

Understanding the Attackers and Their Methods



Dale Meredith

MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: [@dalemeredith](https://twitter.com/dalemeredith) | LinkedIn: [dalemeredith](https://www.linkedin.com/in/dalemeredith) |

“I don’t even call it violence when it’s self-defense, I call it intelligence.”

Malcolm X

Rapid Growth in Tech = Trouble

What ethical hackers do for companies

Review systems and infrastructure

Test current security

Create solutions

Retest

You **HAVE** to answer questions like:

What can be seen?

What is being monitored?

What can be done?

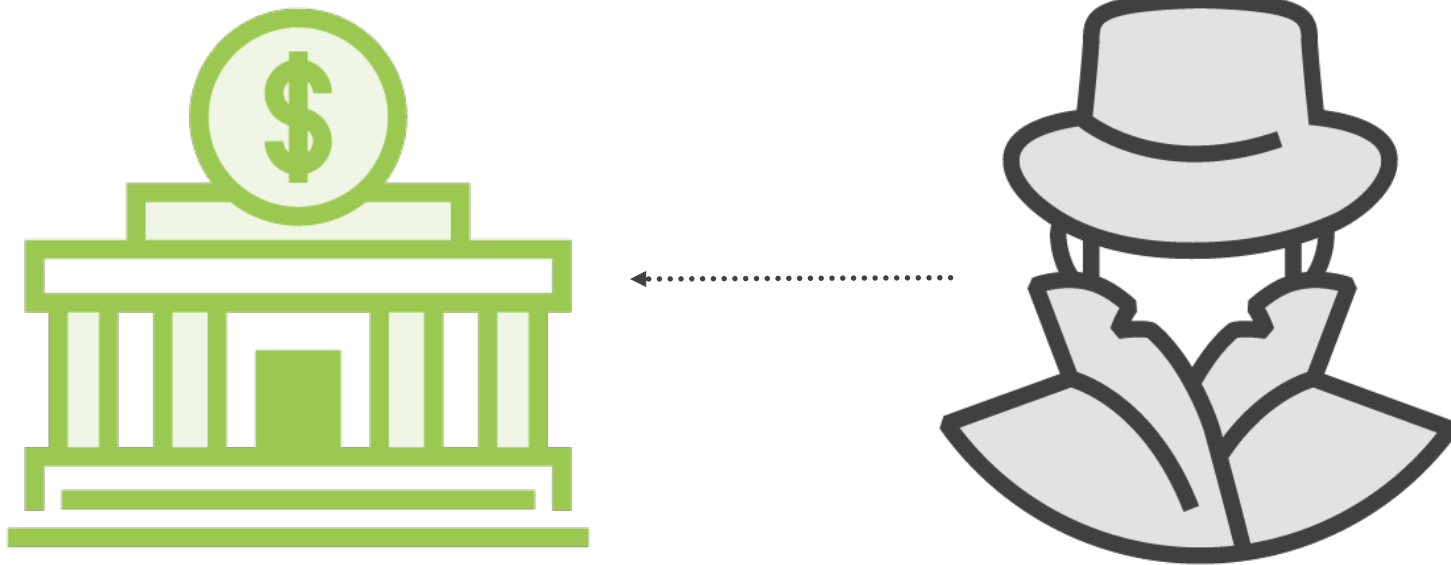
Is there adequate protection?

Are compliances met?

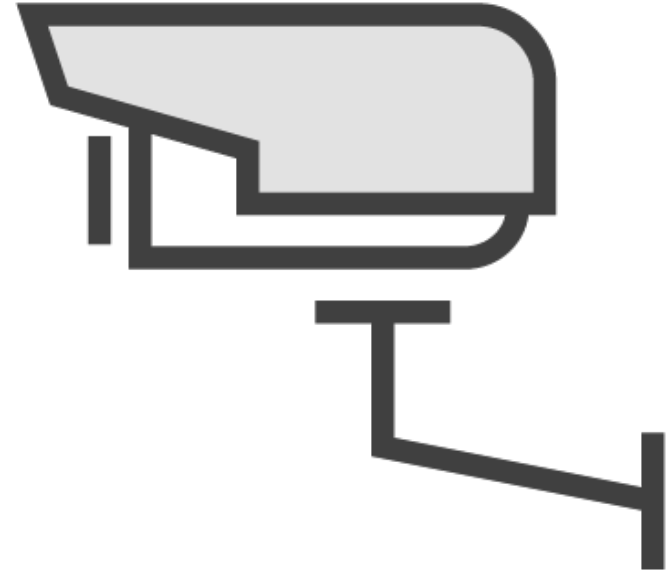
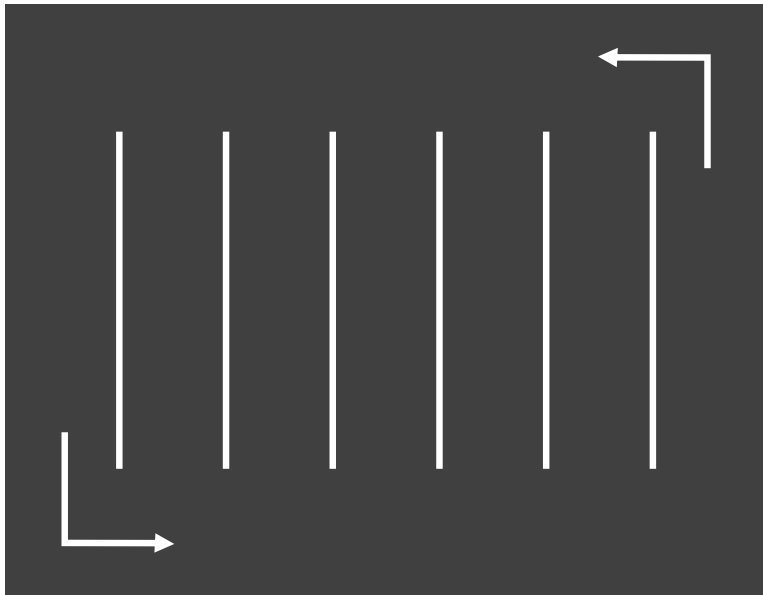
Is Ethical Hacking necessary?

What Is “Defense in Depth”?

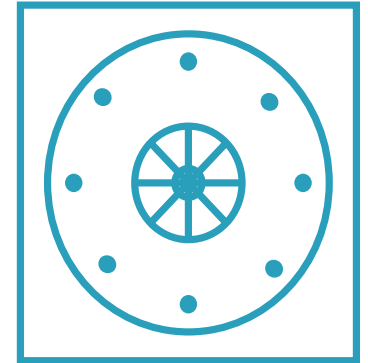
Let's Put on Different Hats for a Second



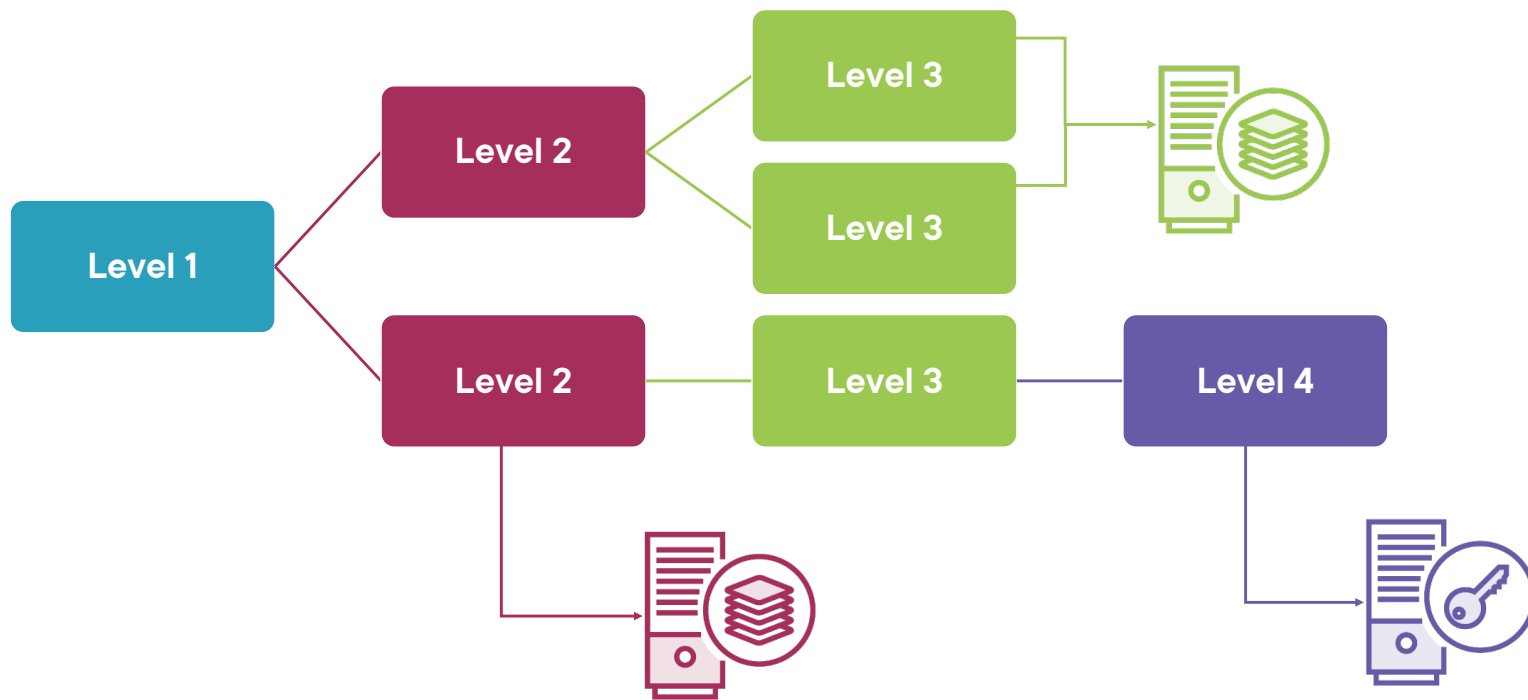
Let's Put on Different Hats for a Second



Let's Put on Different Hats for a Second



Layers, Like Onions

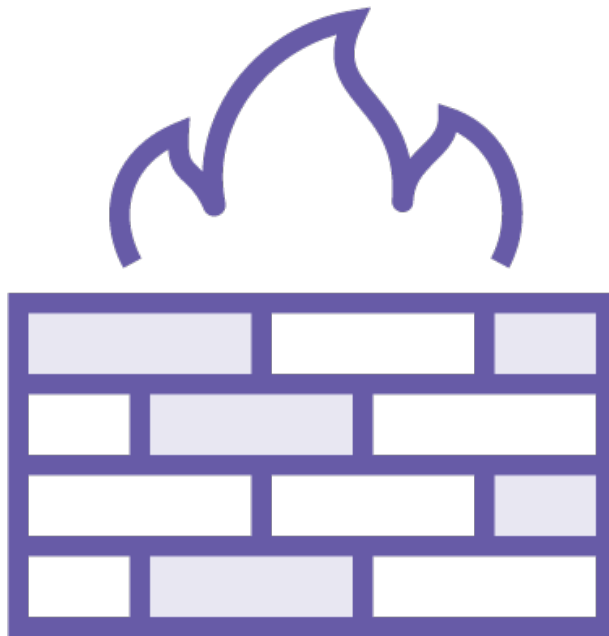


The Last Stand



<https://t.me/learningnets>

The Last Stand

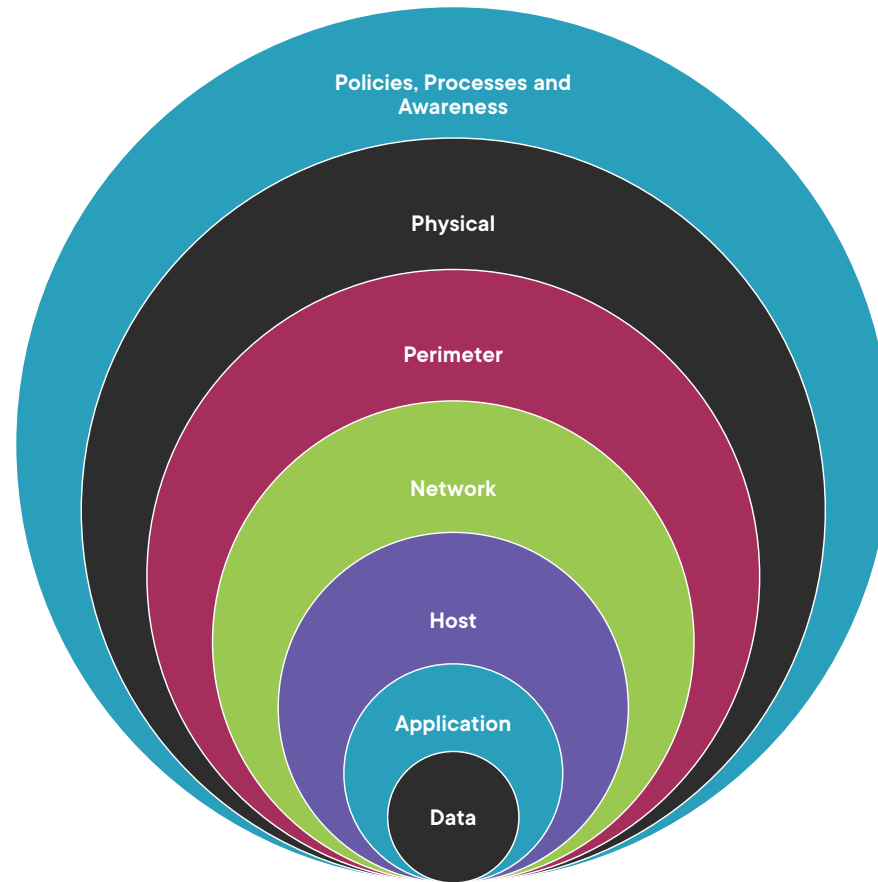


Gentlemen, prepare to defend yourselves!

-Sergeant Major Plumley (We Were Soldiers 2002)

The Levels of Defense in Depth

“You’ve Leveled Up”



Consider This



Never ignore the edge



Follow the workflow



Zero Trust Security Posture

What Is the Risk?

Risk = Threats x Vulnerabilities x Impact

Level	Consequence	Action
Extreme / High	Serious	Immediate action is required
Medium	Moderate	Action should be prioritized
Low	Negligible	Preventive steps

Risk Levels

Probability	Consequences					
	Insignificant	Minor	Moderate	Major	Severe	
81 - 100%	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 - 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High

Risk Matrix

Threat Modeling

Threat Modeling Adversary Capability

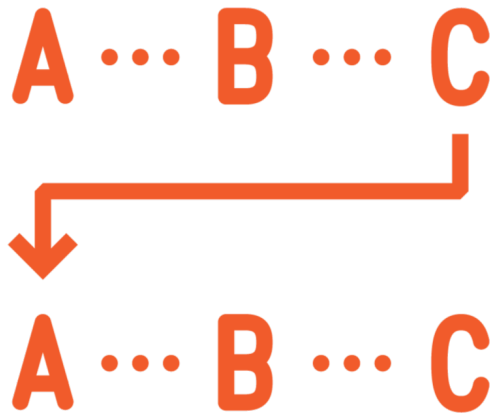


Identify threats

Identify vulnerabilities

Improve your security designs

Things to Keep in Mind



Adversary Capability

Identify security objectives

Application overview

Decompose the application

Identify threats

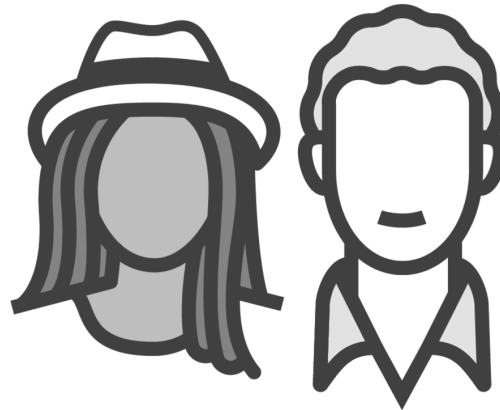
Identify vulnerabilities



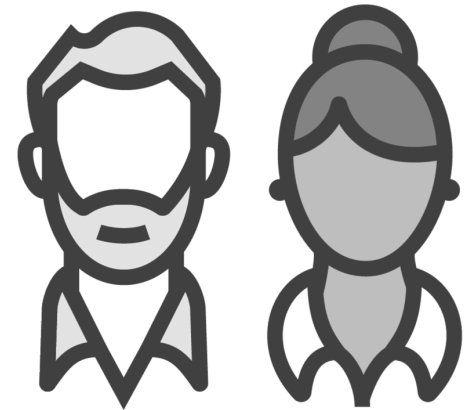
Identify Roles



Read



Update

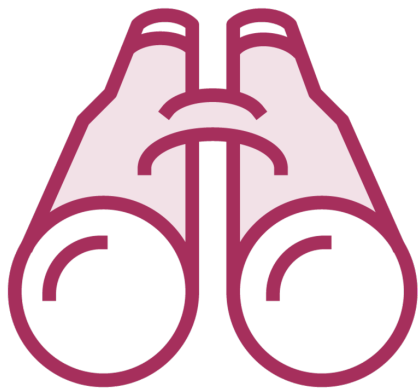


Delete

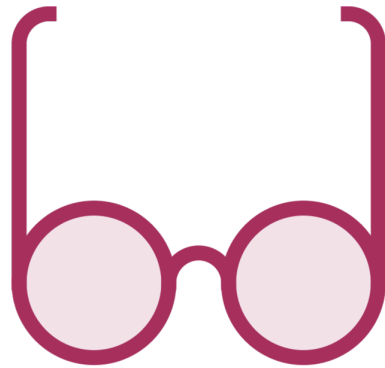
Probability		Consequences				
		Insignificant	Minor	Moderate	Major	Severe
81 - 100%	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 - 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High

Incident Management

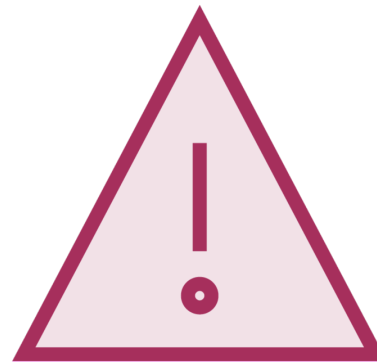
Think Outside the Box



Identify



Analyze



Prioritize



Resolve

The “Why” of Incident Management

**Better service
quality**

Proactive

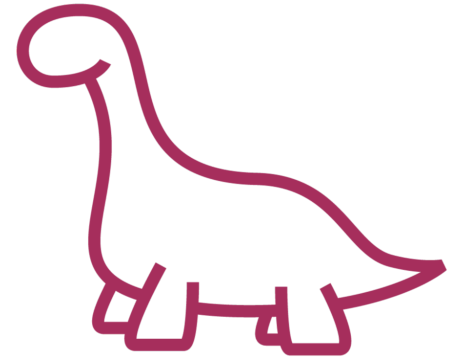
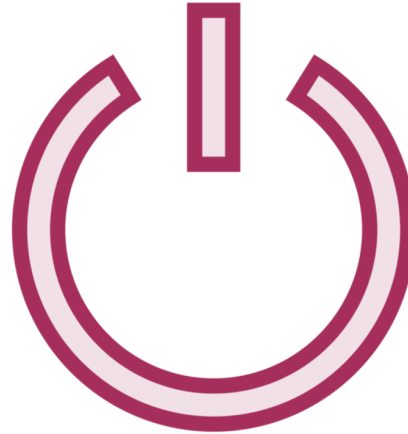
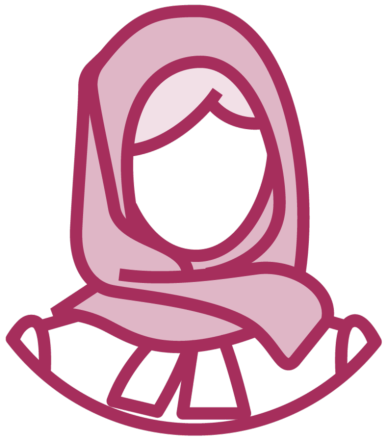
Reduces impact

Meets availability

**More efficient
and productive**

**Customer/user
satisfaction**

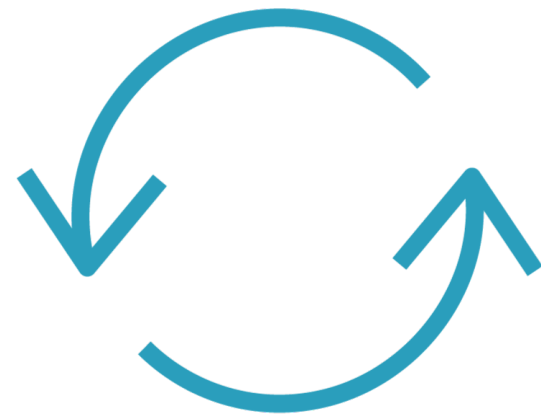
Proactive



The Incident Handling and Response (IH&R)

IH&R Process

- 1 Prepare for Event Handling and Reaction
- 2 Incident Recording and Assignment
- 3 Triage
- 4 Notification
- 5 Containment
- 6 Forensic Examination
- 7 Eradication
- 8 Recovery
- 9 Post-incident Actions



The Role of AI/ML

“I’m Sorry Dale, I’m Afraid I Can’t Do That”



Not just for cars

Beware

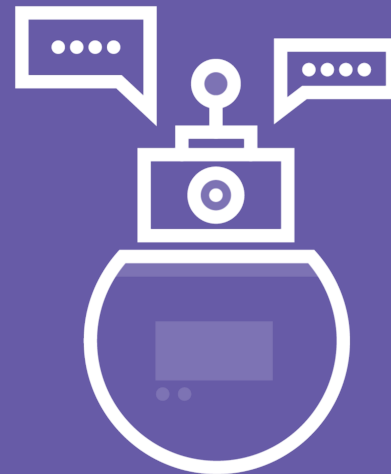
Machine Learning

We're #4

AI is Appearing Everywhere



AI is Appearing Everywhere



Know the Concept of AI and Machine Learning

Can AI and ML Stop Attacks?



Authentication and password protection



Phishing



Threat detection



Vulnerability management



Behavioral analysis

Can AI and ML Stop Attacks?

AI-based antivirus

Botnets

Fraud

Network security

AI vs. AI

Learning Check

Learning Check



Risk



Machine Learning



Risk matrix



Containment



Decompose the application



Eradication

Key Terms



Ways AI and ML prevent attacks



Incident Handling and Response



Risk



Up Next:

Differentiate Information Security Laws
and Standards
