Threat-Based Risk Management

Julian Cohen
Justin Berman

Julian Cohen | @HockeyInJune | http://hake.co/

- Security | Insurance Technology
- Founder | http://playbook.delivery/

Previously

- Product Security | Flatiron Health
- Application Security | Financial Services
- Vulnerability Researcher | Defense Contracting
- Penetration Tester | Boutique Consulting
- Educator | Universities

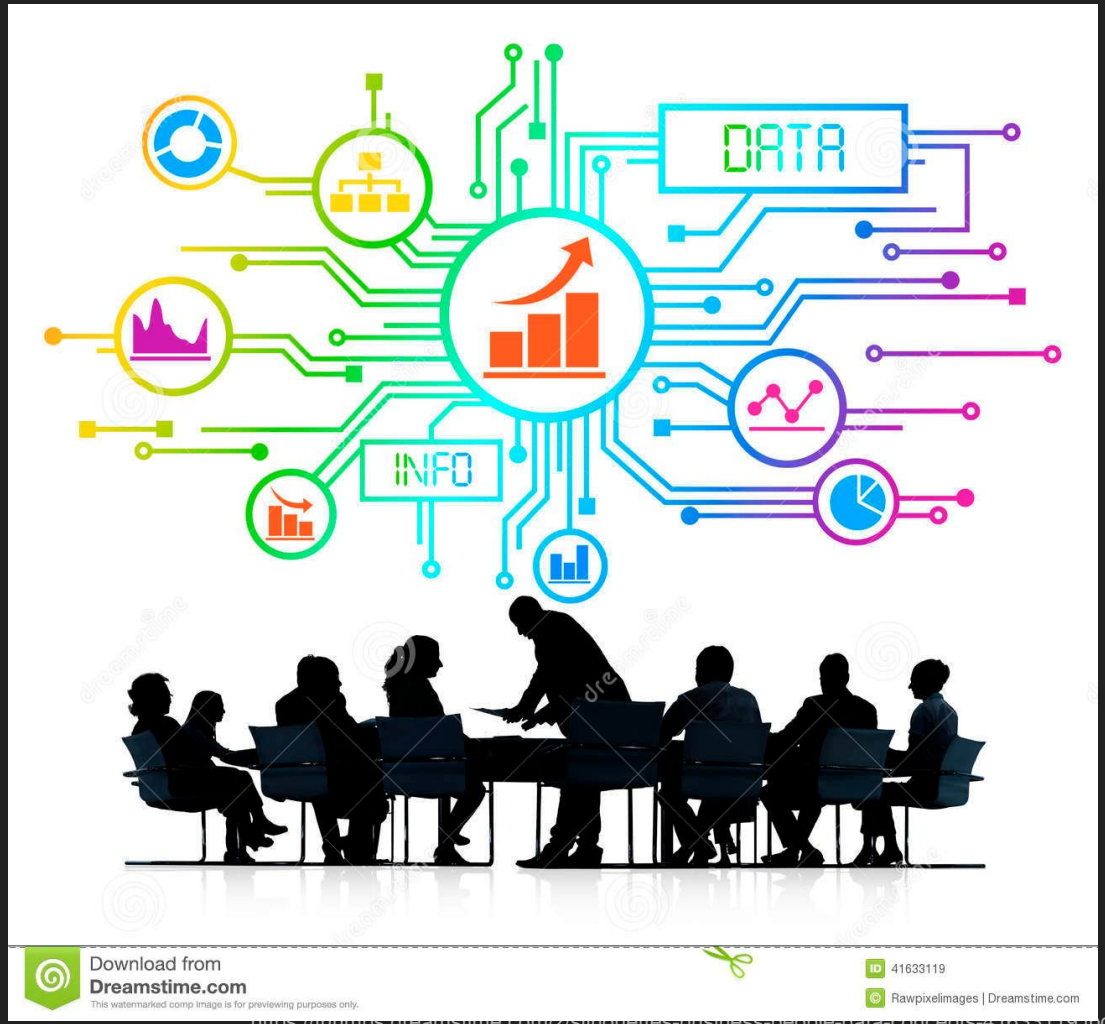
Justin Berman | @justinmberman

- CISO | Zenefits

Previously

- VP of Information Security | Flatiron Health
- Head of Security Architecture | Financial Services
- Principal Consultant | Boutique Consulting
- Application Developer | Hi-Tech

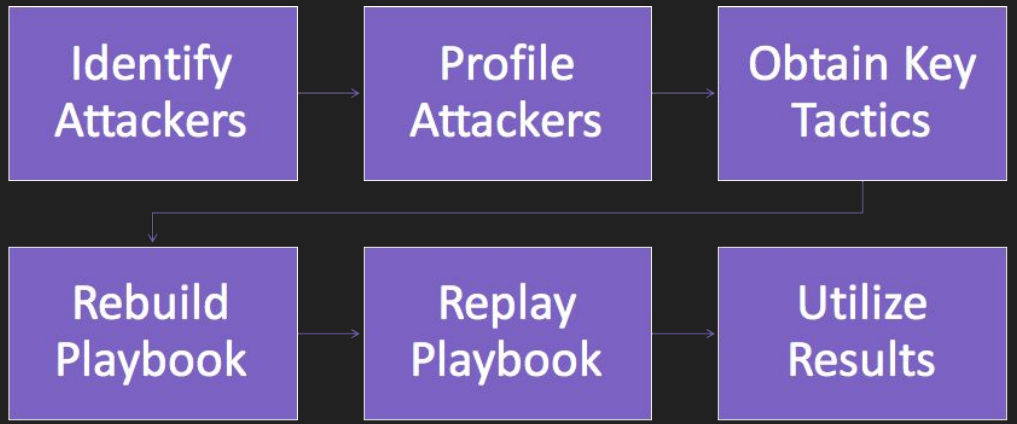
Concepts



https://thumbs.dreamstime.com/z/silhouettes-business-people-data-concepts-41633119.jpg

Intelligence

- Not hashes and IP address
- Actionable tactics and procedures
- Motivation, resourcing, strategies
- Expertise to distill and apply intelligence

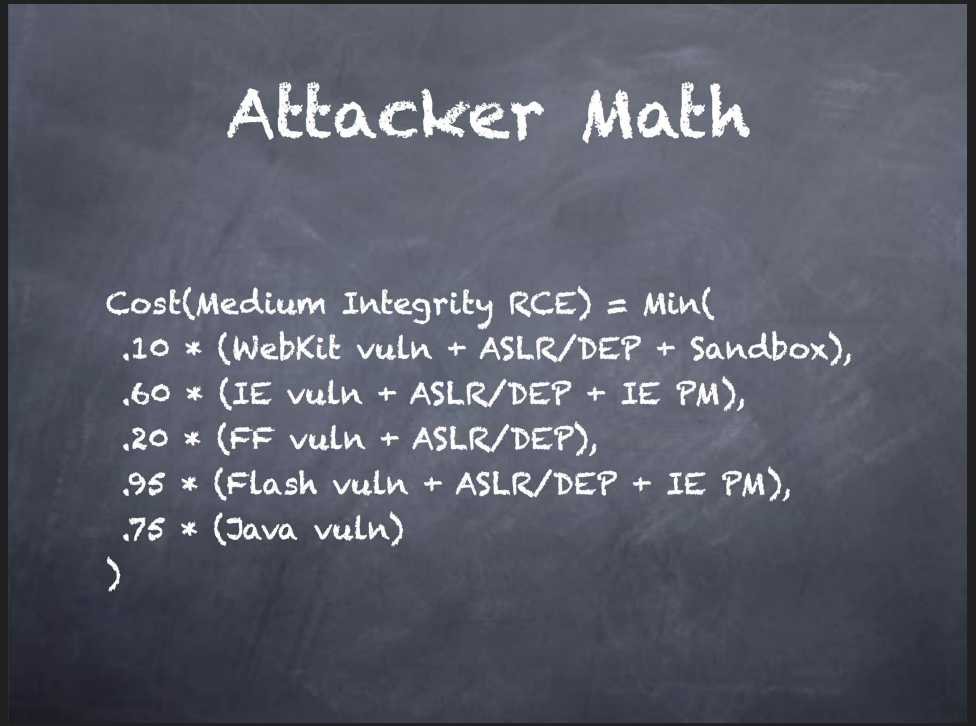


https://www.nettitude.com/uk/eight-things-to-consider-before-deploying-cyber-threat-intelligence/
https://medium.com/@HockeyInJune/playbook-based-testing-5df4b656113a

Attacker Cost

- The total cost of an attack is the minimum of cost times the success rate

- Cost factors
  - Expertise
  - Time
  - Money
  - Resources
- Success factors
  - Target ubiquity
  - Probability
  - Access



https://trailofbits.files.wordpress.com/2011/08/attacker-math.pdf

Attacker Value

All attackers are resource constrained — @*dinodaizovi*
All attackers have a boss and a budget — @*philvenables*

Repeatability: The capability to change the target and have the attack still work with the same success rate
Scalability: The capability to launch the attack against multiple targets with minimal cost per additional target

https://medium.com/@HockeyInJune/playbook-based-testing-5df4b656113a

Attacker Efficiency

Attackers determine the least costly and most valuable attacks based on

Who are the targets
Required success rate
Speed of conversion

Common Attacks

Inexpensive, valuable, scalable, or repeatable:

Phishing
Credential reuse
Known vulnerabilities with public exploits
Office macros
Spyware
Vendor compromise

Costly, valueless, unscalable, or unrepeatable:

Web vulnerabilities
0-day exploits
Known vulnerabilities without public exploits
Embedded devices
Crypto weaknesses
Insider threat

Lockheed Martin’s Intrusion Kill Chain

- Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.
- 6th International Conference Information Warfare and Security (ICIW 11)

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Offensive Experience

- Attacker constraints
  - Resourcing, expertise, time
- Political constraints
  - Management
- Motivations
  - Military, financial, political
- Research and development
  - Pipelines, iterations, constraints

http://www.cyberwar.news/wp-content/uploads/sites/32/2015/10/china_cyberwar.jpg

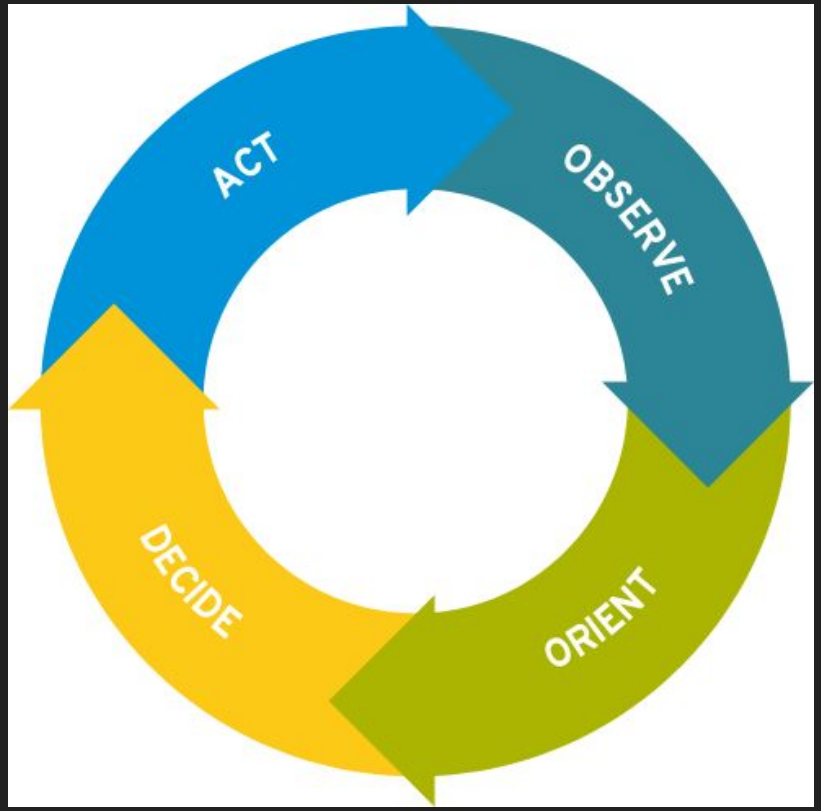
Integrating Concepts Into Programs

STRUCTURE AND CONTENT OF ISO/IEC 27001

ISO/IEC 27001:2005 has the following sections:	
0	Introduction - the standard uses a process approach.
1	Scope - specifies generic ISMS requirements suitable for organizations of any type, size, or nature.
2	Normative references - only ISO/IEC 27002:2005 is considered absolutely essential to the use of 27001.
3	Terms and definitions - a brief, formalized glossary, soon to be superseded by ISO/IEC 27000.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

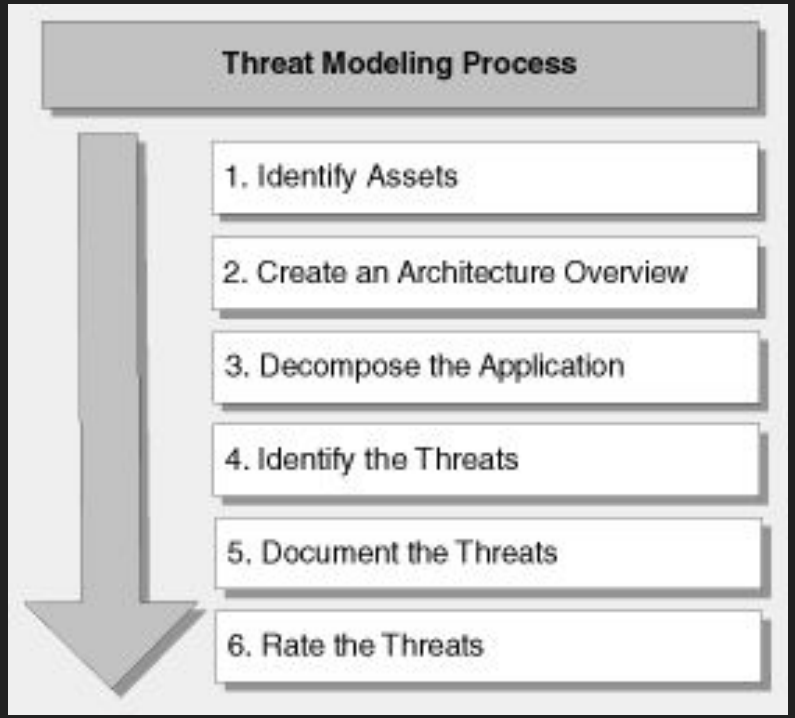
The Cycle



The OODA Loop as Applied To A Security Program

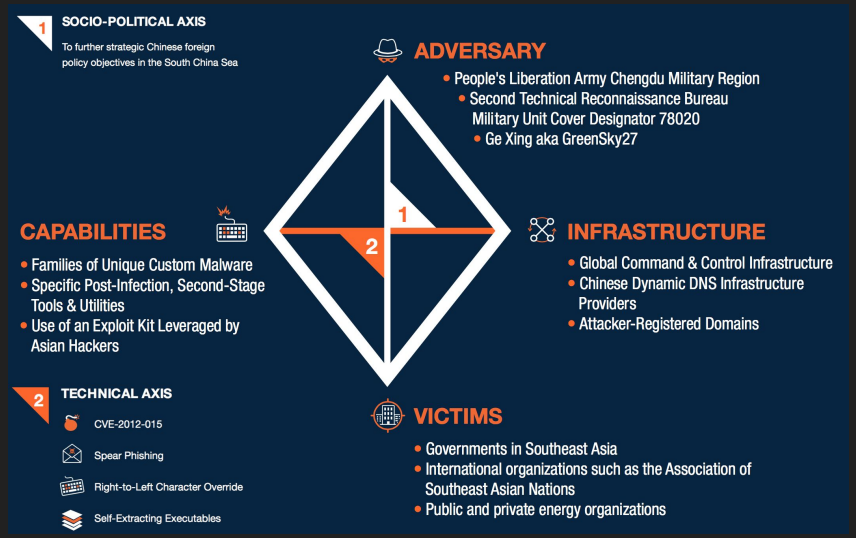
- **Observe** - Collect Intelligence
- **Orient** - Model Threats
- **Decide** - Prioritize
- **Act** - Design and Build

Observe and Orient - The Traditional Way



Building Intrusion Kill Chains

- Analyze existing intelligence
  - Reports, news, breaches
- Analyze whitehat research
  - Presentations, reports, tools
- Collect intelligence
  - Honeypots, scanners, logging
- Understand motivations and resourcing
  - Military, criminal, political
- Use expertise to build theories
  - From experience, breaches, and research



https://www.threatconnect.com/wp-content/uploads/cshydiamond_full.png

An Example Intrusion Kill Chain

- **Recon**: E-mail harvesting
- **Weapon**: Office macros
- **Delivery**: Phishing
- **Exploit**: Target runs macro
- **Install**: Poison Ivy
- **C2**: Poison Ivy
- **Actions**: Pivots to active directory

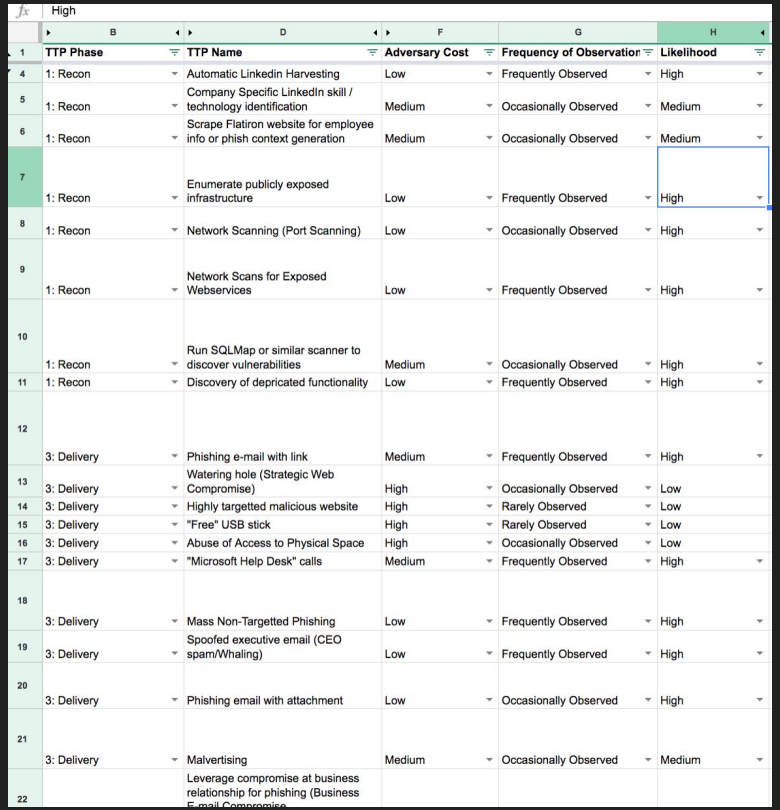
Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Observe and Orient - Integrating Intelligence

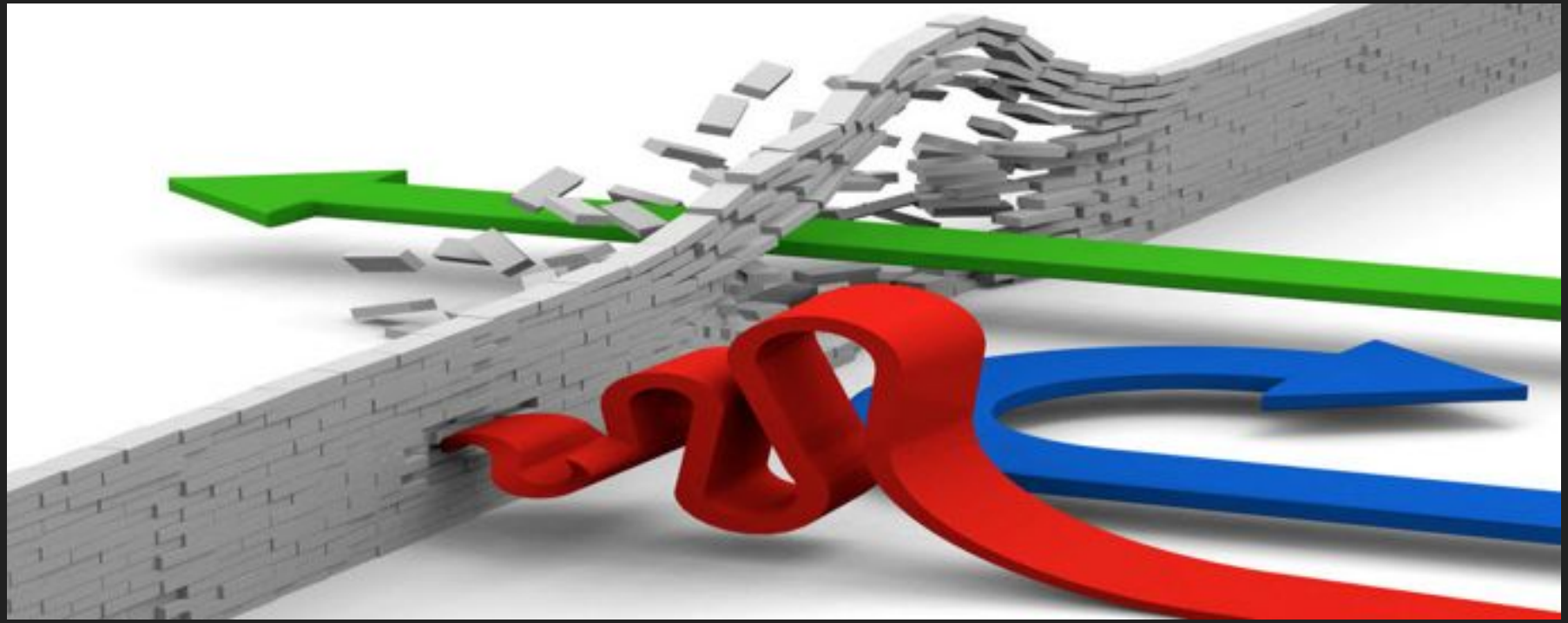
Observe and Orient - Integrating Intelligence



High

	B	D	F	G	H
1	TTP Phase	TTP Name	Adversary Cost	Frequency of Observation	Likelihood
4	1: Recon	Automatic Linkedin Harvesting	Low	Frequently Observed	High
5	1: Recon	Company Specific LinkedIn skill / technology identification	Medium	Occasionally Observed	Medium
6	1: Recon	Scrape Flatiron website for employee info or phish context generation	Medium	Occasionally Observed	Medium
7	1: Recon	Enumerate publicly exposed infrastructure	Low	Frequently Observed	High
8	1: Recon	Network Scanning (Port Scanning)	Low	Occasionally Observed	High
9	1: Recon	Network Scans for Exposed Webservices	Low	Frequently Observed	High
10	1: Recon	Run SQLMap or similar scanner to discover vulnerabilities	Medium	Occasionally Observed	High
11	1: Recon	Discovery of depricated functionality	Low	Frequently Observed	High
12	3: Delivery	Phishing e-mail with link	Medium	Frequently Observed	High
13	3: Delivery	Watering hole (Strategic Web Compromise)	High	Occasionally Observed	Low
14	3: Delivery	Highly targetted malicious website	High	Rarely Observed	Low
15	3: Delivery	"Free" USB stick	High	Rarely Observed	Low
16	3: Delivery	Abuse of Access to Physical Space	High	Occasionally Observed	Low
17	3: Delivery	"Microsoft Help Desk" calls	Medium	Frequently Observed	High
18	3: Delivery	Mass Non-Targetted Phishing	Low	Frequently Observed	High
19	3: Delivery	Spoofed executive email (CEO spam/Whaling)	Low	Frequently Observed	High
20	3: Delivery	Phishing email with attachment	Low	Occasionally Observed	High
21	3: Delivery	Malvertising	Medium	Occasionally Observed	Medium
22		Leverage compromise at business relationship for phishing (Business E-mail Compromise			

Observe and Orient - Integrating Intelligence



Decide - Traditional

Likelihood	Near Certainty	Medium	Medium	High	Critical	Critical
	Likely	Low	Medium	High	High	Critical
	Possible	Low	Low	Medium	High	High
	Unlikely	Very Low	Low	Low	Medium	High
	Rare	Very Low	Very Low	Low	Low	Medium
		Minimal	Minor	Major	Serious	Catastrophic
		Impact				

Intrusion Kill Chain Courses of Actions Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
E-mail harvesting	Fake employee		Policy	Policy	Fake employee	
Office macros			Kill whitehats			Hack
Phishing	Mail gateway	Mail gateway	Mail gateway	Training		
Target runs macro	EPP	EPP	Macros off	No local admin	Sandbox	
Poison Ivy	EPP	EPP	EPP	Sandbox	Sandbox	
Poison Ivy	NIDS	Firewall	NIPS	Web proxy	Sandbox	
Pivots to active directory	Logging	2-factor auth	SMB signing	Segmentation	Honeypot	

Key:
EPP: Endpoint Protection Platform
NIDS: Network Intrusion Detection System
NIPS: Network Intrusion Prevention System
SMB: Server Message Block Protocol

Likelihood Versus Impact

- SQL Injection Vulnerability
- Authenticated
- VPN
- Customer Data
- Yields: Full Database Access
- High Impact, Low Likelihood

CVSSv3: 7.7
Unlikely to occur

- PDF Memory Corruption Vulnerability
- Commercial Software
- Support Staff
- Customer Data
- Yields: Some Data and Foothold Machine
- Low Impact, Medium Likelihood

CVSSv3: 6.7
Likely to occur

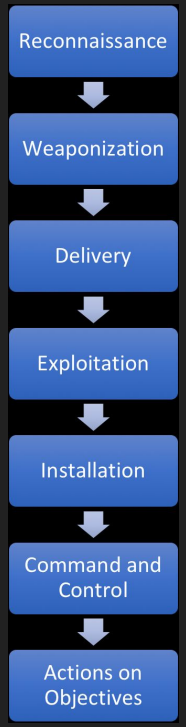
- Conclusion: Treat everything as High Impact, most issues should be scored on Likelihood

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Attacker Cost

State-sponsored, well-resourced group
Resources focused towards target set
Strategy: Attack everyone and wait

- **Recon**: E-mail harvesting
- **Weapon**: Office macros
- **Delivery**: Phishing
- **Exploit**: Target runs macro
- **Install**: Poison Ivy
- **C2**: Poison Ivy
- **Actions**: Pivots to active directory



Financially-motivated, medium-resourced group
Resources focused towards what's necessary
Strategy: Collect credit card numbers

- **Recon**: LinkedIn harvesting
- **Weapon**: Angler exploit kit
- **Delivery**: Phishing
- **Exploit**: Browser exploits runs
- **Install**: Custom malware
- **C2**: Custom encrypted channel
- **Actions**: Pivots to database servers

Attacker Cost

Common Tactics

- **Recon**: E-mail harvesting
- **Weapon**: Office macros
- **Delivery**: Phishing
- **Exploit**: Target runs macro
- **Install**: Poison Ivy
- **C2**: Poison Ivy
- **Actions**: Pivots to active directory

- **Recon**: LinkedIn harvesting
- **Weapon**: Angler exploit kit
- **Delivery**: Phishing
- **Exploit**: Browser exploits runs
- **Install**: Custom malware
- **C2**: Custom encrypted channel
- **Actions**: Pivots to database servers

Key:
White: Shared attacks

Attacker Cost

Attacker Cost (Likelihood)

- **Recon**: E-mail harvesting
- **Weapon**: Office macros
- **Delivery**: Phishing
- **Exploit**: Target runs macro
- **Install**: Poison Ivy
- **C2**: Poison Ivy
- **Actions**: Pivots to active directory

- **Recon**: LinkedIn harvesting
- **Weapon**: Angler exploit kit
- **Delivery**: Phishing
- **Exploit**: Browser exploits runs
- **Install**: Custom malware
- **C2**: Custom encrypted channel
- **Actions**: Pivots to database servers

Key:
Red: Low-cost to attacker, high likelihood of attack

Attacker Cost

Cost to Change (Future Likelihood)

- **Recon**: E-mail harvesting
- **Weapon**: Office macros
- **Delivery**: Phishing
- **Exploit**: Target runs macro
- **Install**: Poison Ivy
- **C2**: Poison Ivy
- **Actions**: Pivots to active directory

- **Recon**: LinkedIn harvesting
- **Weapon**: Angler exploit kit
- **Delivery**: Phishing
- **Exploit**: Browser exploits runs
- **Install**: Custom malware
- **C2**: Custom encrypted channel
- **Actions**: Pivots to database servers

Key:
Red: High-cost to change, high likelihood of attack

Attacker Cost

Defender Cost

- **Recon**: E-mail harvesting
- **Weapon**: Office macros
- **Delivery**: Phishing
- **Exploit**: Target runs macro
- **Install**: Poison Ivy
- **C2**: Poison Ivy
- **Actions**: Pivots to active directory

- **Recon**: LinkedIn harvesting
- **Weapon**: Angler exploit kit
- **Delivery**: Phishing
- **Exploit**: Browser exploits runs
- **Install**: Custom malware
- **C2**: Custom encrypted channel
- **Actions**: Pivots to database servers

Key:
Green: Low-cost to defend

Intrusion Kill Chain Courses of Actions Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
E-mail harvesting	Fake employee		Policy	Policy	Fake employee	
Office macros			Kill whitehats			Hack
Phishing	Mail gateway	Mail gateway	Mail gateway	Training		
Target runs macro	EPP	EPP	Macros off	No local admin	Sandbox	
Poison Ivy	EPP	EPP	EPP	Sandbox	Sandbox	
Poison Ivy	NIDS	Firewall	NIPS	Web proxy	Sandbox	
Pivots to active directory	Logging	2-factor auth	SMB signing	Segmentation	Honeypot	

Key:
Green: Low-cost to defender
Red: High-cost to attacker

Key:
EPP: Endpoint Protection Platform
NIDS: Network Intrusion Detection System
NIPS: Network Intrusion Prevention System
SMB: Server Message Block Protocol

Decide - Integrating Intelligence

Act - Traditional

Attacker Efficiency

- Message authenticity, signatures, and intelligence feeds
  - Bottom 20% attackers use blacklisted domains, fingerprintable templates, known malware
- Sanity checks and heuristics
  - Next 30% of attackers use new domains, obvious templates, unknown malware
- Sandbox for attachments and links
  - Next 30% of attackers use techniques designed to bypass common protections
- Difficult to detect or custom sandbox
  - Next 15% of attackers use sandbox evasion techniques
- Top 5% of attackers will bypass the mail gateway

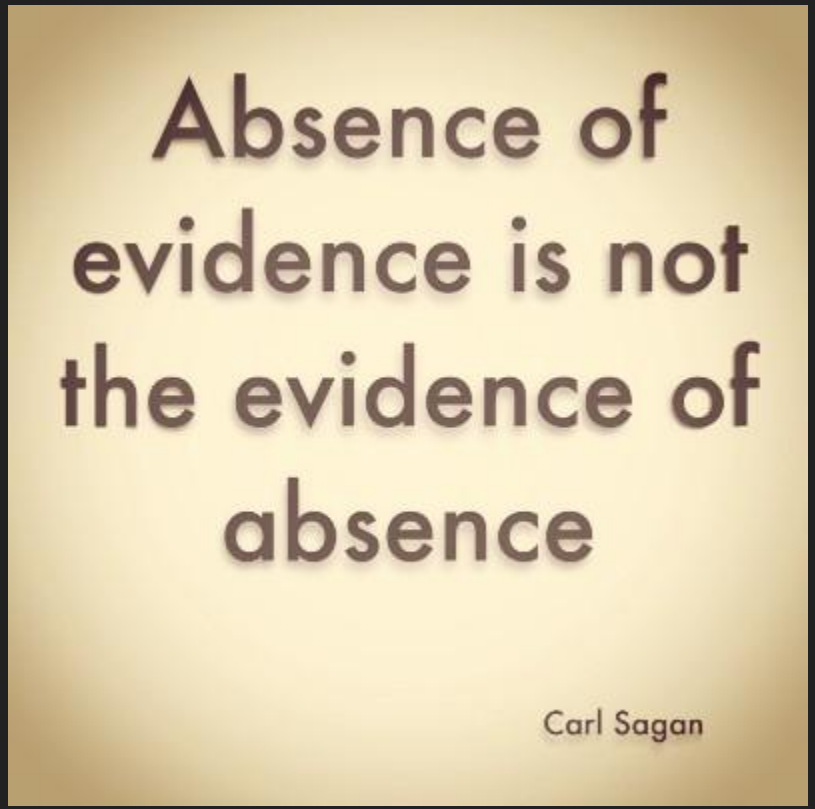
Act - Integrating Intelligence

State-sponsored, well-resourced group
Resources focused towards target set
Strategy: Attack everyone and wait

Financially-motivated, medium-resourced group
Resources focused towards what's necessary
Strategy: Collect credit card numbers

Demonstrate Success

The Challenge



Key Question 1

- Do we know the set of attackers that are relevant for our organization?
  - Are these right attackers?
  - Have we enumerated their playbooks?
  - Are their playbooks accurate?

Key Question 2

- Are we able to defend against the playbooks we are focused on?
  - Have we tested that?

Key Question 3

- Have we effectively prioritized existing gaps against the most likely attackers?
  - Are we making reasonable progress towards reducing risk?
  - Do we have enough resources allocated to these efforts?

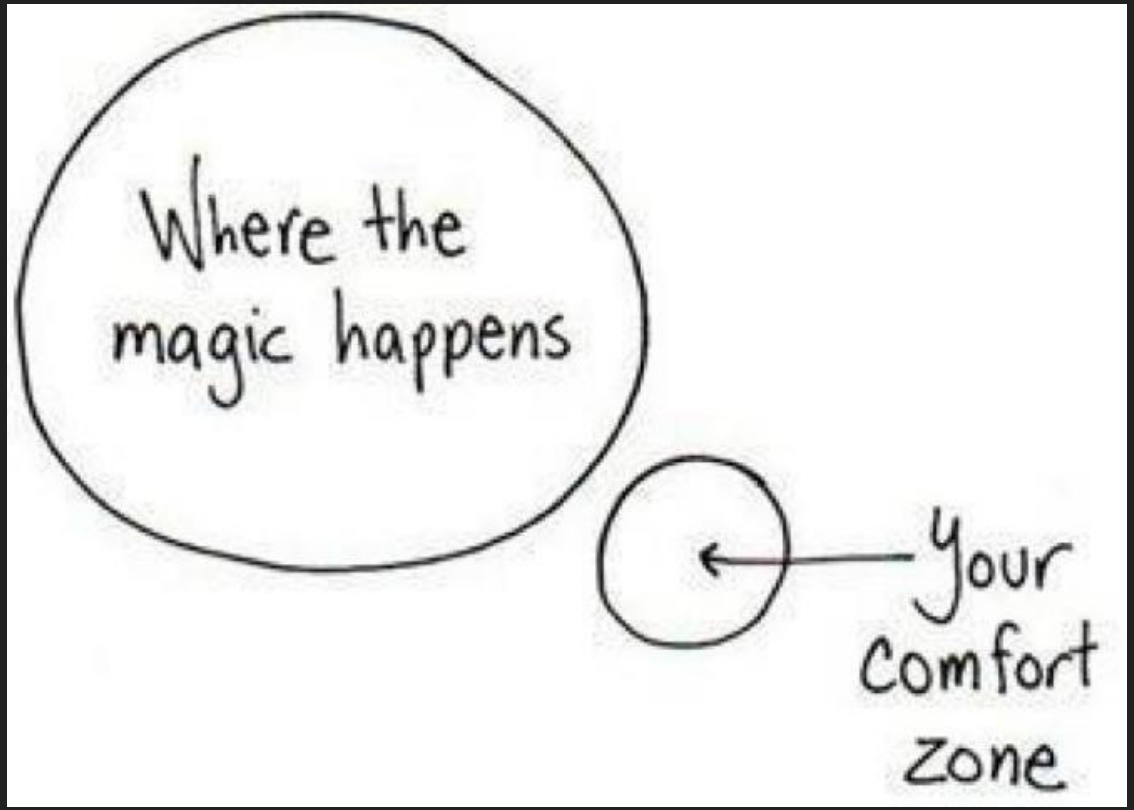
Key Question 4

- Are we accurately and effectively predicting future changes?
  - When and who will become new attackers in the future?
  - Which and when will attacker playbooks change?

Combat Common Issues

Objective and Easy To Analyze Data Is Hard To Get

Diverges From Management Comfort Zones



What about Regulations?

Shortage of Talent Capable of Executing

Justin's Hiring!

Director - Incident Response and Cyber Threat Intel
Director, Product Security
Senior Cloud Security Engineer
Senior Security Engineer (IR)
Technical Program Manager (Security & IT)

security@zenefits.com
jberman@zenefits.com