SPECTEROPS

Attack Path Management

THE BLOODHOUND ENTERPRISE WAY

TODAY'HOST

BLOODHOUND
ENTERPRISE

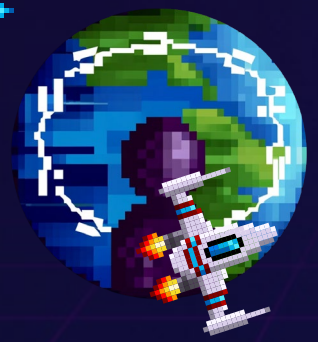
Q&A

KAY
DASKALAKIS

- SOLUTIONS ARCHITECT
- INCIDENT RESPONSE
- COMPROMISE RECOVERY

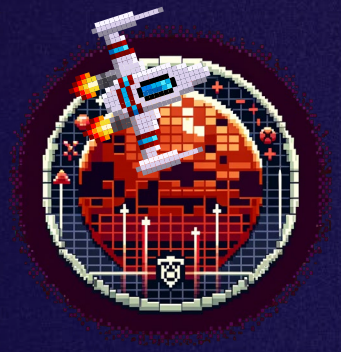
MISSION BRIEF

Total Duration: 45 Mins



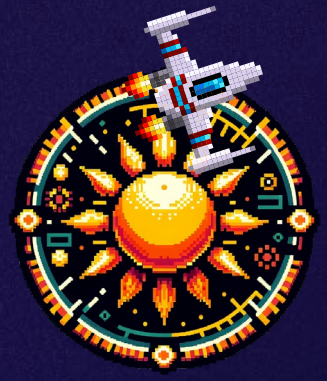
Identity Attack Paths

LEVEL 1



Threat Informed Defense

LEVEL 2



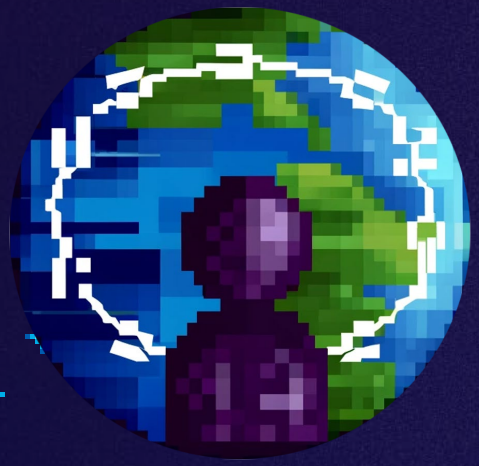
Attack Path Management

LEVEL 3

DEMO

DEMO

DEMO



Identity Attack Paths

LEVEL 1

SPECTEROPS

SPACE-COLD FACTS

Identity Attack Paths

LEVEL 1

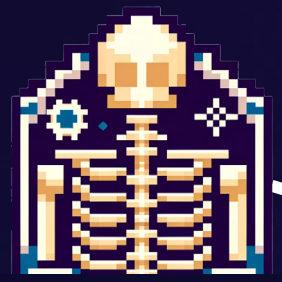
Active Directory

- Initial access doesn't matter
- Misconfigurations are by design
- Hiding in plain sight is easy
- CVEs are resilient and respawn
- Improving detection does not add immunity

UNIVERSAL TRUTHS

Identity Attack Paths

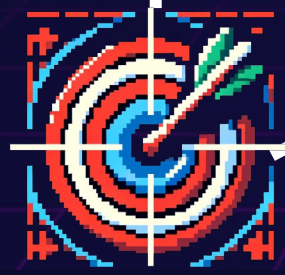
LEVEL 1



IDENTITY BACKBONE

NOT GOING AWAY

Active Directory



PRIMARY TARGET

TECHNICAL DEBT

HIDDEN TRUTH

Identity Attack Paths

LEVEL 1

ACTIVE DIRECTORY WAS NEVER DESIGNED TO SERVE AS A

CONTEXTUAL ACCESS SYSTEM

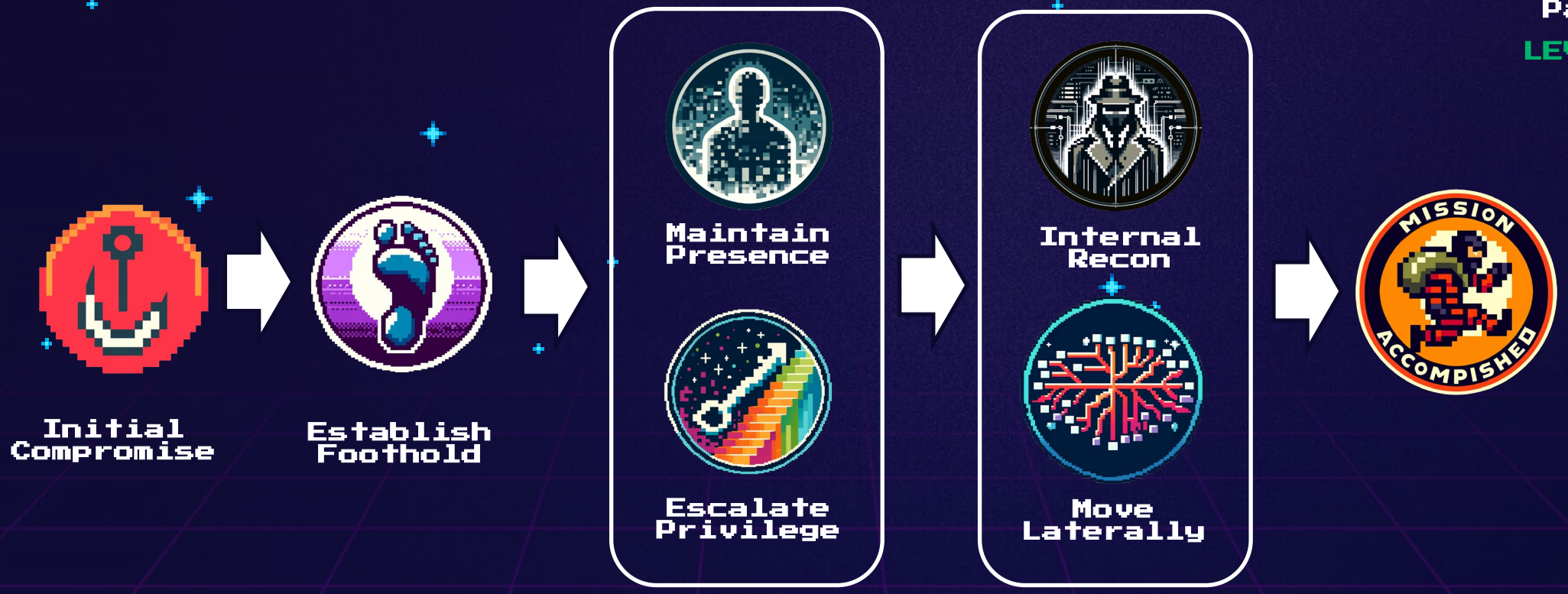
CAN I REALLY ENFORCE ZERO TRUST?

DOES HYBRID IDENTITY MAKE IT ANY BETTER?

ATTACK PATHS (IN GENERAL)

Identity Attack Paths

LEVEL 1



A SERIES OF LOGICAL STEPS ATTACKERS TAKE TO ACHIEVE THEIR OBJECTIVES

Source: Mandiant, Targeted Attack Lifecycle (Compromise Recovery Insights Section)

ONE RING TO... BIND THEM

Identity Attack Paths

LEVEL 1

1 OUT OF 3

ACCOUNT ABUSE

71%

Identity

CRITICAL INFRA

70%

KERBEROASTING

100%

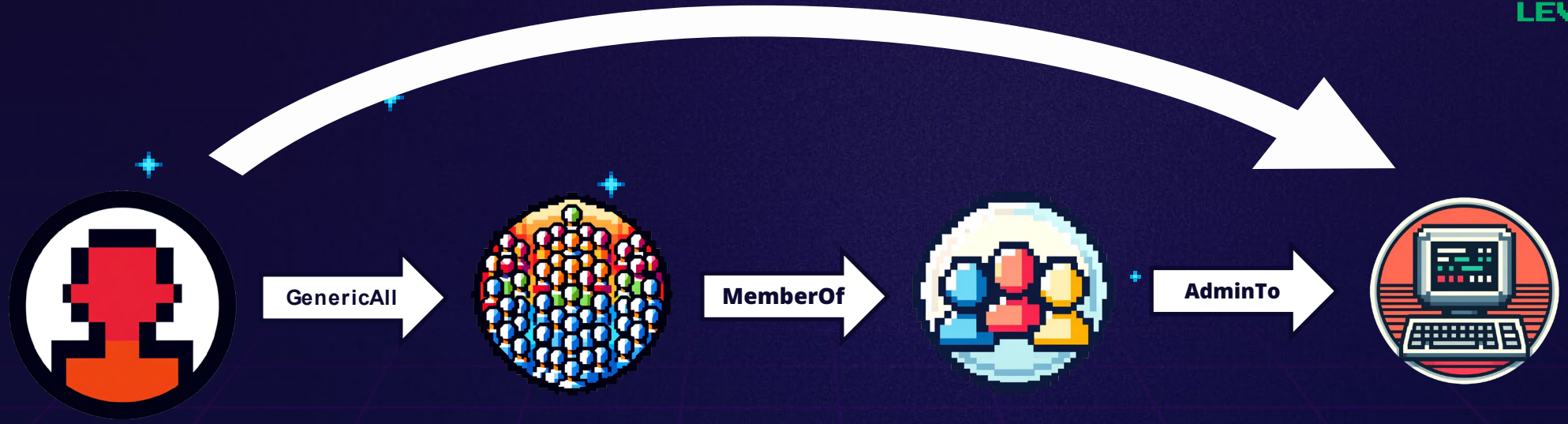
SPECTEROPS

Source: IBM Report Identity Comes Under Attack, Straining Enterprises' Recovery Time from Breaches (Feb 21, 2024)

ATTACK PATHS

Identity Attack Paths

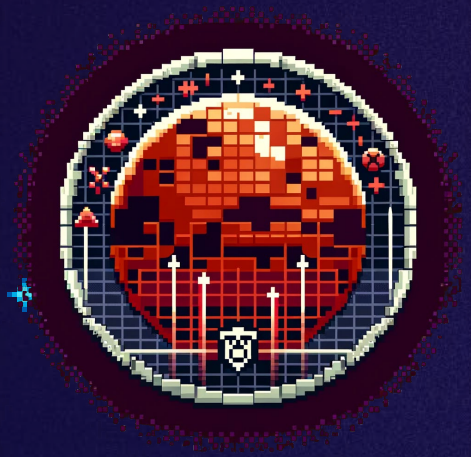
LEVEL 1



ATTACK PATHS BY SPECTEROPS

*Attack Paths are the **chains** of **abusable privileges** and **user behaviours** that create direct and indirect connections between resources and identities.*

SPECTEROPS



THREAT INFORMED DEFENCE

LEVEL 2

SPECTEROPS

SECURITY AS A JOURNEY

Threat Informed Defense

LEVEL 2

SUPER SECURE SYSTEM

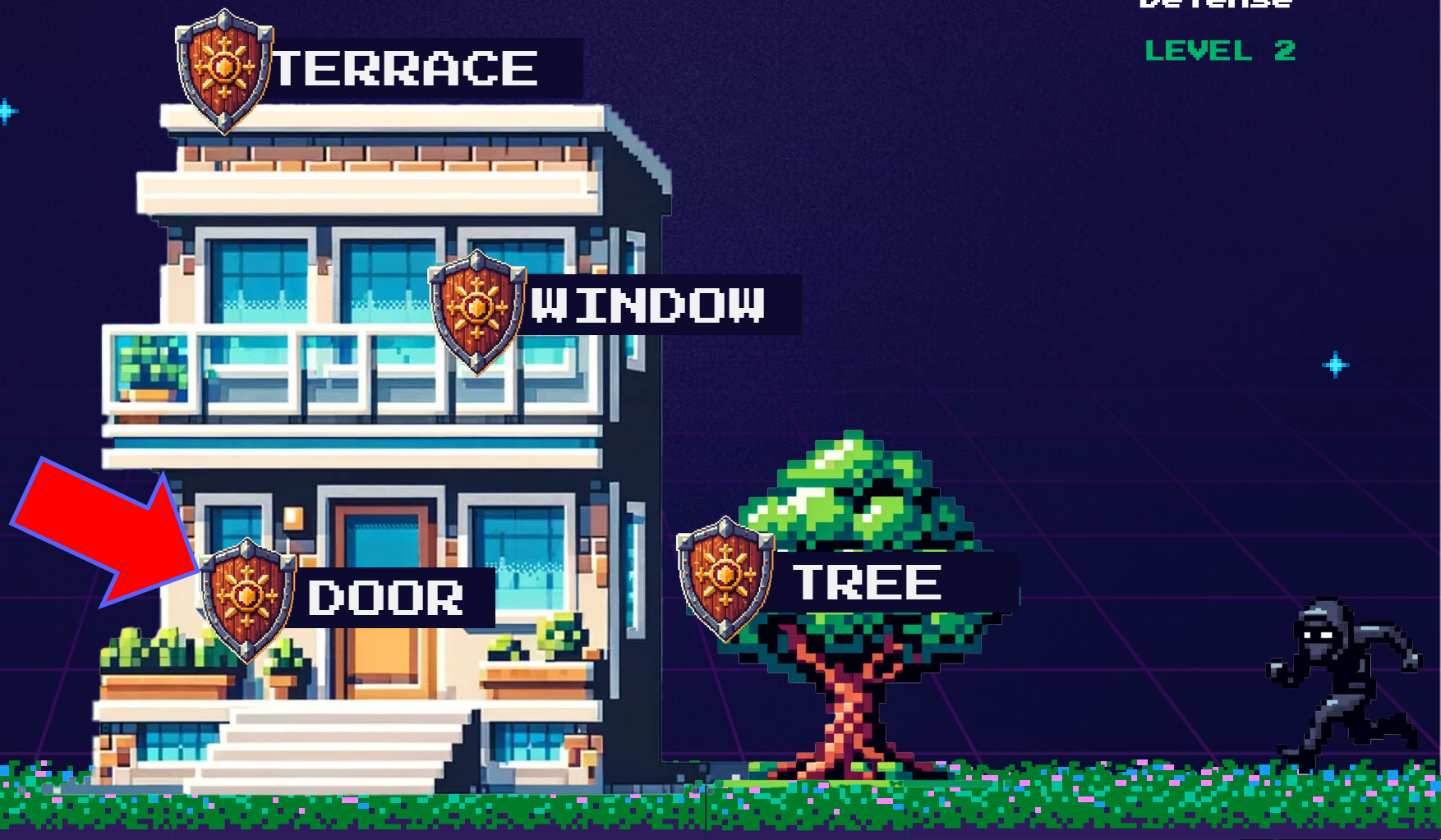
DEFINE YOUR SACRIFICE

FOCUS ON APPROPRIATE CONTROLS

A GAME OF PROBABILITIES

Threat Informed Defense

LEVEL 2



SPECTEROPS

NUMBERS THAT MATTER

Threat Informed Defense

LEVEL 2

29K

CVEs

VULNERABILITY CENTRIC APPROACHES ARE **IMPRACTICAL**

49

Enterprise ATT&CK Techniques

ADVERSARY BEHAVIOURS **DO NOT** RELY ON EXPLOITABLE VULNERABILITIES

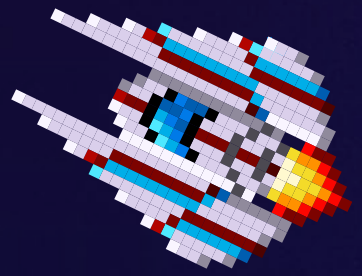
Sources: (1) Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2024 YTD (Jan 9, 2024) (2) MITRE ATT&CK: New Techniques added between October 25, 2022 to April 22, 2024

SPECTEROPS

LIVING OFF THE LAND

Threat Informed Defense

LEVEL 2



I will defend!

We are good!

ONCE INITIAL ACCESS IS ACHIEVED

ADVERSARIES ARE NO DIFFERENT FROM USERS

Disclaimer: No cats were harmed by Bloodhounds during this presentation

DEMYSTIFY...THE ATTACKER

Threat Informed Defense

LEVEL 2

BEST WAY TO **INFORM** DEFENCE ?

SYSTEMATICALLY

LEARN

ADOPT

ADVERSARY TRADECRAFT & TECHNOLOGY

SPECTEROPS

SO WHY NOT USE BHCE?

Threat Informed Defense

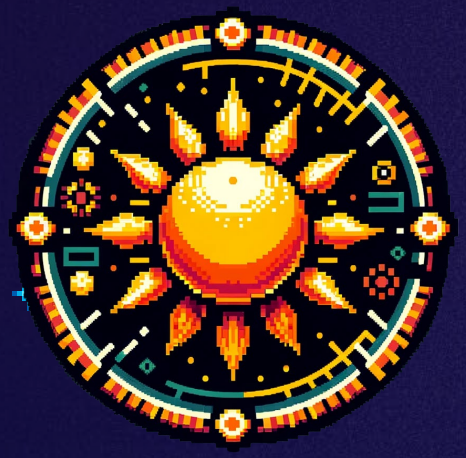
LEVEL 2

BLOODHOUND COMMUNITY EDITION IS

NOT SYSTEMATIC

It is built to enable the **security testing** mission, not defence.

SPECTEROPS



ATTACK PATH MANAGEMENT

LEVEL 3

SPECTEROPS

WHAT IS APM?

Attack Path Management

LEVEL 3

CONTINUOUSLY MAP ATTACK PATHS

IDENTIFY CHOKE POINTS AND ASSESS IMPACT

ATTACK PATH MANAGEMENT

REMEDIATION GUIDANCE

Source: The Attack Path Management Manifesto | by Andy Robbins (May 25, 2021)

APM IN A PROGRAMME

Attack Path Management

LEVEL 3

ATTACK PATH MANAGEMENT

I

I

C

IDENTITY RISK

IDENTITY GOVERNANCE

IDENTITY MANAGEMENT

Reference: CISO MindMap 2024: What do InfoSec Professionals Really Do?

SPECTEROPS

WHAT IS BHE?

Attack Path Management

LEVEL 3

BLOODHOUND ENTERPRISE

FIRST OF ITS KIND

ADVERSARY EXPERTISE

REAL WORLD RESEARCH

DISRUPT LATERAL MOVEMENT

AVOID LOSING CONTROL

Disclaimer (again): No cats were harmed during domain takeover attempts

WHY BHE FOR APM?

Attack Path Management

LEVEL 3

DON'T

- AFTER THE SILVER BULLET
- POINT-IN-TIME IS ENOUGH
- PREFER DETECTION OVER PREVENTION
- SECURITY IS NOT A PRIORITY

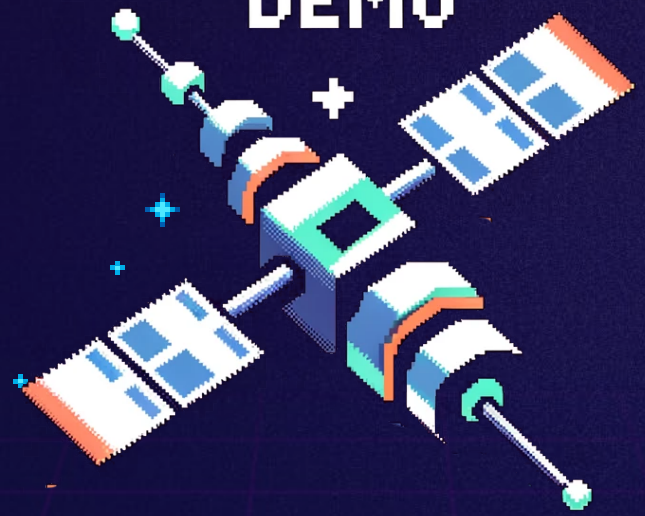
DO

- DEFINITIVE, QUANTITATIVE RESULTS
- PROVEN SCALE AND SPEED
- PIONEERING APPLIED RESEARCH
- CROSS-FUNCTIONAL TOOLKIT

DEMO

SPECTEROPS

DEMO



Q&A

We are hosting our **virtual EU trainings June 24-27**.

Learn more and register at https://ghst.ly/june-trainings. Use the code '**webinarwatcher**' to get 15% off.

SPECTEROPS

THANKS FOR PLAYING

Kay Daskalakis | kdaskalakis@specterops.io

https://bloodhoundenterprise.io/demo/