Attacker Cryptonite, How To Threat Model Your Way To A Good Night’s Sleep

Lockdown 2017
Why This Talk

Story
Extraordinary Security Comes From Within
Allows For Security Enablement
I Want You To Sleep
Problem Statement

Your work prioritization is almost always determined by forces outside of your control.
Vulnerabilities Have Become FUD
Lead To Poor Security Practices
Hurt Business Relationships
Money Makers
Vulnerabilities (Continued)

They Are Not Org Specific

Attempts To Score Vulnerabilities For Severity Are Disconnected From The Reality of Exploiting Them
What Do You Look At?

“When you Change The Way You Look At Things, what You Look At Changes”

-Wayne Dyer
Threat Modeling Step 1

Document, don’t create
Network Topology?
Threat Modeling Step 2

Clearly Define All of Your Security Controls Across Your Organization

Don’t Forget things like AD and External MSSPs
Threat Modeling Step 3

Map Your Network Topology To Your Security Controls and Identify Easy Gaps
“If Someone Is Earning 25k a year it is not because they want to it is because they are not aware of how to earn 50k” – Bob Proctor

Attackers Do Why Don’t Defenders?

MITRE ATT&CK Framework
Let's Do Some Math

Network Topology + Security Controls + Framework + Central Logging = Success
Blue Team Ethos

Complete Ownership

This is **YOUR** Environment Not the Attackers

It’s Not About Good Security It’s About Having Frustrating Security
Contact Info

Eric Groce
@IA_Every_Day