

Quick 90 mins version



Defenders of the Park

Today's team



Anders Enqvist
Technical Sales
Engineer Nordics



Liora Herman
Senior Director,
Field & Channel
Marketing



Björn Björkman
Solution Advisor,
NetNordic



Christian Sierau
Solution Advisor,
NetNordic



Fabian Jacobsson
Strategic Advisor,
NetNordic



Pontus Ek
Security Delivery Senior
Analyst, NetNordic

November 7, 2025

Uppsala, Sweden

Red Teaming

Workshop

Workshop WIFI

SSID: penterarocks

Password: penterarocks

Documentation: Please download at:

<http://192.168.0.103:8000/>

You can AFTER DOWNLOAD use the UKK_Guest / UKK_2007

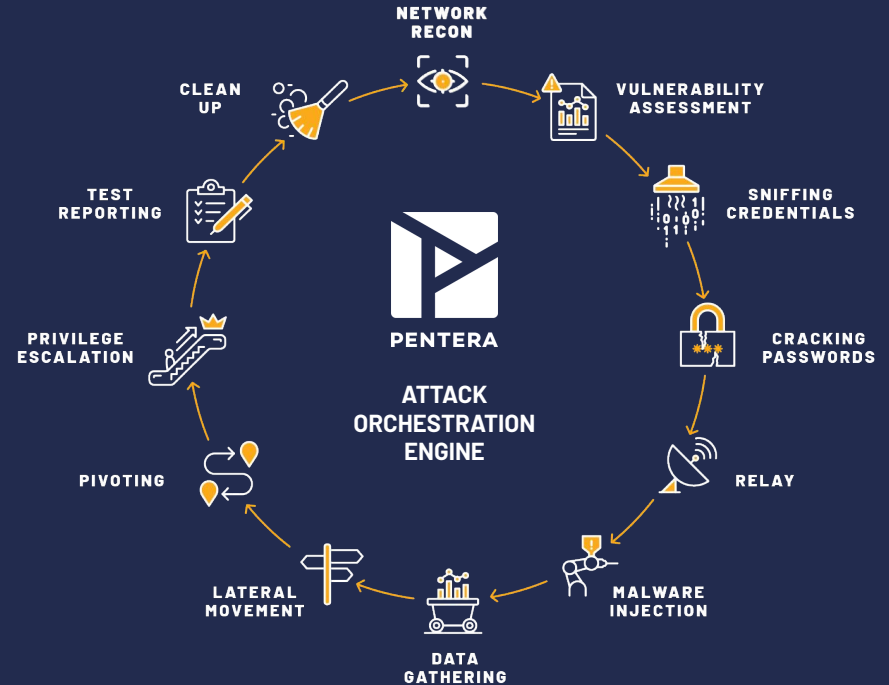




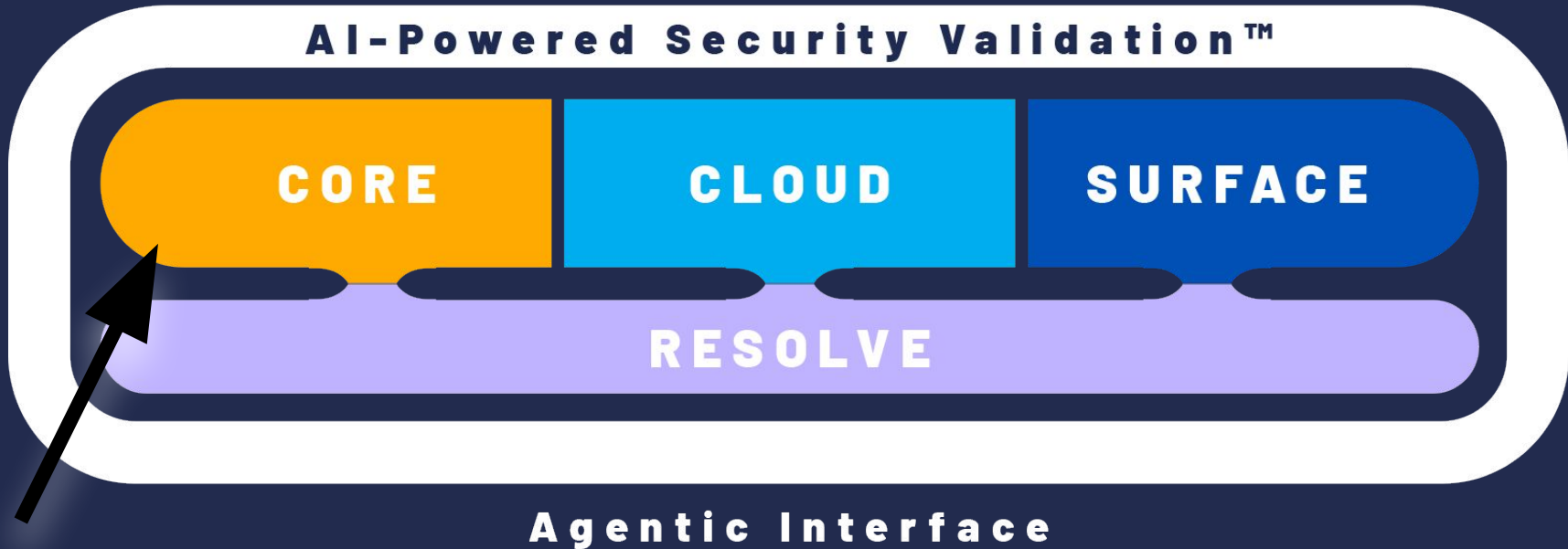
**How
CONFIDENT
T are you in
your security
posture?**

Pentera Red Team Workshop Agenda

- REAL** ethical attacks in production
- ALGORITHM-BASED** - no playbooks
- COMPREHENSIVE** attack coverage
- ENTERPRISE-WIDE** agentless deployment
- SAFE** - no risk to operations or data



Pentera Platform



Our scope

A Unified Validation to Remediation Platform

Pentera New service offering

Pentera Offensive Security Services +

**Research-Led Offensive Testing
for AI Infrastructure and Applications**



<https://pentera.io/offensive-security/>

<https://pentera.io/resources/data-sheets/offensive-security-services/>

Pentera Red Team Workshop Agenda



- **Welcome & Introduction**
 - House rules & expectations
- **Agenda overview**
 - Black Box
 - Leaked Credentials
 - ADPA (already run and results given as an imported historical run)
 - Gray Box
 - Ransomware
 - Wrap-Up & Discussion
 - Key takeaways
 - Final Q&A

House Rules

- Don't change any config options
- Don't just poke around
- Don't delete pre-existing scenarios
- Don't start pre-existing scenarios
- Don't delete history entries
- We start the scenarios together (once every group finished their config)
- We end the scenarios together (and discuss results)

Let's break the rules

Lab Environment - Pentera Login

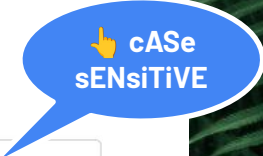
- **Main Node:**
 - <https://tu25-1xx.lab.pentera.life:8181>
 - <https://tu25-2xx.lab.pentera.life:8181>
(101,..122 and 201 to 222)
- **Username:** pentera
- **Password:** P@ssw0rd



The image shows a screenshot of the Pentera login page. At the top left is the Pentera logo and name. Below it is the text "Making sure it's you". To the right of this text is a blue speech bubble containing a yellow hand icon pointing to the text "cAsE sENSiTiVe". Below the text are two input fields: "User Name * pentera" and "Password * P@ssw0rd". To the right of the password field is a small icon of an eye with a slash through it. Below the input fields is a grey "Sign in" button.

 **PENTERA**

Making sure it's you



User Name * pentera

Password * P@ssw0rd 

Sign in



Welcome to Isla InGen

Somewhere deep in the Pacific, Isla InGen is a sanctuary, a place where the ancient past could live again. But now, it's under siege.

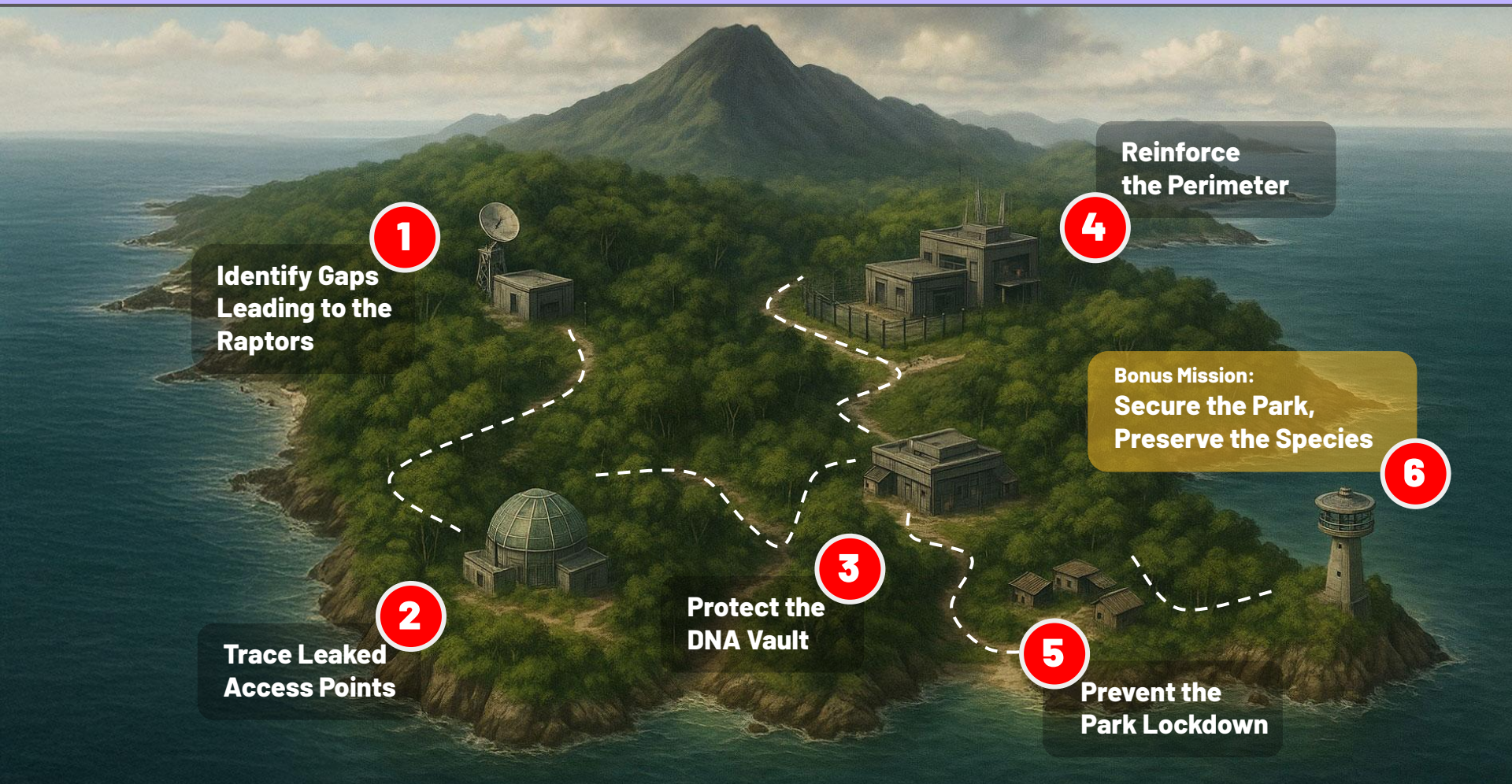
A rogue hacktivist collective known as Epoch has declared war on the island. They believe reviving extinct species is unnatural, dangerous, and must be undone. Their goal: bring down the park's systems and trigger extinction.

You are part of the last line of defense. A red team strike force tasked with preservation.

By emulating real-world attackers, you'll uncover the island's digital weak points *before Epoch can exploit them*.

This is a race against time. Because if the systems fall, the dinosaurs go with them. Your mission is clear: Save the park. Protect the species. Preserve history.

Each mission targets a threat vector that could compromise containment, control, or care for the creatures.

**1**

**Identify Gaps
Leading to the
Raptors**

2

**Trace Leaked
Access Points**

3

**Protect the
DNA Vault**

4

**Reinforce
the Perimeter**

6

**Bonus Mission:
Secure the Park,
Preserve the Species**

5

**Prevent the
Park Lockdown**



Mission 1:

Identify Gaps Leading to the Raptors

BLACK BOX

Module:

Black Box

Objective:

Map the network and discover exposed assets.

Narrative:

You've landed on the island with with only a foothold to internal access. Epoch will be scanning for security gaps, so you need to find them first. Locate critical systems tied to habitat sensors and feeding mechanisms before they're damaged.

Win Condition:

Identify exposed entry points and make your way to the Raptors' habitat.



NO ACCESS

Mission 2:

Trace Leaked Access Points

Module:

Leaked Credentials

Objective:

Investigate the impact of leaked credentials on the Island's security posture.

Narrative:

Employees keep reusing breached passwords. Epoch thrives on this laziness. Identify where legacy credentials could still open doors and shut them permanently.

Win Condition:

Gain access via OSINT or breach data; flag all exploitable paths.



Mission 3:

Protect the DNA Vault

Module:

Password Cracking

Objective:

Crack weak passwords and secure critical systems.

Narrative:

The genetic archive is the lifeblood of Isla InGen. Epoch wants to wipe it out to end the program forever. Test how easily these keys can be cracked and locked down for good.

Win Condition:

Access the vault using weak credentials, then help secure it.



Mission 4:

Reinforce the Perimeter

Module:

Gray Box

Objective:

Use insider-level access to test internal resilience.

Narrative:

A stolen employee badge has surfaced on the dark web. If Epoch uses it, they can disrupt electric fences and tracking systems. Run the insider breach before they do and ensure systems can resist the attack.

Win Condition:

Test internal escalation paths and reinforce segmented access.



Mission 5:

Prevent the Park Lockdown

Module:

Ransomware

Objective:

Emulate a ransomware attack on park operations.

Narrative:

Epoch will try to shut down the Island and encrypt the Island systems. You need to make sure their ransomware campaign is unsuccessful. Simulate this attack to uncover the path they'd take and shut it down.

Win Condition:

Demonstrate potential ransomware spread and advise on defenses to keep habitats running.



Bonus Mission:

Secure the Park, Preserve the Species

SECURE
THE PARK
PRESERVE
THE SPECIES

Module:

Reports

Objective:



Validate security posture and recommend actionable fixes.

Narrative:

You've walked the attacker's path. Now, become the guardian. Use your findings to brief the InGen response team, prioritize remediation, and ensure the island is safe, not just today, but tomorrow.

Win Condition:

Deliver a clear, prioritized remediation plan based on real attack paths.



Thank You.