The Value of Predictive Security Intelligence

Dave Shackleford

Founder, Voodoo Security

Introduction

- Today's security programs aren't as effective as they should be.

- We're doing a lot of things right, but are we spending the right amount of time on the best processes and technologies?

The Security Cycle

- A simple outline of how security gets done today:
  - We define data criticality/sensitivity
  - We put controls in place to “protect” the data
  - We spend a ton of money on controls that detect problems.
  - We react to the problems.
  - Data still gets out

Framing risk analysis

- Threats: Things that can cause us harm.
  - Hackers from Elbonia
  - Competitors hiring hackers from Elbonia
  - Insiders
  - Natural disasters
  - Etc.
- Vulnerabilities: Security weaknesses (process, people, technology) that threats can take advantage of.
  - Missing patches
  - Poor coding practices in Web apps
  - Etc.

Framing risk analysis (2)

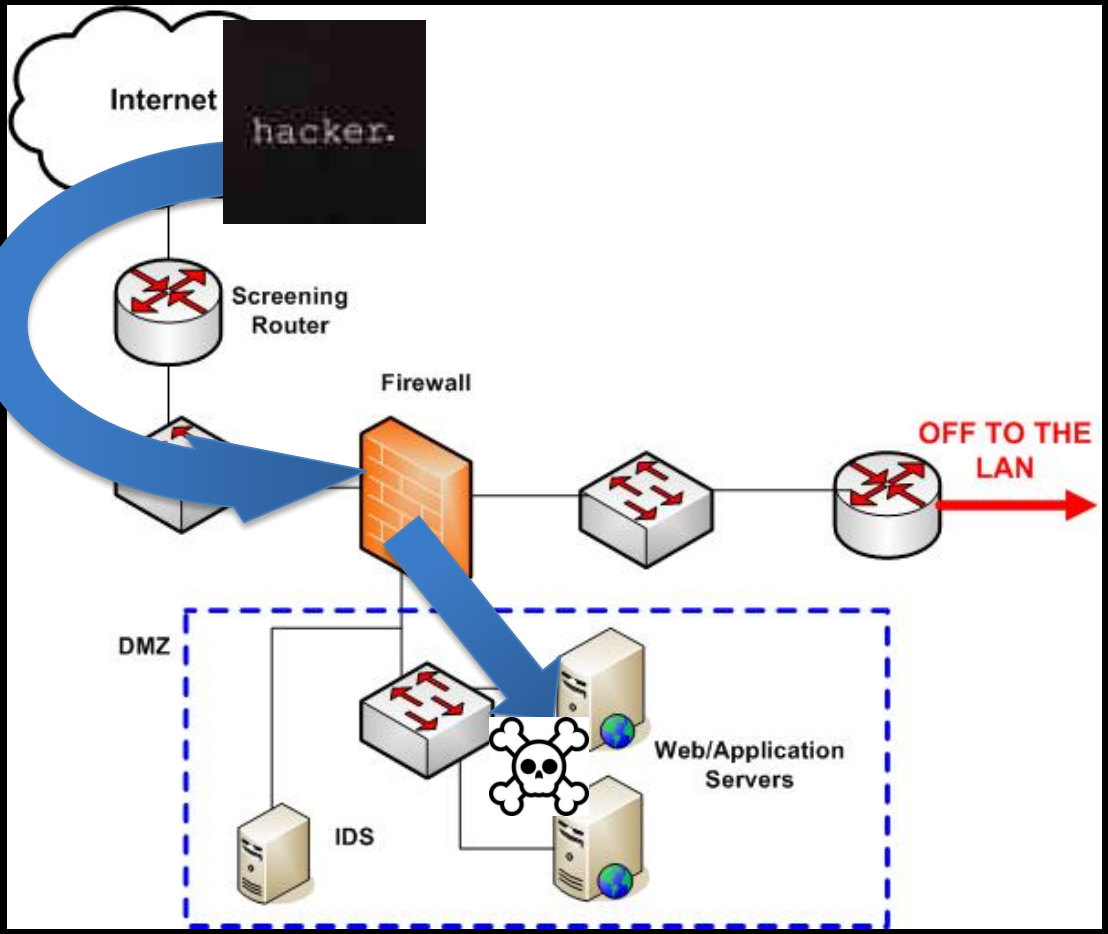
- **Impact: How badly things affect us.**
  - System and applications are unavailable.
  - Systems and applications are corrupted (integrity)
  - Data is breached (confidentiality)
  - Reputation is impacted
  - We incur monetary losses and/or fines.
- **Likelihood: How likely the threat is to actually successfully exploit a vulnerability/vector**
  - Exposure level of systems and apps plays a role
  - Severity of vulnerability is also relevant
  - Mobility, awareness, etc. are all relevant, as well.

Risk is “supposed to” shake out of this.

- Threats and Vulnerabilities and Likelihood and Impact!
- (Oh my!)
- But the question we have to ask is: are we just guessing half the time?
  - Sure, we have to guess at some of the threats.
- We have to estimate the impact, which we can do reasonably in many cases today.
- But what about vulnerabilities? Likelihood?
  - How do we assess these?

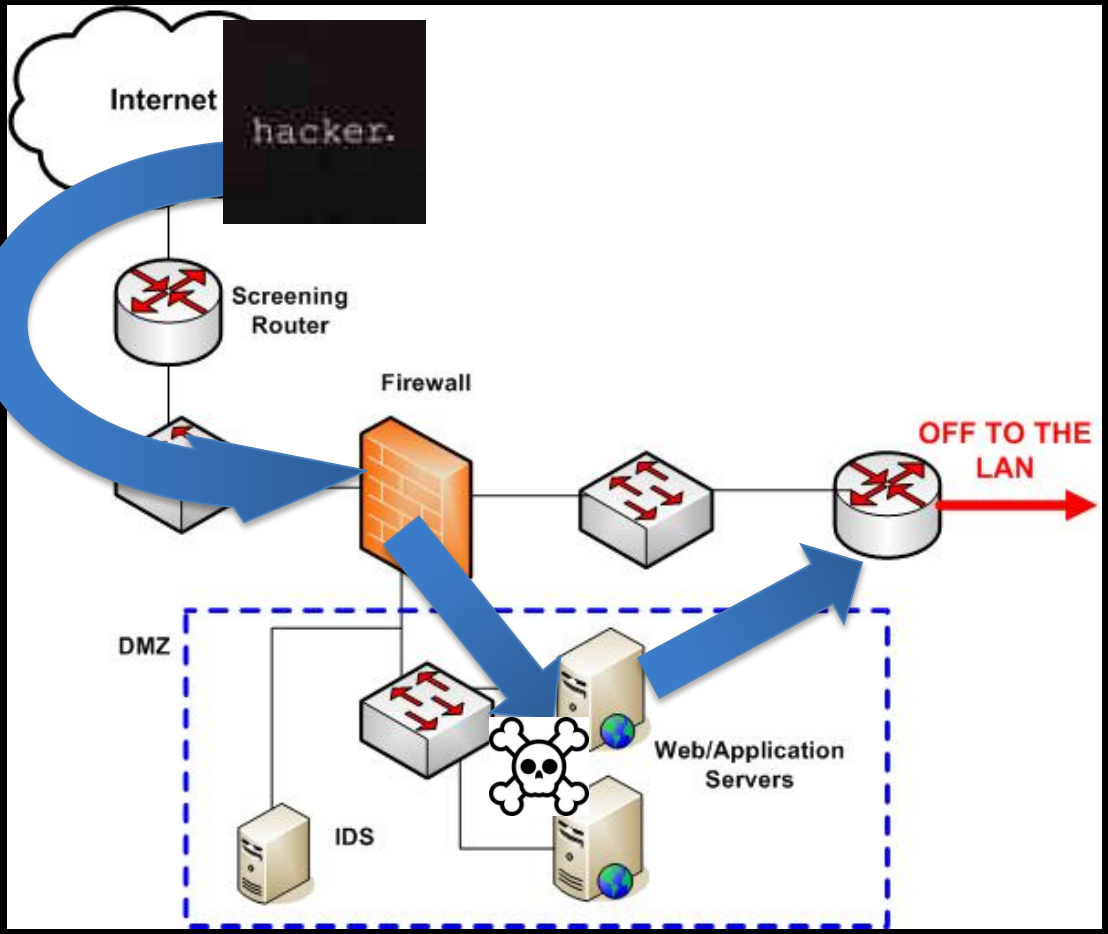
A Simple Illustration

- Threats:
  - Outside attackers
- Vulnerabilities:
  - Weak router and firewall ACLs
  - Missing patches
  - Coding issues
  - Config issues

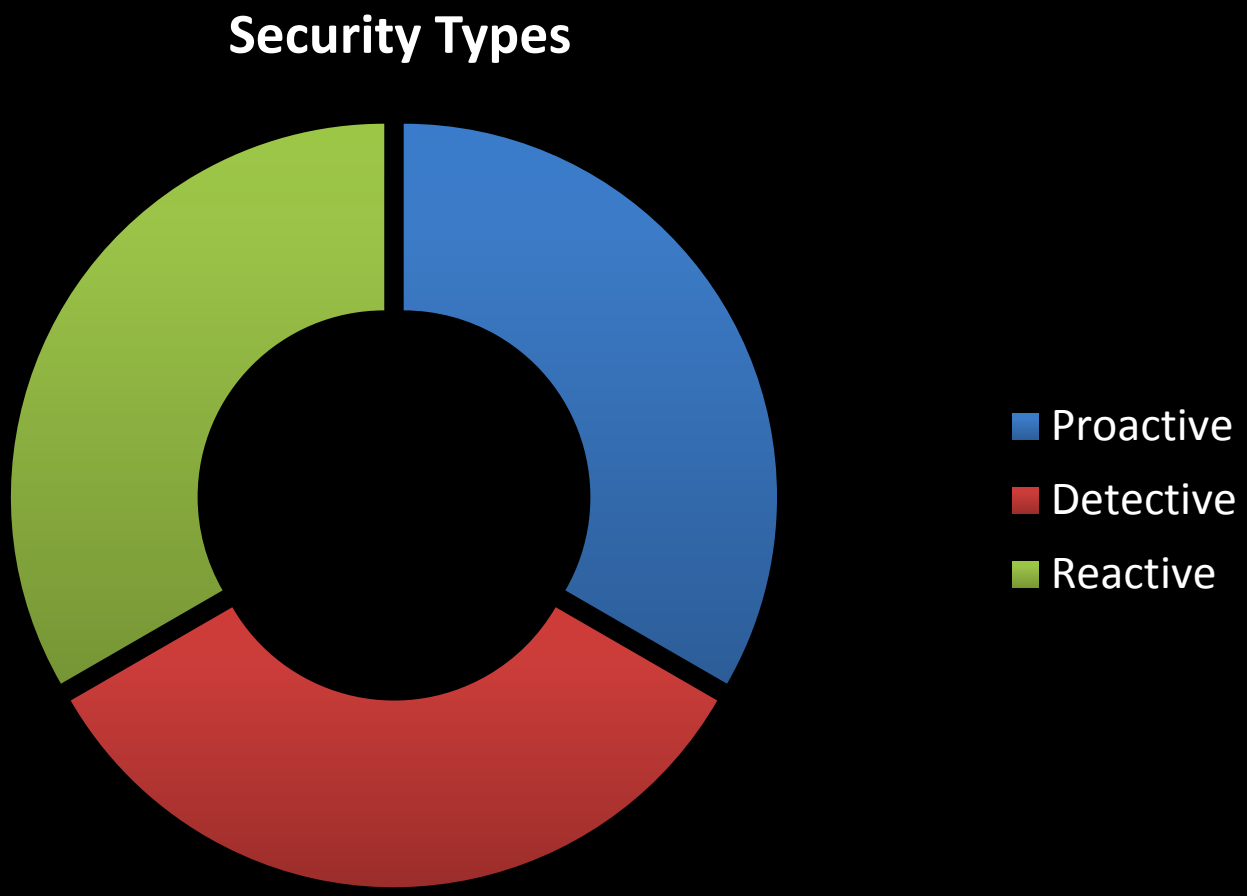


A Simple Illustration (2)

- Impact:
  - Loss of e-commerce and Web apps
  - Loss of reputation
  - Loss of back end DB data
- Likelihood:
  - Hmmmm…



The 3 “types” of security



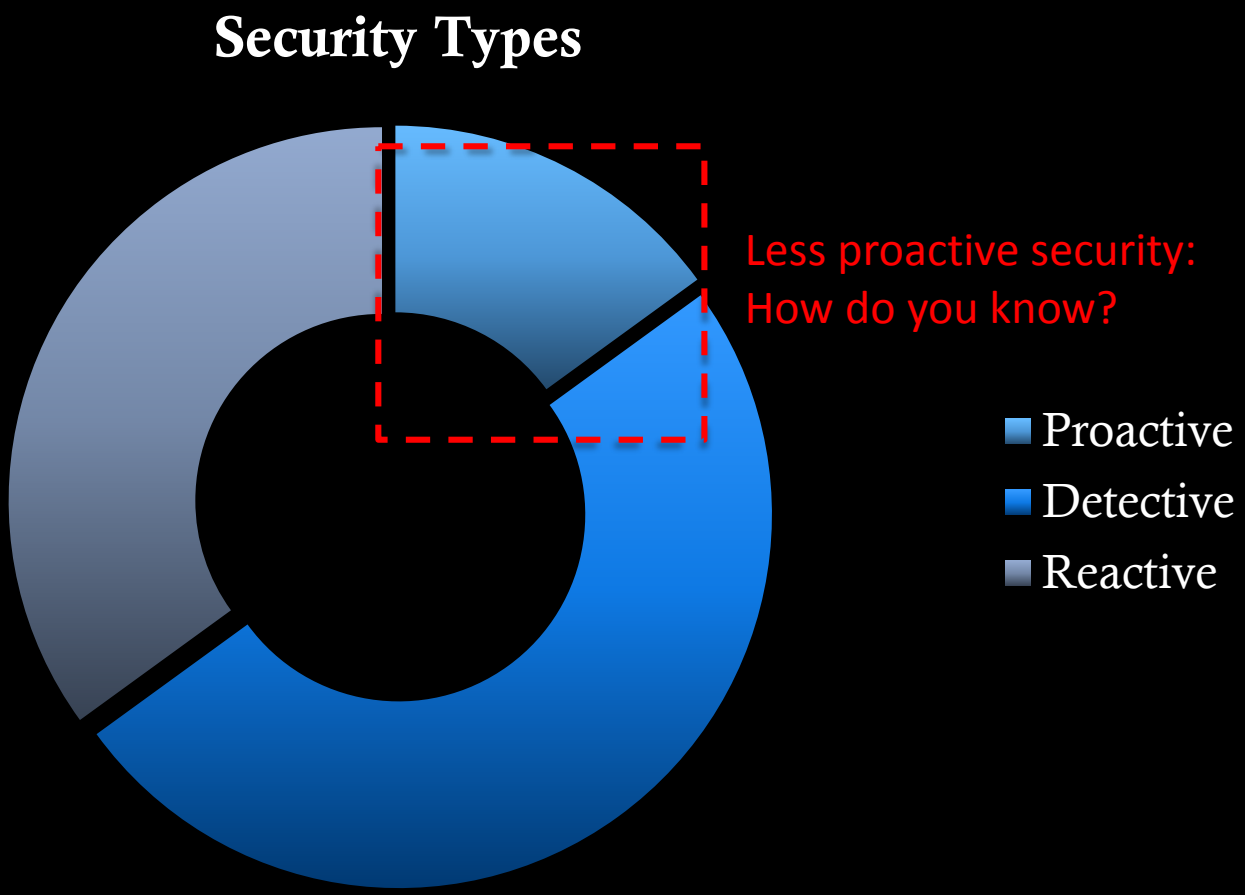
What's in these types?

Reactive

- Proactive/Preventive:
  - Patching and config management
  - Change control
  - Network access controls (firewalls)
  - SDLC and QA
  - Audits
  - Network/app vulnerability scanning and pen testing
- Detective:
  - Host and network IDS/IPS
  - Firewall alerts
  - System and app logs
  - Code reviews
  - DLP

EXAMPLES

The “reality” of security operations



Be More Proactive.

Data Correlation & Analysis

- First things first: We have lots of data
- Detective and reactive solutions need to sift through this normalized data and find patterns that trigger events
- We're not doing a good job of telling "stories" or matching "real world" scenarios though.

The pesky question of “how do you know”?

- We can speculate on the threats and potential impact.
- When it comes to vulnerabilities, what do you rely on?
  - Patch management systems?
  - Configuration management systems?
  - Systems and network admins?
  - Developers and DBAs?
- For likelihood, we can speculate based on exposure level and overall attack frequency
  - We still need to demonstrably prove attacks are possible.

VA and Pen Testing

- Why do vulnerability assessments and pen testing?
  - Find holes before attackers do!
  - Prove that security issues exist to skeptical management
  - Raise overall security awareness
  - Verify secure system configurations
  - Test new technology
  - Discover gaps in compliance posture and satisfy legal and/or governmental requirements
- Performing your own assessments adds a significant proactive component to your security program.

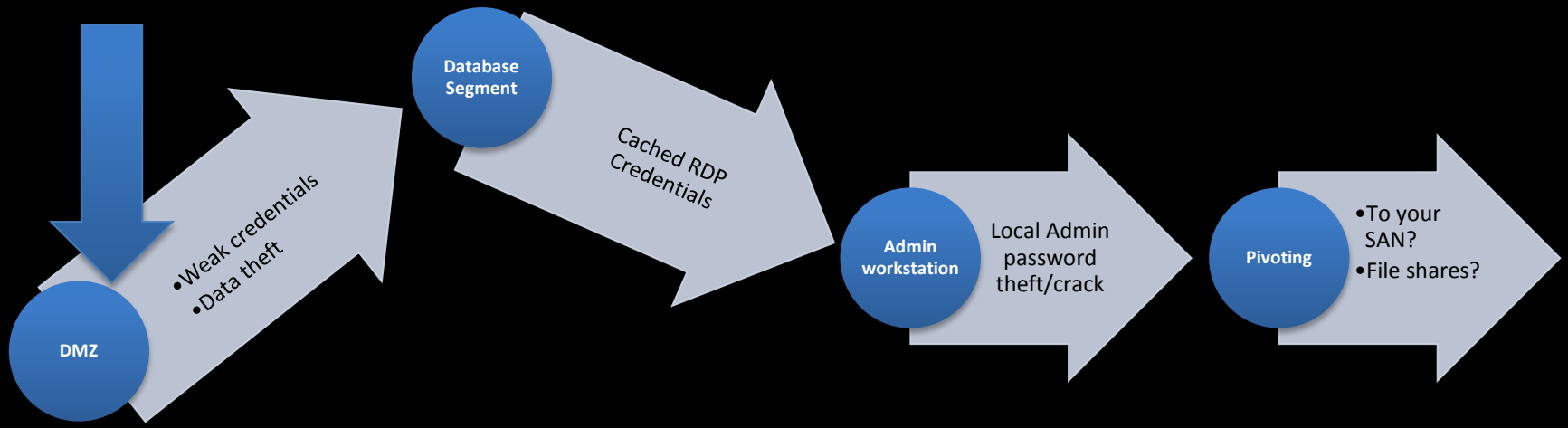
It’s never this simple.

- OK, so these are the basics.
- We have two much bigger issues, that tie back to the way we think.
  - We WAIT for input to learn from.
  - We do not model REAL-WORLD scenarios that depict how threats will exploit vulnerabilities and access sensitive data.

  - **We will never, ever get there by just gathering data from sensors and dashboards.**

Real Threat Modeling

Windows 2008
Server IIS Hack



What about social engineering with your users? Behavioral monitoring?

So…Predictive Intelligence?

- We always say “think like a hacker”…but do we?
- There’s no way to ever completely predict how attacks will come.
- To effectively spend detective and reactive time and $$$, we need to model the real threats.
  - This provides predictive intelligence.

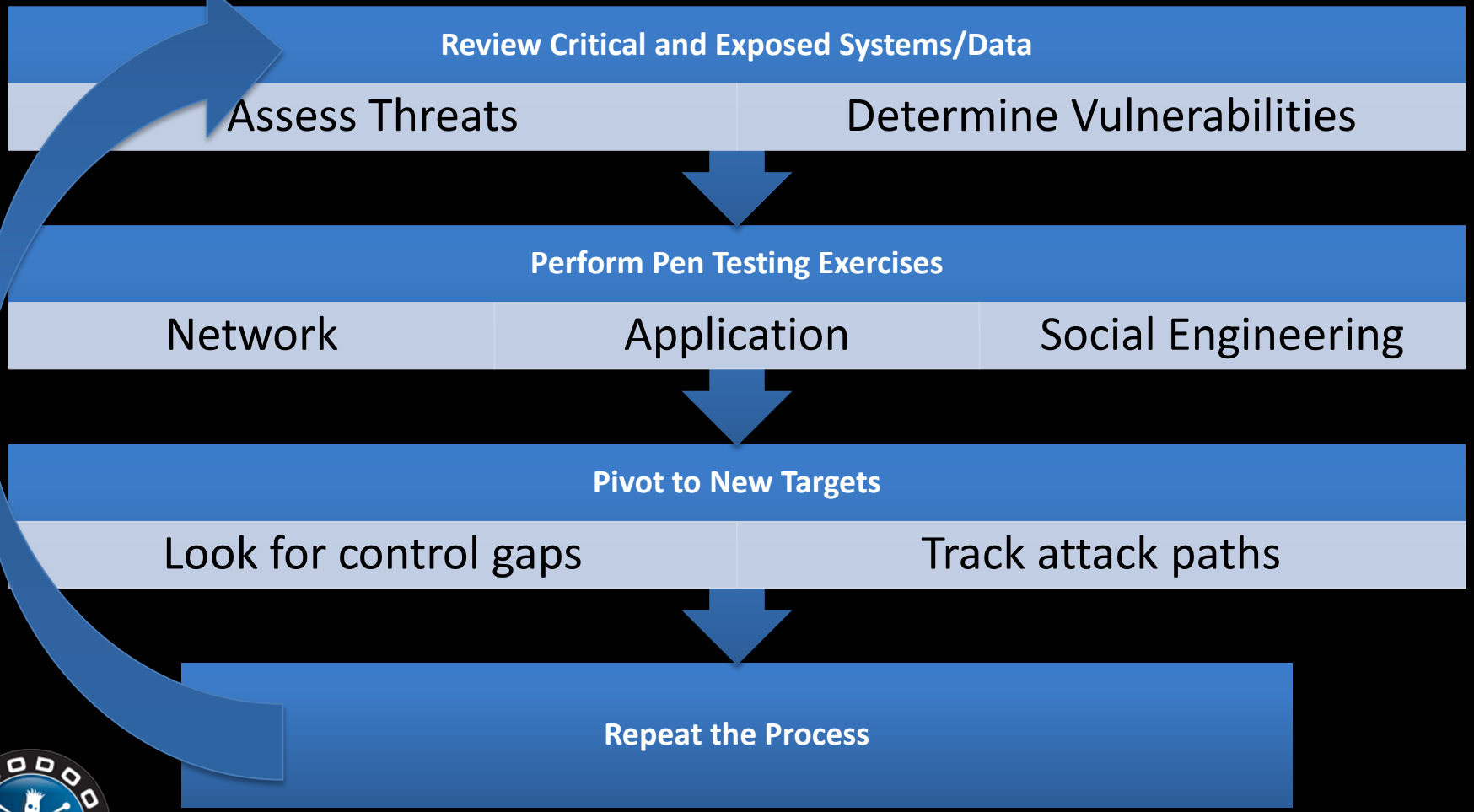
How to get started

- Start with two major considerations:
  - Criticality of systems/data
  - Exposure of systems/data
- Look at how an attacker could get to critical data via exposed systems and apps
  - Do not forget social engineering and client systems

How to get started (2)

- Attack Yourself.
- A classic mistake in pen tests is to just “go” without having goals.
  - Have goals. Look for things of value.
- Couple testing scenarios with response team efforts.
  - More of a “red team” scenario

Make testing a process



The Rub

- We spend a lot of time and money on detective and reactive tools and processes.
- We do NOT spend enough time emulating threats and attack vectors.
- There is no better way to prove attacks are real vs. hypothetical.
- What could bring your company to its knees? Is it possible?