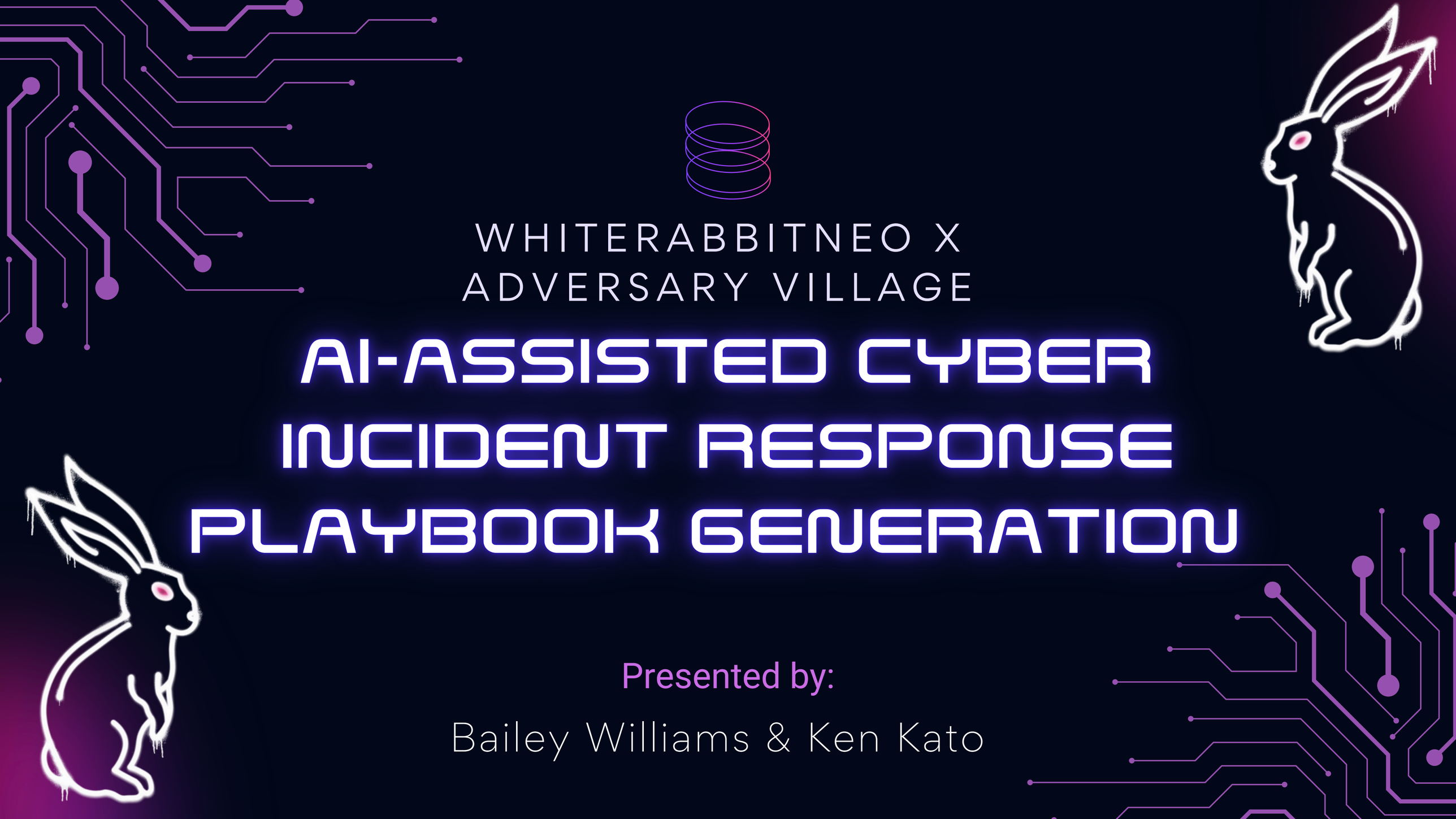


WHITERABBITNEO X
ADVERSARY VILLAGE

AI-ASSISTED CYBER INCIDENT RESPONSE PLAYBOOK GENERATION

Presented by:

Bailey Williams & Ken Kato

WHAT IS WHITERABBITNEO?

UNCENSORED, OPEN-SOURCE AI FOR DEVSECOPS

Open-source and community-driven

Uses the current best software engineering LLM as the foundational model

Promotes human-in-the-loop AI usage

AI RUNBOOKS EXPLAINED

While traditional runbooks give your employees a checklist to follow when specific scenarios occur, AI allows you design runbooks that run automatically when pre-defined events occur, such as irregular server logs.

BUILDING YOUR RUNBOOK

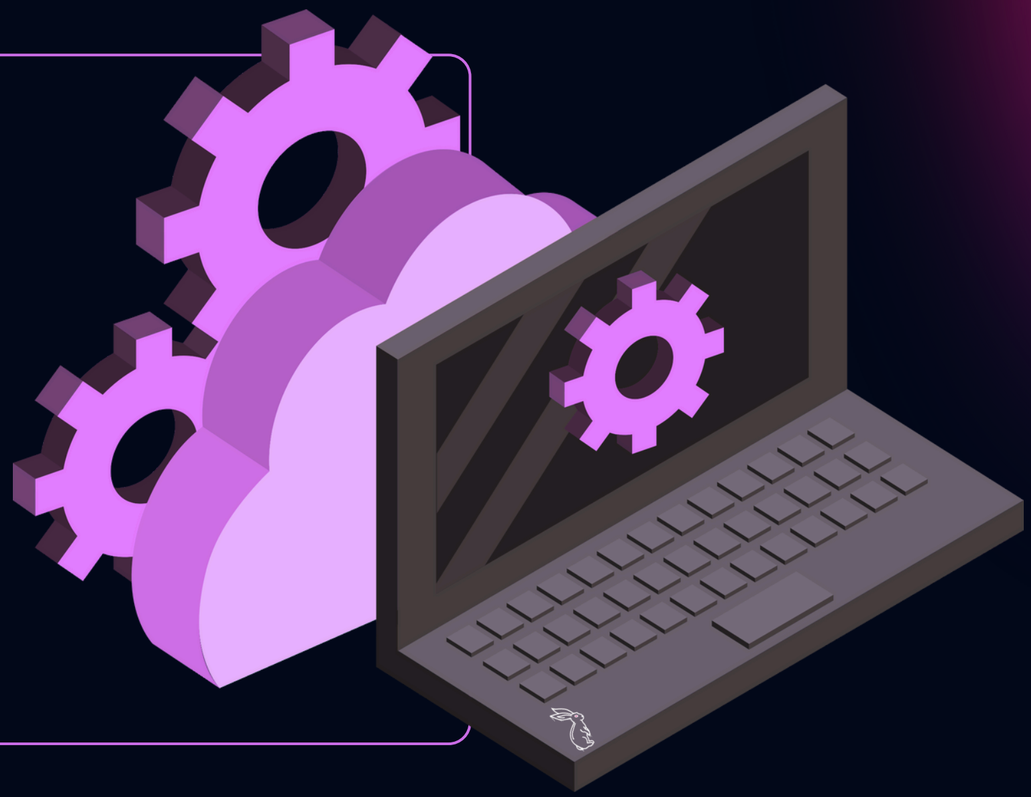
1. Log in to Kindo. You'll find the login instructions at the top of the handout at each station.
2. Arrange the runbook steps in the order you think they should be in. All steps may not be used.
3. Once your steps are arranged, add blocks to your runbook within Kindo.
4. Run your runbook and watch the scoreboard change as you progress through the challenge.

SCENARIO

It’s 3:17 AM, and Ahmed, the night-shift analyst, is facing his worst enemy—a flood of alerts. Over 600 alerts in the past hour alone. Most of them are harmless noise—a printer searching for a lost driver, someone typing the wrong password, a VPN session failing after a network hiccup, an automated backup job triggering an unusual file access pattern, a misconfigured script generating repeated authentication attempts, a legitimate software update causing unexpected process execution, or an IoT device reconnecting after a brief network dropout. But buried somewhere in that flood is a real incident—a malicious Ingress has appeared. It’s a sign of a Kubernetes cluster takeover, but Ahmed doesn’t know it yet. The true signal is lost inside the ocean of noise.

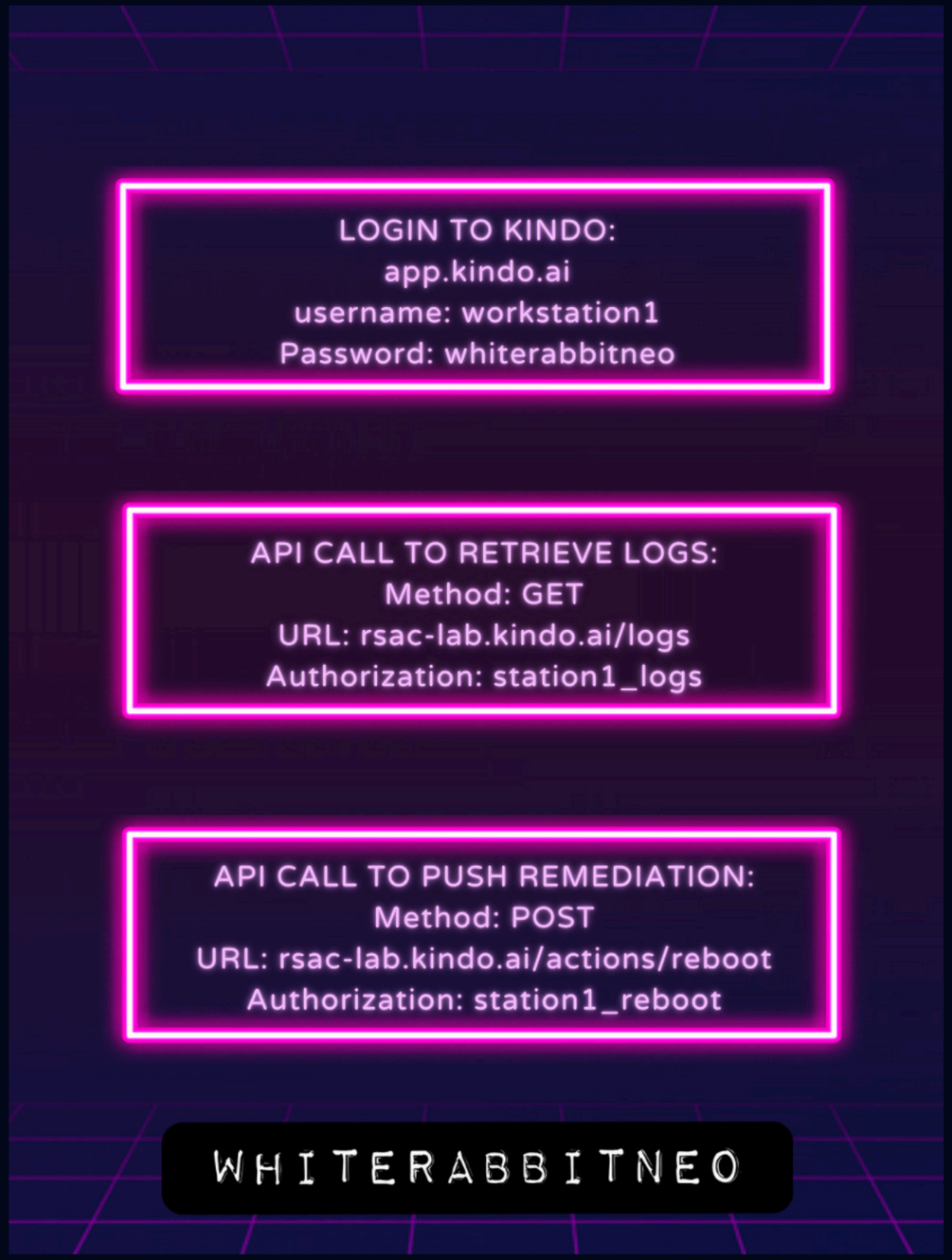
RUNBOOK PROMPT

This runbook is triggered to run upon receiving log files from a server. When these logs are received, the runbook should query a vulnerability database, determine the vulnerability, recommend a fix, and then push that fix to production.



HANDOUT

please refer to your physical handout for your actual credentials



WHITERABBITNEO X
ADVERSARY VILLAGE

THANK YOU

QUESTIONS?

WHITERABBITNEO.COM

Presented by:

Bailey Williams & Ken Kato