# NEST Arena

## Noibit Enhanced Security Training

**Are you ready to test the readiness of your cybersecurity team?**

Be prepared to prevent, detect, and react to major security incidents in the vividly simulated environment.

- 2-day Intensive On-site cybersecurity polygon (Noibit's or Customer's premises)
- Realistic exercise conducted as a wargame-style simulation
- Experienced Senior Cybersecurity Consultants and Analysts serving as mentors
- Seasoned and battle-tested Red Team simulating advanced persistent threats (APTs)
- AI-powered, fully simulated and realistic environment —dynamic and immersive "living grounds"

Noibit Enhanced Security Training Arena

NEST Arena

Noibit

## Immersive Defensive Security Training for Blue Teamers

**Two-day hands-on training**, specifically designed for blue team professionals, offering a unique and immersive experience in defensive cybersecurity through **live attack simulations**. Participants will engage with a simulated adversary in a **realistic** corporate network environment, sharpening their skills in threat detection, incident response, and **cyber defence strategy**.

## Agenda

Participants will be guided by an experienced Blue Team instructor throughout the training. The course is designed to reflect the **latest attacker techniques**, blending both stealthy and overt tactics to challenge and expand your defensive capabilities. Each exercise is structured to **simulate real-world scenarios**, encouraging participants to think critically and respond effectively.

If participants are unfamiliar with any of the tools used, the instructor will provide concise, practical introductions to ensure everyone can fully engage with the hands-on activities. The focus is on real-time application—learning by doing in a **dynamic, threat-rich** environment.

## Target Audience

This technical training is ideal for IT and cybersecurity professionals seeking to deepen their expertise in blue teaming, threat hunting, and detection engineering. Participants will face a **live, ongoing cyberattack** and gain hands-on experience in how collaborative defence strategies can significantly improve an organisation's resilience against real-world threats.

**Recommended for:**

- Cybersecurity Professionals
- Threat Hunters
- Incident Responders
- SOC Analysts
- Detection Engineers
- IT Professionals with a strong interest in technical cybersecurity

## Training Highlights

**Realistic Attack Simulations:**
Over two days, participants will navigate a series of escalating attack scenarios starting with foundational detection techniques and progressing to advanced tactics such as:

- Webshell deployment
- Credential dumping
- Command and control (C2) techniques
- Website exploitation
- Various attacks on critical applications and services
- Social engineering
- Lateral movement
- And more

**Guided Threat Hunting & Detection Engineering:**
Through structured exercises, participants will craft and apply detection rules to identify and neutralise adversarial activity in real time.

**Purple Team Collaboration:**
Post-Mortem Joint sessions between offensive (red) and defensive (blue) roles foster a deeper understanding of attacker methodologies and defensive countermeasures, enhancing cross-team collaboration.

**Toolset & Technology Integration:**
Participants will gain hands-on experience with a wide range of Microsoft and security tools, including:

- Microsoft Sentinel SIEM
- Defender for Endpoint, Cloud Apps, Office 365, Identity, Cloud, and IoT
- Web Application Firewalls, traditional firewalls, and other defensive technologies

**By the end of the training, attendees will be equipped to:**

- Develop and implement custom detection queries
- Design proactive threat-hunting strategies
- Strengthen red-blue team collaboration
- Enhance their organisation’s overall security posture

# Advanced Persistent Threat Emulation

Continuous multi chained attacks based on tactics, techniques and procedures used by real threat actors, run by experienced **Noibit Red Team**

## Cloud Environment

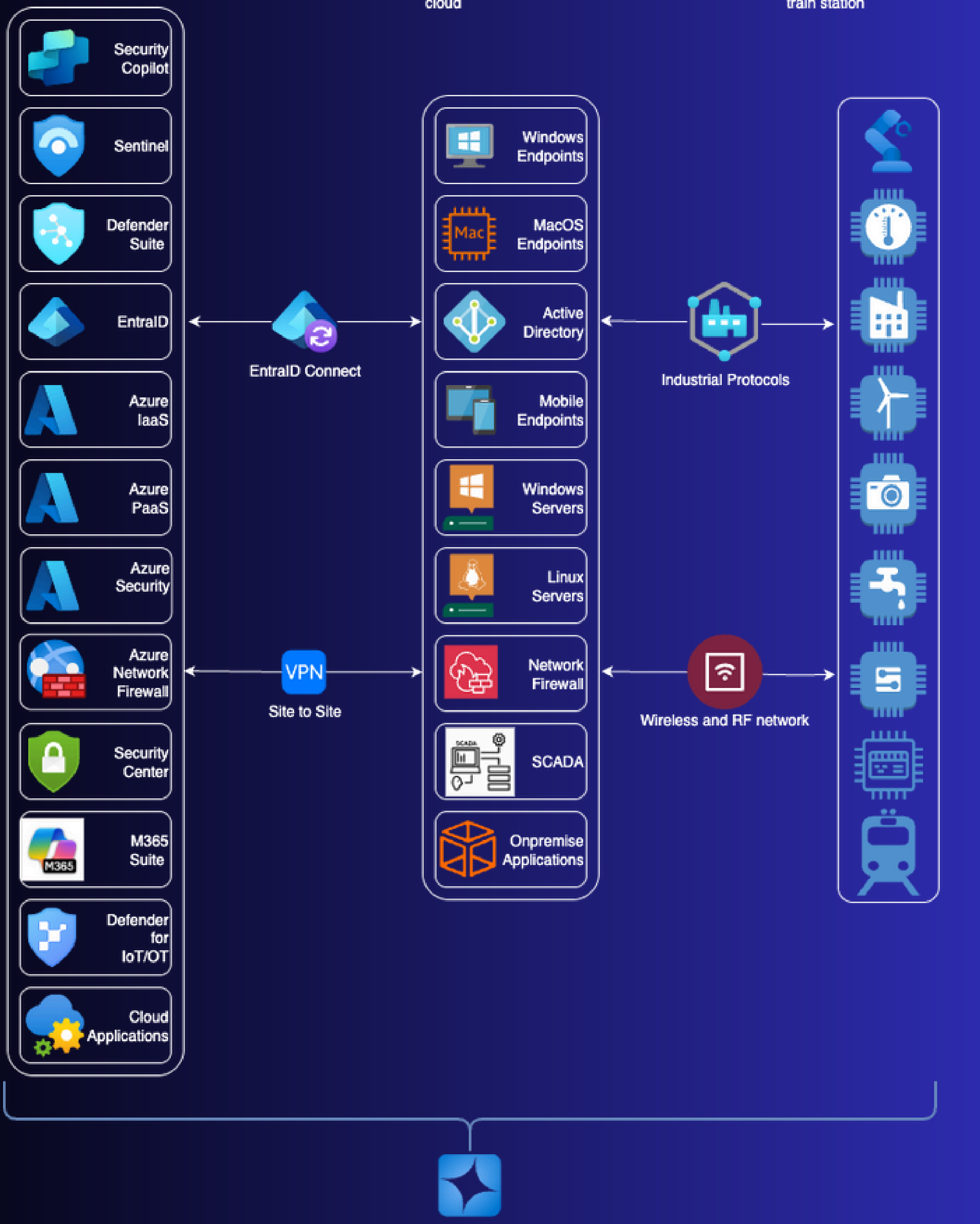
Live Environment in Azure and M365 Clouds

## On Premise Environment

Live On Premise Environment connected to cloud

## IoT/OT/ICS Environment

Live and complex industrial and IoT environment with train station



Security Copilot

Sentinel

Defender Suite

EntraID

Azure IaaS

Azure PaaS

Azure Security

Azure Network Firewall

Security Center

M365 Suite

Defender for IoT/OT

Cloud Applications

EntraID Connect

VPN

Site to Site

Windows Endpoints

MacOS Endpoints

Active Directory

Mobile Endpoints

Windows Servers

Linux Servers

Network Firewall

SCADA

Onpremise Applications

Industrial Protocols

Wireless and RF network

## Living Environment powered by Azure Open AI

Complex set of Gen AI agents which are used for simulation of everyday life in simulated environment

Noibit

## Training grounds

The whole exercise will be held in a virtual environment, where students will have access to a simulated network rated as **critical infrastructure of the state**. The environment will include various systems, applications, and services that mimic a real-world infrastructure, including:

- **M365 tenant** with collaboration tools like Teams, SharePoint, OneDrive, and Exchange Online,
- **EntraID** for identity and access management,
- **Azure** resources, including virtual machines, databases, platform services, and web applications,
- On-premises infrastructure with **Windows and Linux** servers, workstations, and network devices,
- **Apple** (macOS and iOS) and **Android** endpoints,
- **Industrial systems (ICS), OT**, and IoT devices, such as **SCADA** systems, printers, cameras, and other devices. Including network and industrial protocols like Modbus and others.

## Simulated Live Environment Powered by Generative AI

The entire training takes place within a **fully simulated**, lifelike corporate environment—carefully crafted to mirror the complexity and unpredictability of the real world. This environment is enriched by cutting-edge generative AI and large language models (LLMs), which **emulate realistic user behaviour, business operations**, and adversarial activity.

Participants will interact with a **dynamic digital ecosystem** where employees, systems, and workflows behave as they would in a real organisation. From simulated helpdesk tickets and email communications to user logins and behavioural anomalies, every element is designed to create a truly immersive experience.

This AI-driven realism ensures that defenders are **not just reacting to static scenarios** but are actively engaging with a living, breathing environment, where decisions have consequences, and attackers adapt to defensive actions. It's the closest you can get to **defending a real network without the risk**.

## Key Takeaways

By the end of this training, participants will be able to:

- Experience the intensity of a live cyberattack and practice effective response strategies.
- Confidently use defensive tools such as SIEM and XDR platforms.
- Strengthen the skills and readiness of their defensive teams.
- Understand the critical role of threat hunting and detection engineering in modern cybersecurity.
- Recognise and analyse attacker techniques across the kill chain.
- Build and deploy custom detection rules and threat-hunting queries to uncover hidden threats.
- Implement decoy objects (e.g., honeytokens) to proactively detect common attack patterns.
- Foster collaboration between red and blue teams to identify and close security gaps, improving overall detection and response capabilities.

**Contact us**

✉ sales@noibit.com

www.noibit.com

in www.linkedin.com/company/noibit

Noibit