DEMO @ CyberWest Summit 2024

A live hacking demonstration involving common types of attacks

—

Emu Exploit

Orlando Morris-Johnson - Torry Hogan

Emu Exploit

Who are we?

- #1 Competitive Hacking Team Australia
- Founded 2021, students and professionals
- Goal: Grow cybersecurity in AU & Support Students to break into the space

Today's Presenters:

Orlando (q3st1on)

- CTF Player
- Student @ Uni
- Forklift Certified

Torry (torry2)

- CTF Player
- Student @ Uni
- Security Unprofessional

Emu Exploit @ Security Bsides Perth 2023

Welcome

Thank you to **CyberWest**

Agenda: ~40m (Moving Quick)

1. ~5: Introduction - Context & Why
2. ~20: Demo - Walkthrough & How
3. ~5: Outro - Takeaways & Outcomes
4. ~10: Q&A - Curious & What next

Aim:

- **Understand Hacking & its Importance in Cyber-Resilience**
- **Have fun hacking!**

Find Us:

https://emu.team/linkedin
Connect

https://emu.team/twitter
Follow

https://emu.team/discord
Chat

https://emu.team/about
Info

ACKNOWLEDGEMENT TO COUNTRY

Definition: “hacking”

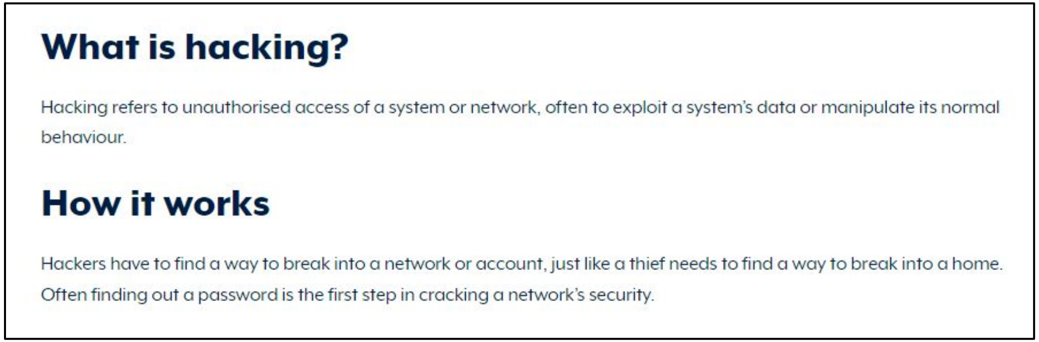
What is it, really?

THEIR CRIME IS CURIOSITY
HACKERS
BOOT UP OR SHUT UP!
UNITED ARTISTS PICTURES PRESENTS AN IAIN SOFTLEY FILM “HACKERS” JONNY LEE MILLER ANGELINA JOLIE FISHER STEVENS AND LORRAINE BRACCO MUSIC BY SIMON BOSWELL
EDITED BY CHRISTOPHER BLUNDEN MARTIN WALSH PRODUCTION DESIGNER JOHN BEARD DIRECTOR OF PHOTOGRAPHY ANDRZEJ SEKULA EXECUTIVE PRODUCER IAIN SOFTLEY CO-PRODUCER JANET GRAHAM
WRITTEN BY RAFAEL MOREU PRODUCED BY MICHAEL PEYSER RALPH WINTER DIRECTED BY IAIN SOFTLEY
READ THE HARPERPAPERBACKS BOOK
UNITED ARTISTS
ON LINE - THIS FALL

Definition: “hacking”

What is it, really?

- “ethical hacking”
- Misconceptions / Cybercrime



What is hacking?

Hacking refers to unauthorised access of a system or network, often to exploit a system’s data or manipulate its normal behaviour.

How it works

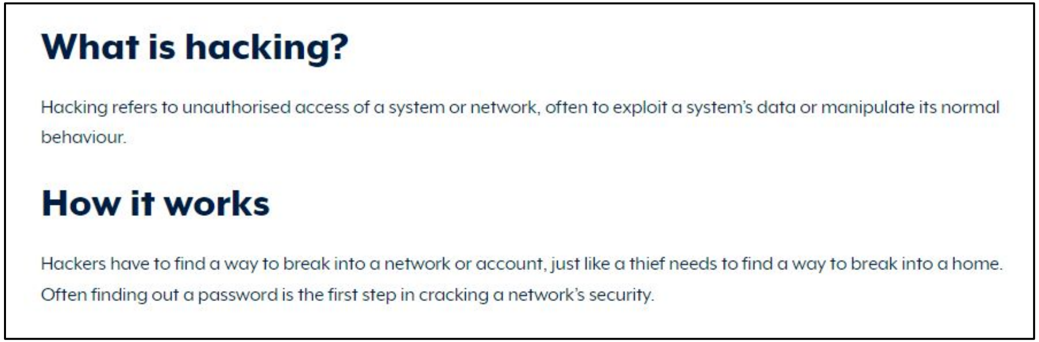
Hackers have to find a way to break into a network or account, just like a thief needs to find a way to break into a home. Often finding out a password is the first step in cracking a network’s security.

https://www.cyber.gov.au/threats/types-threats/hacking

Definition: “hacking”

What is it, really?

- “ethical hacking”
- Misconceptions / Cybercrime



What is hacking?

Hacking refers to unauthorised access of a system or network, often to exploit a system’s data or manipulate its normal behaviour.

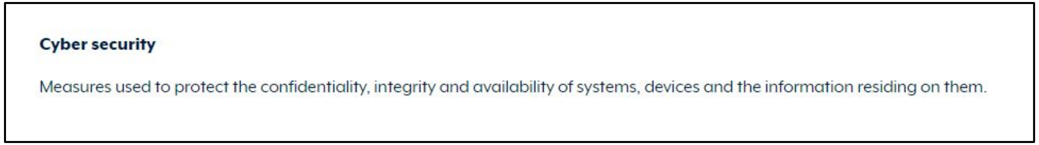
How it works

Hackers have to find a way to break into a network or account, just like a thief needs to find a way to break into a home. Often finding out a password is the first step in cracking a network’s security.

https://www.cyber.gov.au/threats/types-threats/hacking

What do these definitions tell us?

- Attack & Defending
- Frames our approach



Cyber security

Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them.

https://www.cyber.gov.au/learn-basics/view-resources/glossary/c

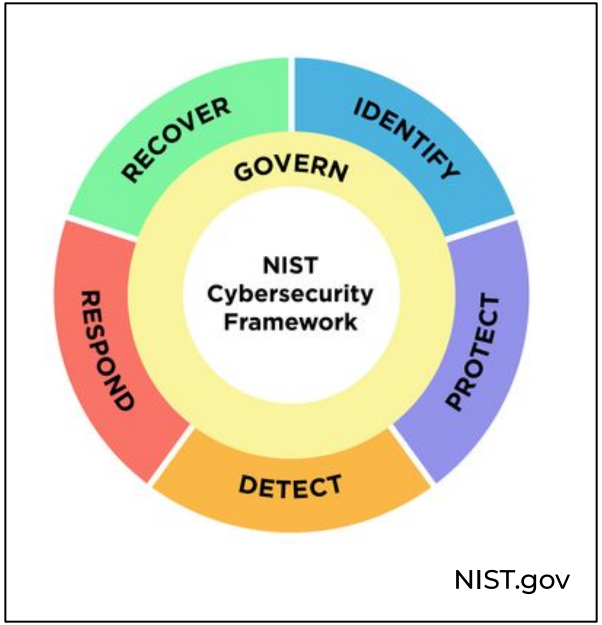
Conventional Wisdom: What it means to defend

Pillars:

- Preventative
- Responsive
- Defensive

“Train, Protect, Respond”

- Straightforward
- This defends extremely well



NIST.gov

How should we build cyber-resilience?

Conventional Wisdom: What it means to defend

Pillars:

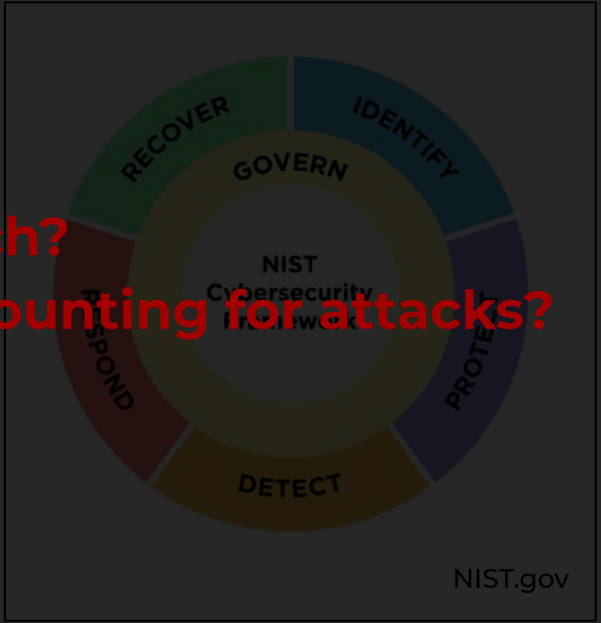
- Preventative
- Responsive
- Defensive

-Are we missing half the approach?

-How is our defence actually accounting for attacks?

“Train, Protect, Respond”

- Straightforward
- This defends extremely well

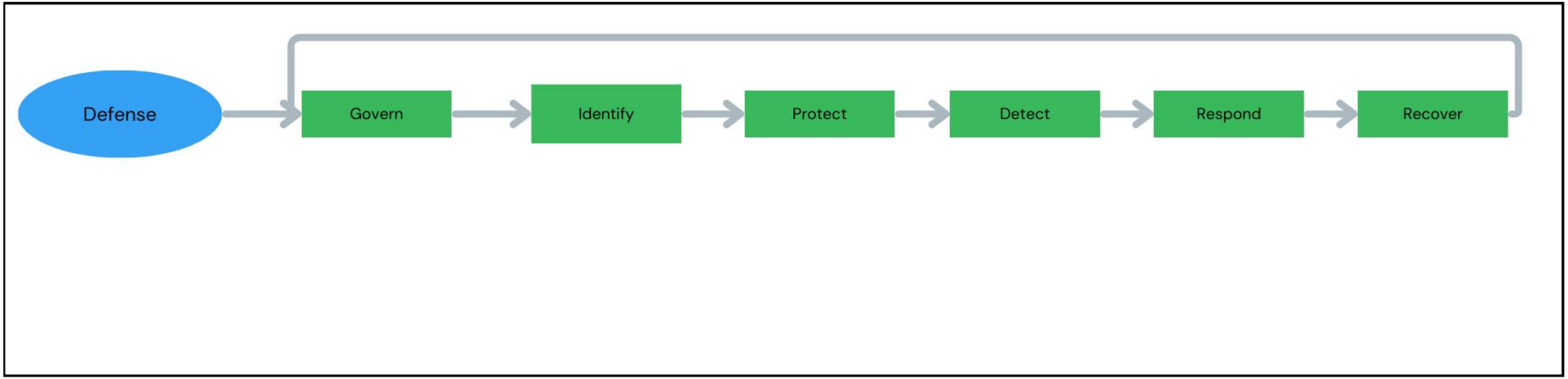


NIST.gov

How should we build cyber-resilience?

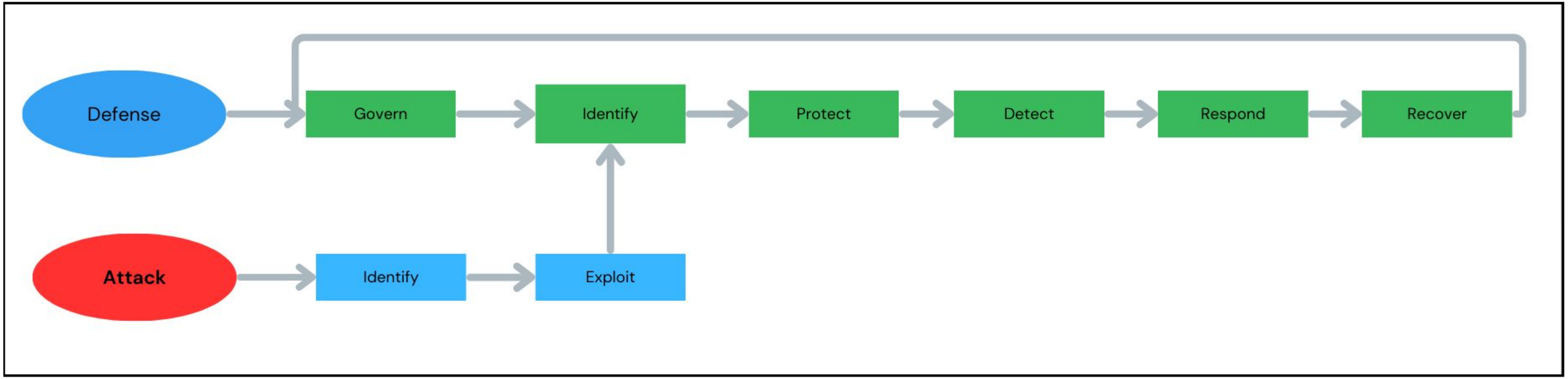
Defending Isn’t Enough: Why this can’t work

We can only defend against attacks we know about.



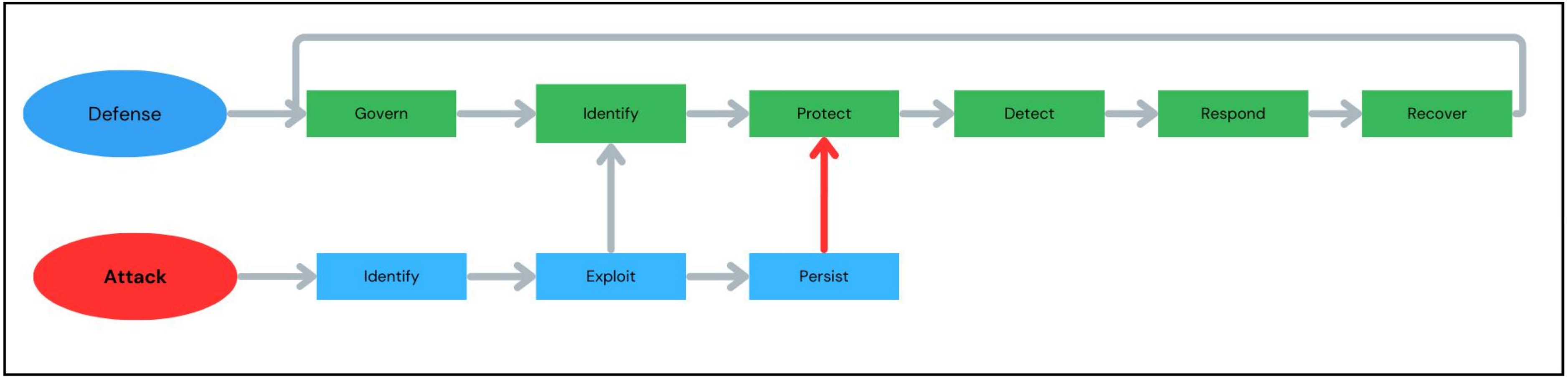
Defending Isn’t Enough: Why this can’t work

We can only defend against attacks we know about.



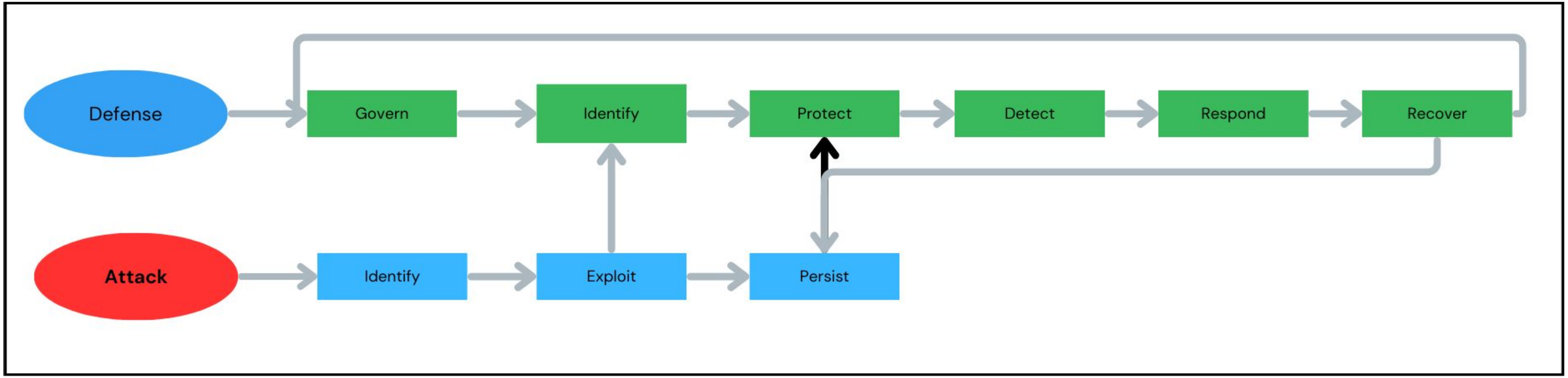
Defending Isn’t Enough: Why this can’t work

We can only defend against attacks we know about.



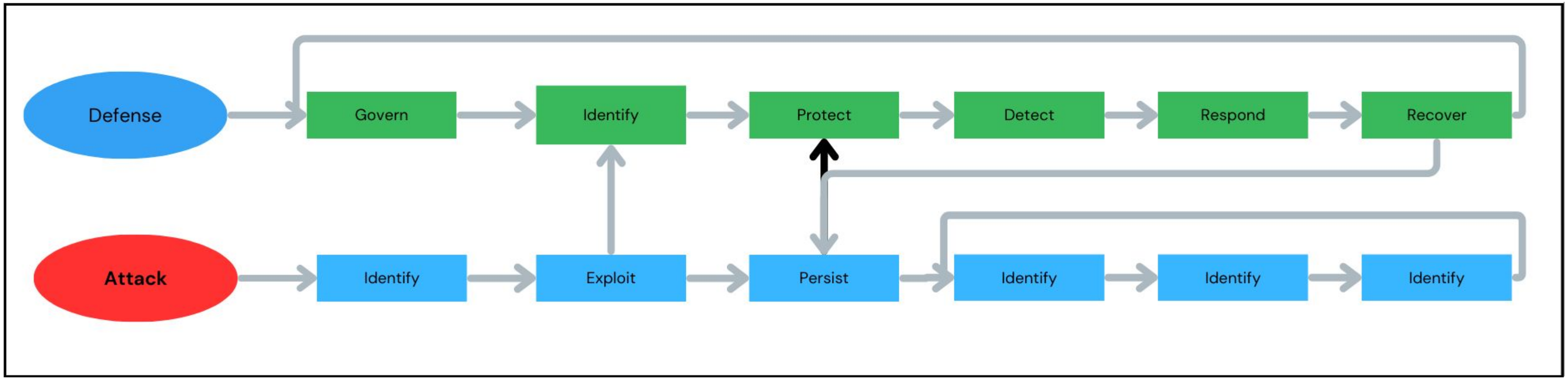
Defending Isn’t Enough: Why this can’t work

We can only defend against attacks we know about.



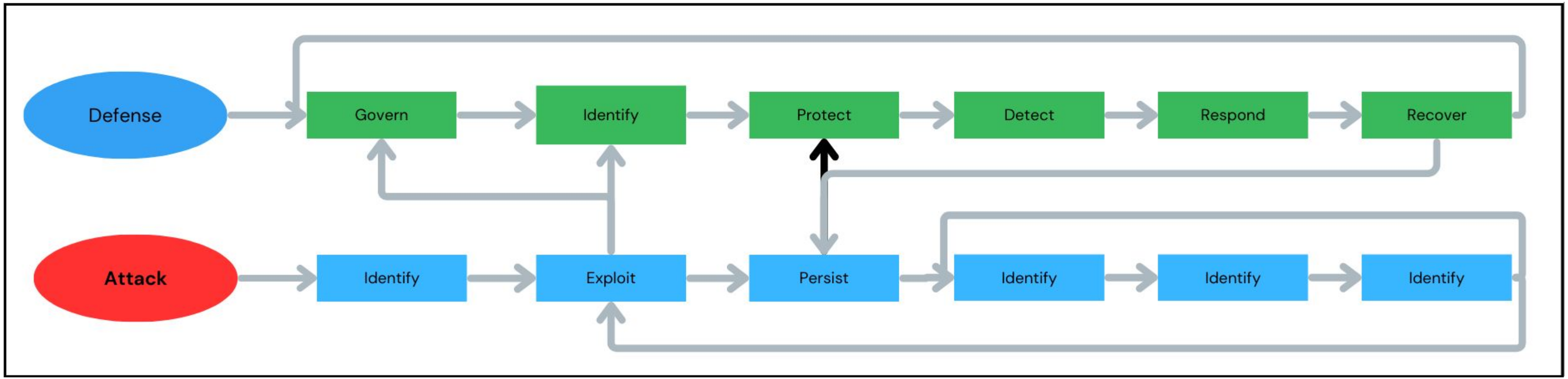
Defending Isn't Enough: Why this can't work

We can only defend against attacks we know about.



Defending Isn’t Enough: Why this can’t work

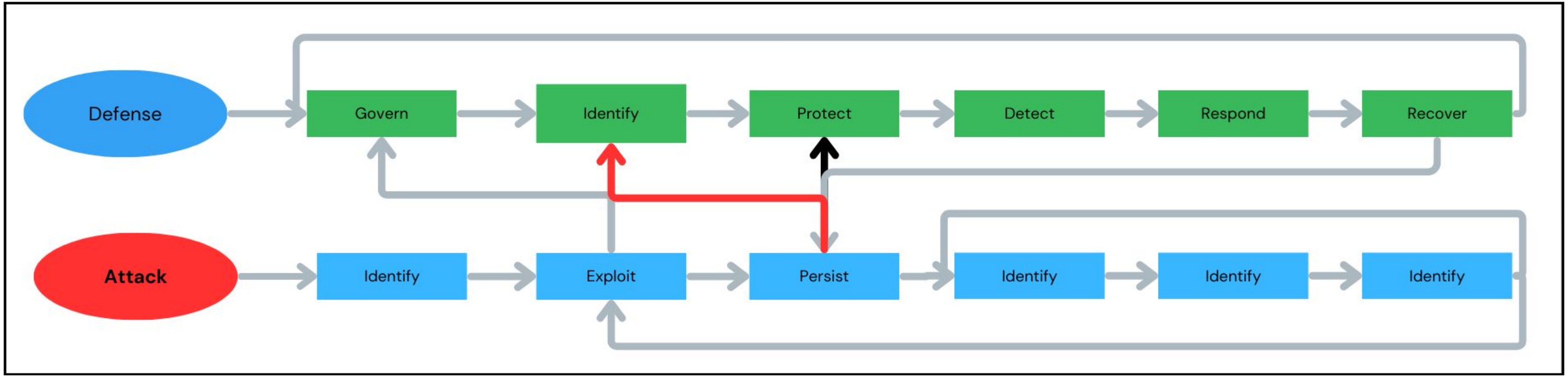
We can only defend against attacks we know about.



Defending Isn’t Enough: Why this can’t work

We can only defend against attacks we know about.

- Attackers **will** beat us unless we cut out the extra steps

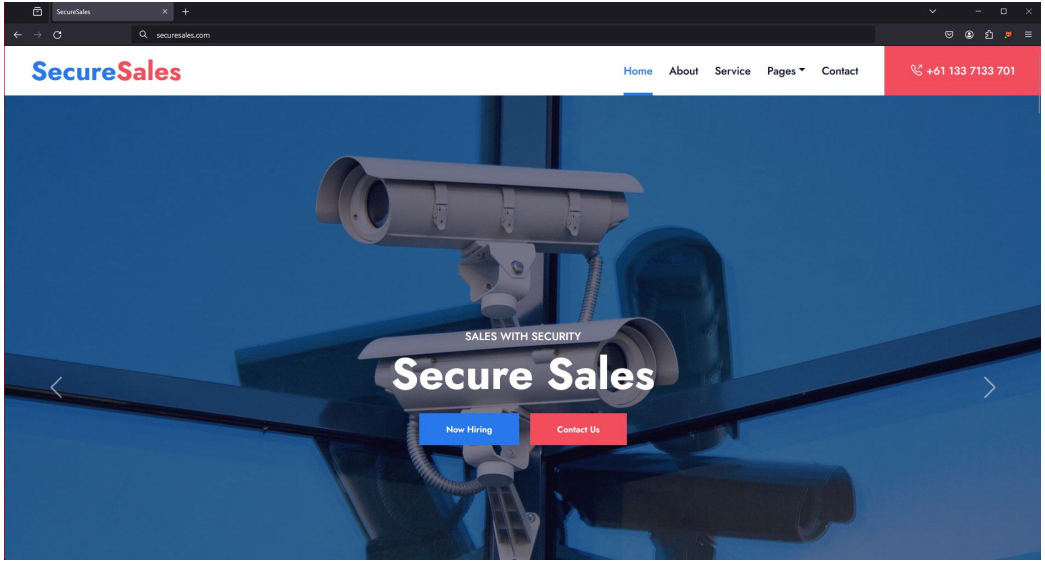


Understanding Attacker's Perspective

Proactive Defence with Offense

Live Demonstration:

Target: “Secure Sales”



- http://securesales.com

[LIVE] [DEMO]

Phase 1: Initial Access	**Phase 2: Compromise**	**Phase 3: Persistence**
Examples: - Web Vulnerabilities (SQL Injection & Directory Traversal) - Backdoors	Examples: - Default/Reused Credentials - Outdated Software	Examples: - Password Cracking - Beyond Compromise
Takeaways: - Threat Landscape Composition - Attack Surface Reality	Takeaways: - Resources across all components - Policy and trusted access	Takeaways: - Proactive/Ongoing Efforts - Inevitable Attack & Compromise

Outcomes:

- **Identified weak points externally**
- **Dug deeper internally**

→

- **“cyberattack” consequences**
- **Long term threat and exhaustive remediation**

Key Takeaways

Attack to Defend

- Win the race
- 6 Pillars apply

Proactive approach

Consider what you’re up against

- Ask your teams;
- Offensive Engagements

https://emu.team/summit

- There's more to hack here, go try it yourself!

You should be hacked.

Just know about it first.

Q&A:

Thank you to **CyberWest**

3:10 pm

EXHIBITION HALL

30 Minutes

Afternoon Tea

All
Delegates

Orlando (q3st1on) — Torry (torry2)

Find Us:

https://emu.team/linkedin
Connect

https://emu.team/twitter
Follow

https://emu.team/discord
Chat

https://emu.team/about
Info

DEMO @ CyberWest Summit 2024

A live hacking demonstration involving common types of attacks

—

Emu Exploit
Orlando Morris-Johnson - Torry Hogan