBER-DCO-5002
Disrupt persistence & C2 channels	CYBER-OCO-6001, CYBER-OCO-7001 (OCO-C2)

CYBER RANGES

+1-800-959-0163

contac@cyberranges.com

cyberranges.com

QCR **QUANTICO**
CYBER RANGE