Deterring Cyber Criminals, Penetration Testers, and APTs with Defense in Depth

Presented By: Joe Christian

Disclaimer

- The views and opinions expressed here represent my own and not those of the people, institutions or organizations that I may or may not be related with unless stated explicitly.

Biography

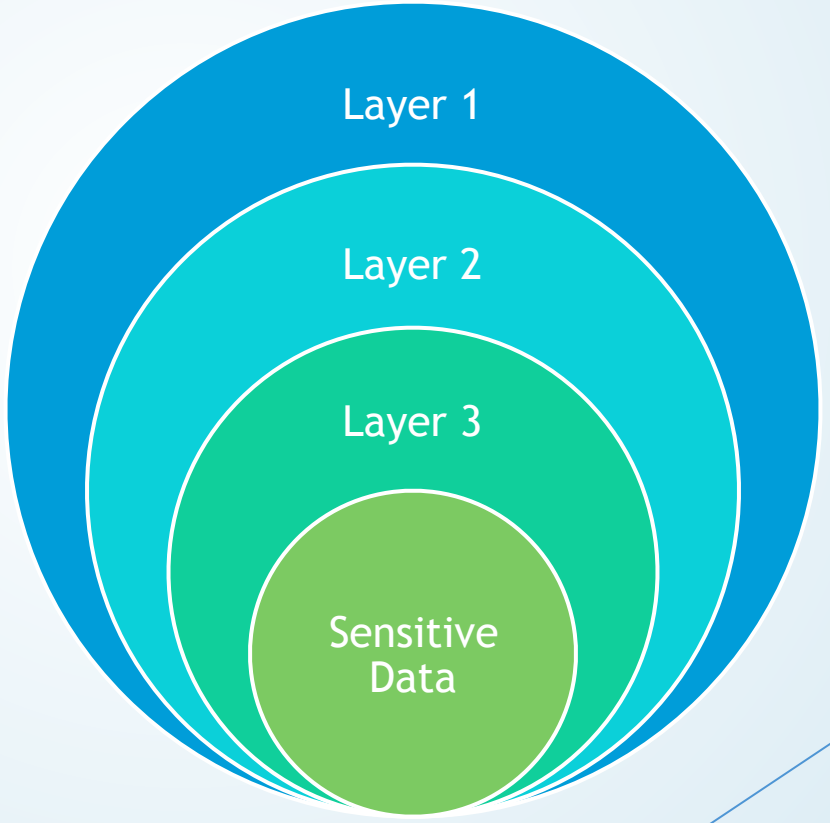
- Joe Christian
  - Gradated from Nazareth College in 2015 with B.S. in Information Technology
  - Former Information Security Intern at Zappos.com
  - Current Master's student at Utica College (M.S. Cybersecurity)
  - Security Engineer at Paychex
  - Bug bounties, Reading, and Exploitation

Overview

- Typical Defense-in-Depth Model
- Understanding the Threat Actors
- Forgotten Elements of Defense-in-Depth
- Summarization of Findings
- Questions and Answers

What is Defense-in-Depth

- Defense-in-Depth is a concept in which multiple layers of security controls (defense) are placed throughout a network or technology system.
- It is a holistic approach to protect all assets.
- The failure of any individual control or layer should not lead to compromise.



Why is Defense-in-Depth necessary for survival?

- It impedes the progress of a cyber intruder.
  - More defensive layers an organization has, the more the intruder will have to pass by…in most cases.
- Enables an organization to detect and respond to the intrusion.
  - Layers should be built with this intent in mind.
- The ultimate goal is to reduce and mitigate the consequences of an eventual breach.
  - No network or system is 100% secure.

Problems typically associated with Defense-in-Depth

- Cost
  - A single security layer can be expensive.
  - Multiple layers may not be achievable because of the associated cost.
- Complexity
  - The more layers that are involved, the harder it is to manage as a cohesive entity.
- False Sense of Security
  - Organizations believe they are sufficiently protected, but layers are misconfigured.
  - More layers may actually make the organization less secure.

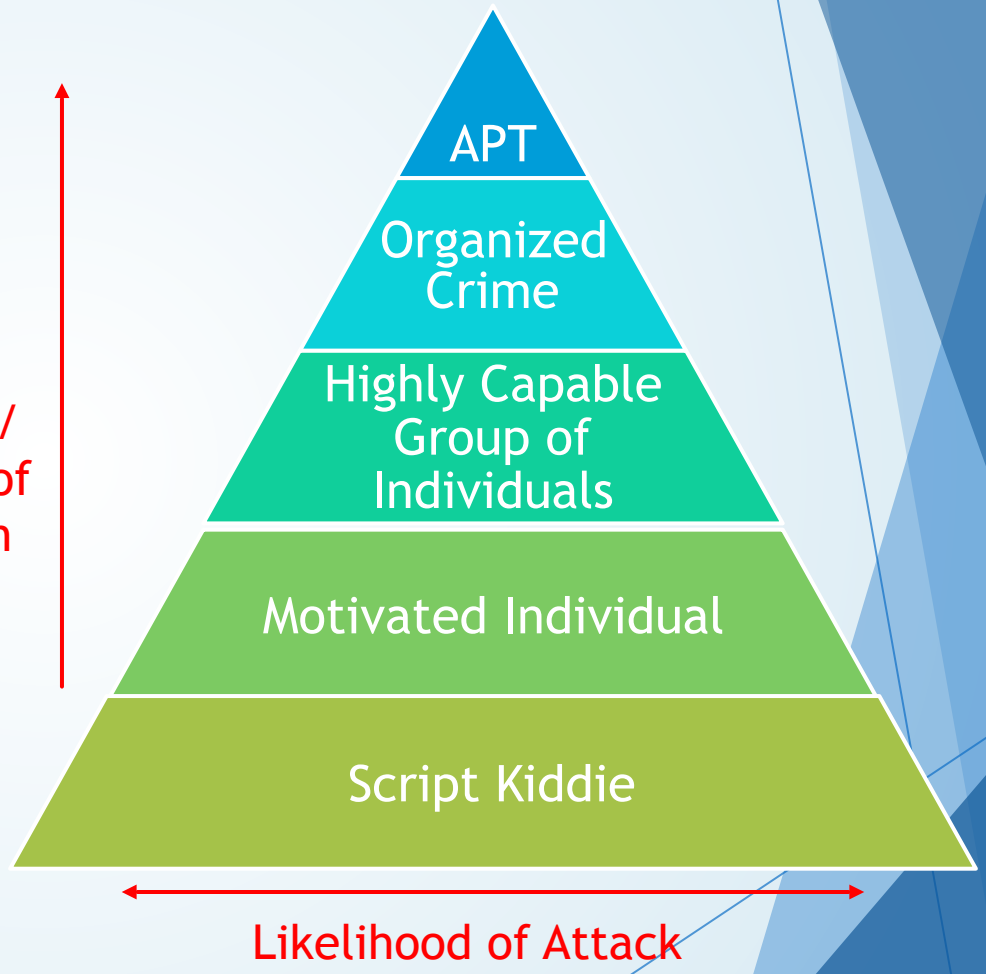
Current Attack Trends

- Majority of attacks are still phishing driven
- More exploit and file-less attacks
  - WannaCry
  - NotPetya
  - Apache Struts
- Targeting and evasion techniques are increasing in sophistication
- Persistence is becoming more common than single heist breaches

Source: SANS

Understanding Threat Agents

- Threat Agents are the actors causing the threat that might exploit a vulnerability.
- Can be a lone individual or large group.
- Their intentions and motivations are different from each other.
  - Understanding this concept is essential to defending your network.



Cyber Criminals

- Cyber Criminals are hackers and other malicious users that use the Internet to commit crimes such as identity theft, spamming, phishing and other types of fraud.
- Cyber Criminals often work together forming cyber gangs.
- Skillsets vary from low to extremely high.

Motives and Targets of Cyber Criminals

- Cyber Criminals are mainly financially motivated.
  - Stealing money directly from banks or individuals.
  - Selling of sensitive information like PII or source code.
  - Extortion through DDoS or ransomware attacks.
- Other factors such as espionage, sabotage, and revenge may motivate criminals.

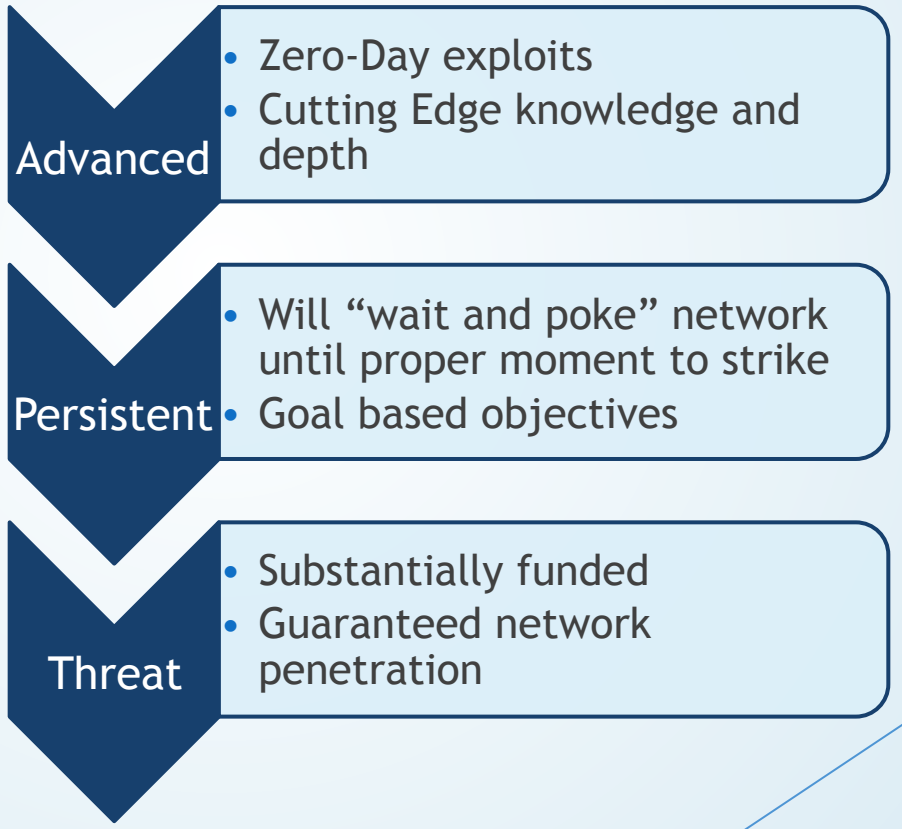
Source: Dell SecureWorks

Known Cyber Criminals

Name	Criminal Act	Action
Aleksandr Andreevich Panin Hamza Bendelladj	Stealing $400 million from US banks	SpyEye Malware
Yevgeniy Bogachev	Stealing $100 million from various bank accounts	Gameover Zeus Malware

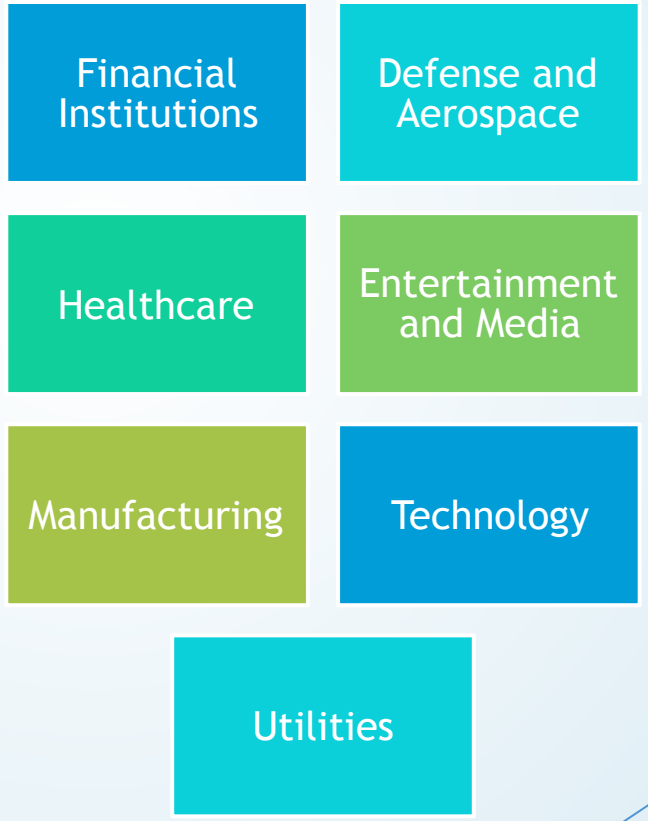
Advanced Persistent Threats (APT)

- APTs may include:
  - Nation-state actors
  - Organized criminal actors
  - Corporate espionage actors
  - Terrorists



Motives and Targets of APTs

- Motives
  - Gain financial advantage
  - Intelligence gathering
  - Gain competitive advantage for industry
  - Obtain a control foothold for later exploitation
  - Embarrass an organization, damage its reputation, and/or take down its systems
  - Obtain indirect access to a targeted affiliate



Source: Dell SecureWorks

Known Government based APTs

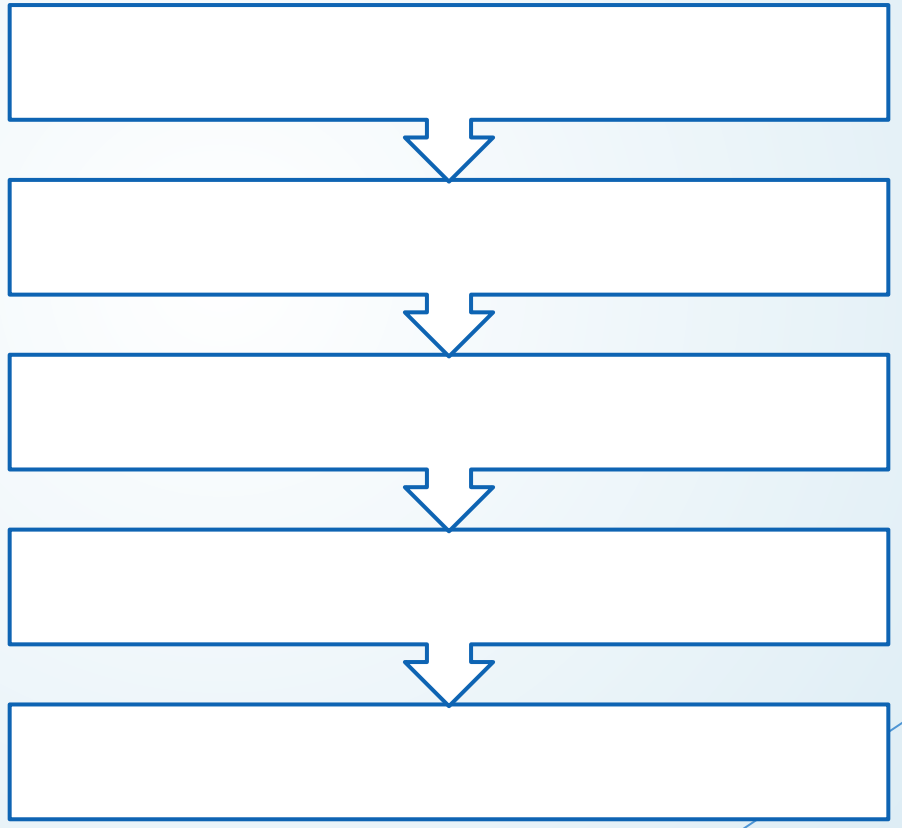
Country	Entity	Example Groups	Objective
Russia	FSB	APT 28, APT 29	Political Espionage (DNC Breach)
Israel	8200	Unknown	Unknown Operations
Britain	GCHQ	JTRIG	Communications Disruption
China	PLA	APT1/Unit 61398	Economic Espionage
USA	NSA TAO	Equation Group	Unknown Operations

Similarities Between Threats and Penetration Testers

- Both cyber criminals and APTs have a defined set of tactics, techniques, and procedures (TTPs).
  - A good penetration tester should attempt to emulate these TTPs to simulate a real attack scenario.
  - The best attackers and testers are extremely creative allowing them to be effective.
- It is only a matter of time before a threat or penetration tester gains access to your sensitive data.
  - Defense-in-Depth will impede all those who are attempting to gain access to the network.
  - Watching a great penetration tester struggle to gain access during a test is a good finding.
    - It proves that your controls are working properly.

Penetration Testers

- Penetration Testers are ethical hackers tasked with finding weaknesses and vulnerabilities in applications, systems, and networks.
- Pen Testers need to be able to assess hosts from an outsiders perspective.
- Testers typically follow a phased approach.
- Tests should be objective based in order to emulate true threats.



Some thoughts about penetration testing and Defense-in-Depth…

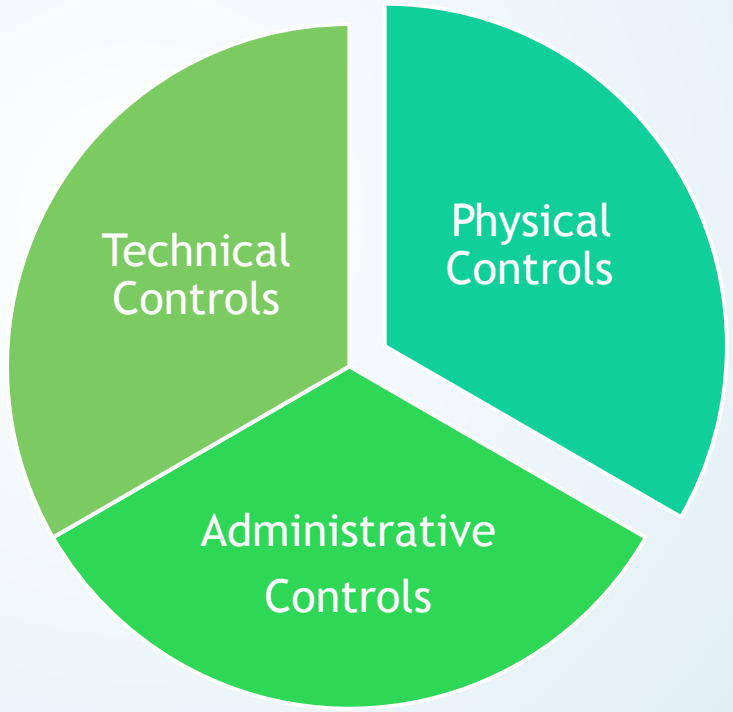
- If entire phases are skipped, are you really conducting a pen test?
  - Does this really test your overall defense like an attacker would?
- You want to have an effective Defense-in-Depth strategy because the tester can tell you which items failed and need to be improved.
- The more you narrow the scope, the less overall defensive posture you are testing.

Getting the most of your penetration testing program

- Objective based testing.
  - Can you obtain shell on a host with sensitive information?
- Remediate items that previous testers have flagged before conducting a new test.
  - Testers are less likely to look for new security flaws if old items were never remediated.
- Let the tester be creative.
  - Allow for exploitation, physical security, social engineering, etc.

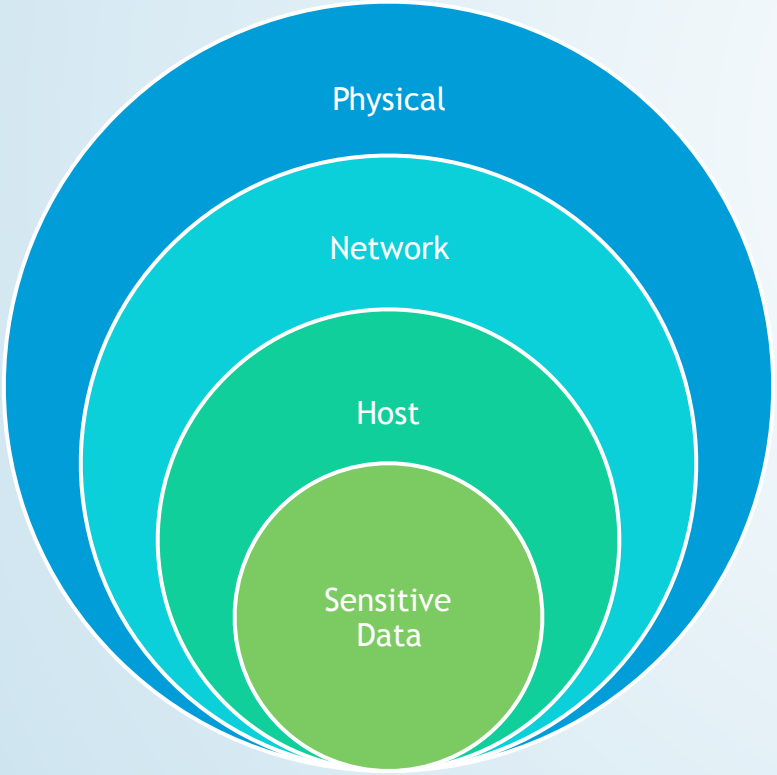
Forgotten elements of Defense-in-Depth

- Physical Controls
  - Lack of cameras, door security, and guards.
- Administrative Controls
  - Lack of policies such as hiring practices, employee training, data handling procedures, and security requirements.
- Technical Controls
  - Majority of focus is on network security, while organizations lack application security or vice versa.

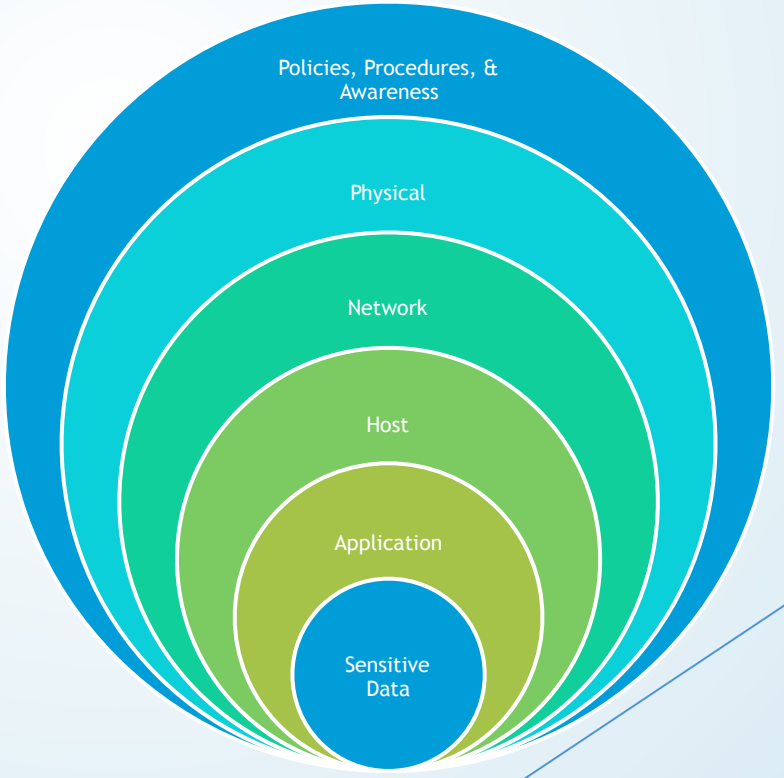


How Defense-in-Depth should look

Example of Typical Network



Example of an Ideal Network



Summarization of Findings

- Proper Defense-in-Depth may be unrealistic.
  - Lack of personnel and budget dollars.
- APTs and Cyber Criminals are unavoidable threats.
  - A proper Defense-in-Depth model only will slow threats down, but may limit the overall data exposure.
- Advocate for frequent and proper penetration testing.
  - Cheating a penetration test is only cheating yourself and your organization.
- A business needs to continue to operate, so some risk is acceptable.
  - The key is to review and manage risk overall.

Questions?