RETHINKING THE CYBER KILL CHAIN

Hack in the Box

Singapore 2018

Alexis Lavi

lavi.alexis@gmail.com

@LexLavi

These slides are redacted from the original presentation.

If you're interested in the entire content, please contact me.

lavi.alexis@gmail.com
@LexLavi

ENVIRONMENT

2010

Availability

2014

Confidentiality

2018

Integrity

Protect

Detect

Respond

ENVIRONMENT

What is next?

What did we miss?

Where do we go?

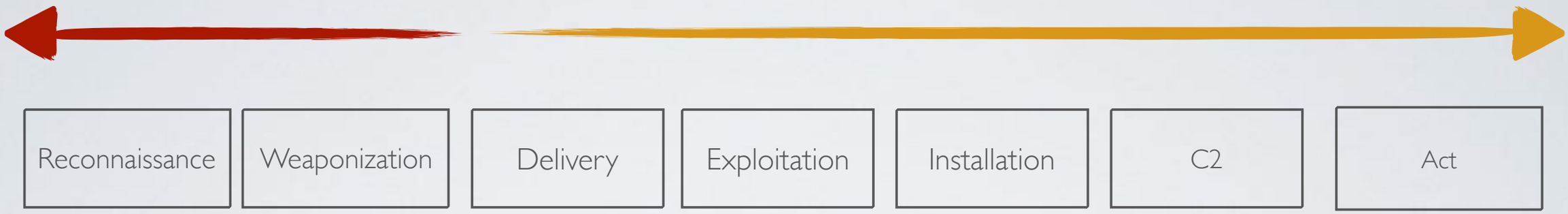
HERE & NOW

Ability to model our attack surface

Avoid predictive snake oil

Prevent security silos

HERE & NOW



+

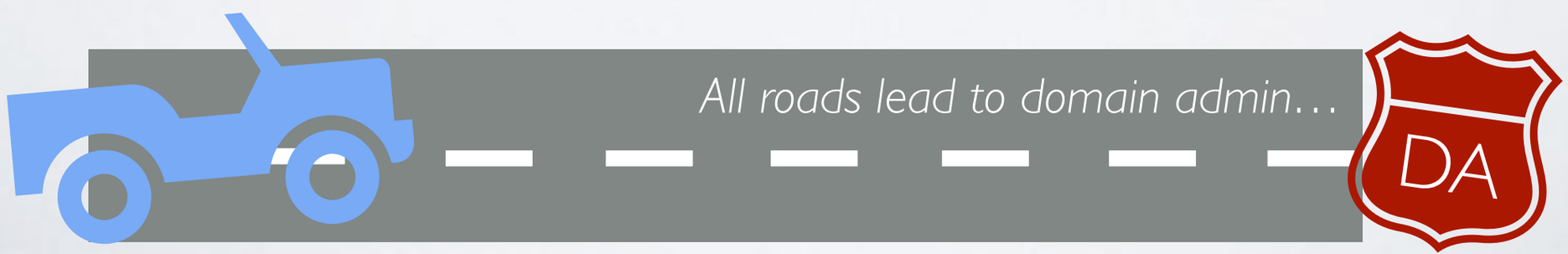
Attack Surface

Exposed areas *that make those systems more vulnerable to cyberattacks. The exposed areas include any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide* ***opportunities*** *for adversaries to exploit weaknesses*

RETHINK

As an attacker, I want to circumvent authentication to an internal app.

Kill Chain	Initial Reconnaissance and Compromise			Establish Foothold / Escalate Privileges / Internal Recon / Maintain Presence			Complete Mission
	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C2	Act
Attack Path	• Social engineer • Unattended computer • Identify default credentials • Sniff traffic • Scan internally	• Modify DB • Steal cookie • Capture cleartext password • Capture hash	• Modify DB • Toolkit/ command	• Impersonate user		• Obtain Domain Admin	• Perform action



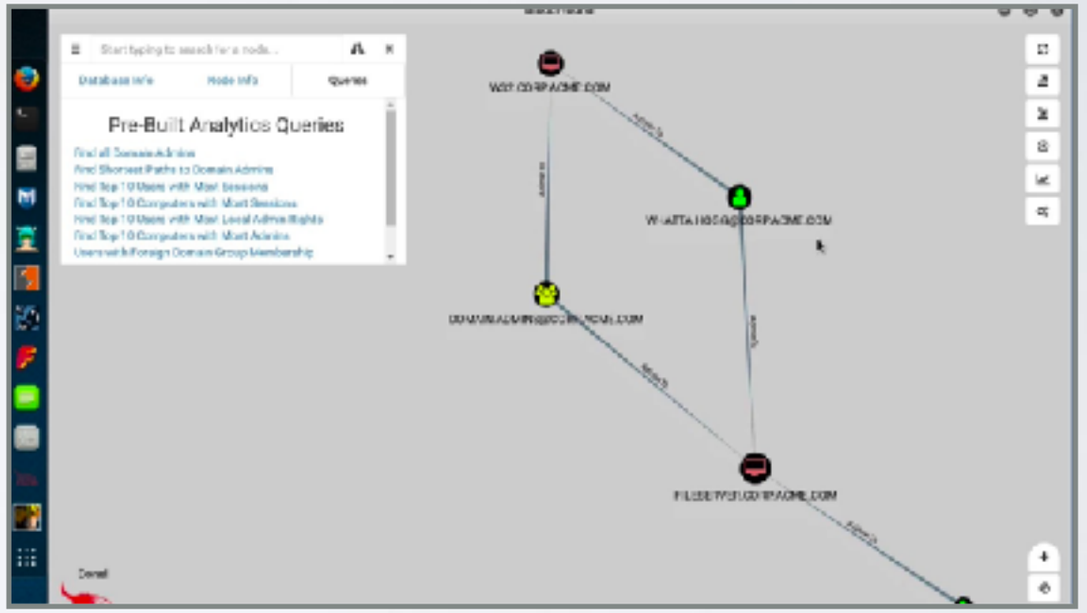
DESIGN

As a defender, I want to protect against pass the hash attacks.

SELECTED COUNTER-MEASURES	Reconnaissance	Weaponize	Delivery	Exploitation	Installation	C2	Act on Objectives
Prevent unauthorized scans: default/deny	●						
Domain admins are not in local admin group		●					
Disable remote logins			●				
Password manager/ unique passwords				●			
Separate accounts for domain admin functions					●		
Enable two- factor for domain admin						●	
Monitor actions of privileged users							●

ENGINEER

*As a defender, I want to **test** against pass the hash attacks.*



Detection Lab

CircleCI: PASSED

Purpose

This lab has been designed with defenders in mind. Its primary purpose is to allow the user to quickly build a Windows domain that comes pre-loaded with security tooling and some best practices when it comes to system logging configurations. It can easily be modified to fit most needs or expanded to include additional hosts.

CAVEATS

Historical Cases

Cloud is Different

Defense is Hard

Manual Approach

Not Predictive

2020

- **Rethink**
- **Design**
- **Engineer**