Leveraging Information Symmetry and Asymmetry for Effective Cyber Defense

JEFF REAVA

NOVEMBER 11, 2016

Target Audience

Future Practitioners (CISOs, Security Operations and Architects)

- Where to start a program buildout
- How to sustain
- How to adapt

Engineers, Researchers:

- How do defender actions affect attacker behavior?
- Is it easier for an attacker to learn and adapt than the defender?

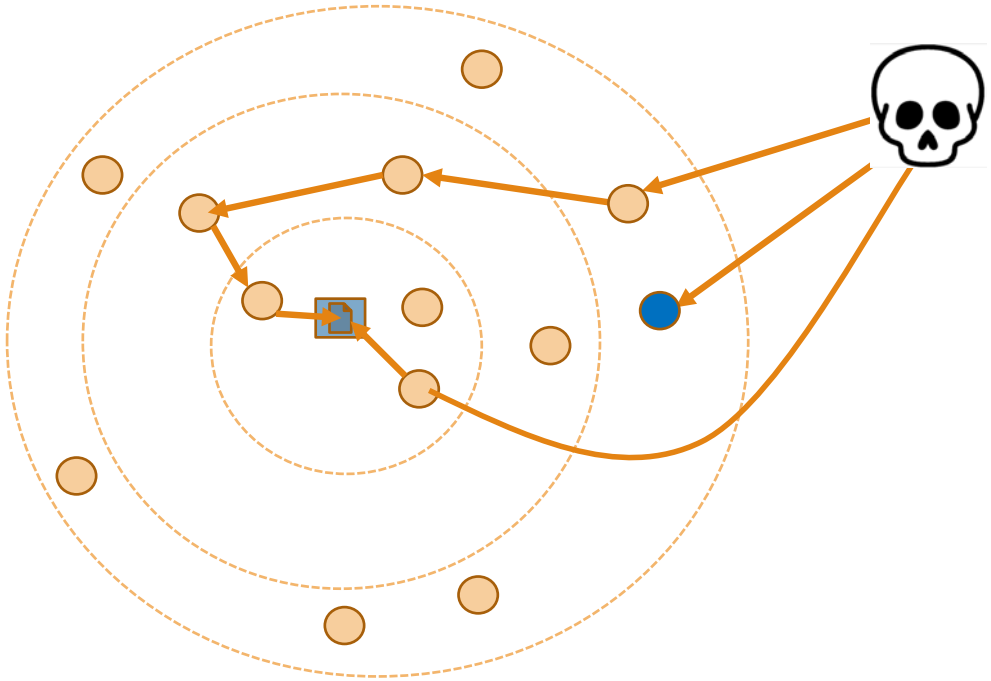
Overview

- Cyber Defense becomes effective when it takes more effort to mount a successful attack than an attacker is willing or able to exert
- Defense in depth is recommended in principle
- In practice, building depth requires time so order becomes important
- Prioritize what to configure, patch, monitor, block, document, proceduralize
- Security posture affects attacker behavior
- Information about security posture has strategic value to the defender, both hidden and known

TL;DR

- Its hard to hide aspects of a security program to patient attackers
- Do what you can to constrain preferred attacker behavior
- Focus effort on attacker behavior you can’t constrain
- Develop and maintain the ability to adapt quickly

Measuring attacker effort



Data Breach

Ransomware

Business Email Compromise

Attacker Cost vs. Defender Cost

Recon

Weaponize

Deliver

Exploit

Install

Command and Control

Actions on Target

Plan

Build

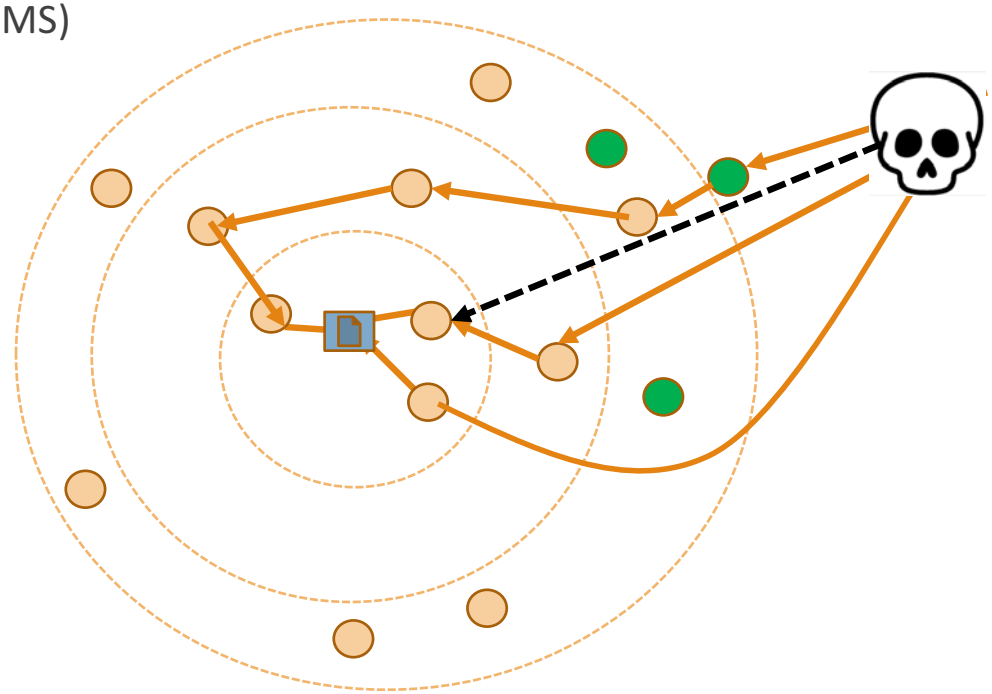
Run

- Detect
- Interpret
- Decision Making
- Response

Control-centric approach

Information Security Management System (ISMS)

- Define scope
- Identify risks
- Select and implement controls
- Manage residual risks

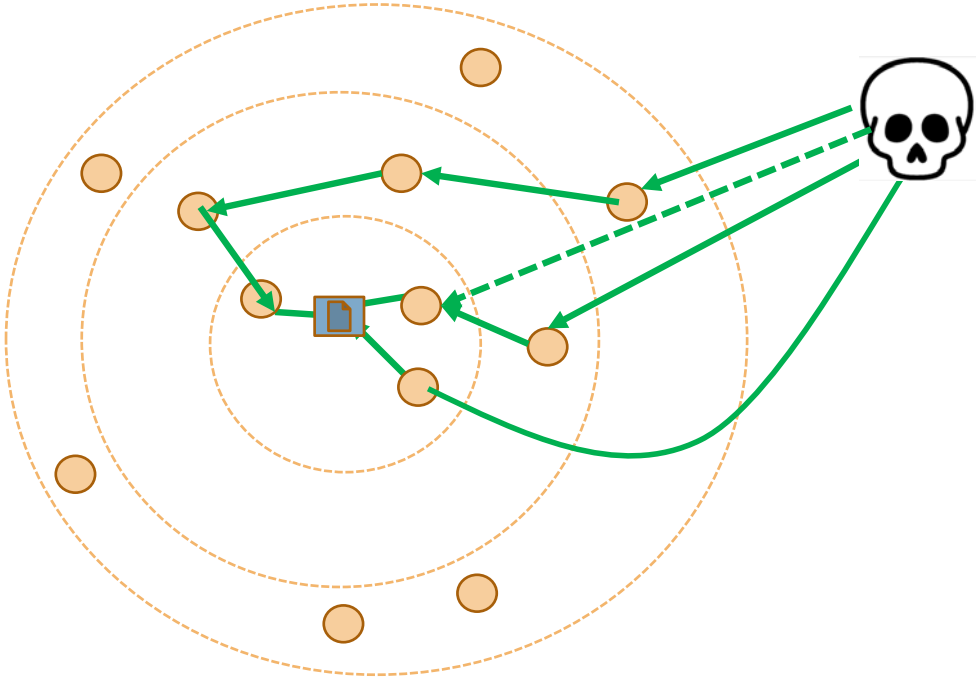


Threat-centric approach

Constrain preferred attacker behavior

Maximize effort to respond

Maintain the ability to adapt quickly



Program Build out: detection + response

Category								
Gateways	76	120	66	39	71	109	106	120
Scanning			7	114	131	140	196	92
Host Defense	9	14	7	3	57	113	98	144
Perimeter Defense						27	63	197
Messaging	3	26	12	17	65	22	33	30
Anomaly Detection		3			33	38	28	77
Insider		2	3		3	17	57	46
Threat Intel							29	50
Unusual Activity								57
IT Related Issues	3	6	5	4	4	9	10	19
Month	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**
Staffing Level	1X			2X			4X	
Training Level	40%			50%			90%	
Procedures	31%			46%			92%	

Detection and Response: 5 Takeaways

- Focus on the edge, run simplified playbook
- Leverage economies of scope: add related capabilities using similar skillsets
- Impose more cost (RWDEICA) than you take on (Plan/Build/Run)
- Block to constrain: monitor and adapt
- Measure to instrument and adjust

Q1

Strengths	Weaknesses
• Endpoint Detection • NBA Capability • SME/Training skill	• Small Staff • Limited Skillset • Tool coverage • Management depth
Opportunities	**Threats**
• Fix 1 thing	• Data Breach • Regulatory / Audit Requirements

- Focus on top attack vector: secure edge
- “Make opponent one-dimensional”
- Block what organization will allow, train and monitor on the rest

Q2

Strengths	Weaknesses
• Training and Onboarding • Threat data	• Limited skillset • Environmental knowledge • Environmental visibility
Opportunities	**Threats**
• Extend capability • Diversify controls • Build management skill • Hire!	• Build v. Run Chaos: - Too many projects - Inadequate response

- Scan and sandbox
- Automate incident response data collection
- Hire and train
- Pen test + review outcomes

Q3

Strengths	Weaknesses
Adequate staffing 24x7 operations Management depth	Change agility Environment visibility (fine grained)
Opportunities	**Threats**
Hunting Staff Development	Management Expectations Silos Problems and Incidents (IT)

- Establish Hunting program: initial narrow scope, depth, frequency
- Training program – curriculum and timeline
- Extend toolset

Next Steps

Strengths	Weaknesses
???	???
Opportunities	**Threats**
???	???