Microsoft

Secure DevOps: Application Security Principles and Practices

Module: Intro to Red and Blue Teams

Microsoft Services

Module Overview

- Lesson: Red and Blue Team Terminology
- Lesson: Red Teaming
- Lesson: Establishing Teams

RED VS. BLUE

Microsoft

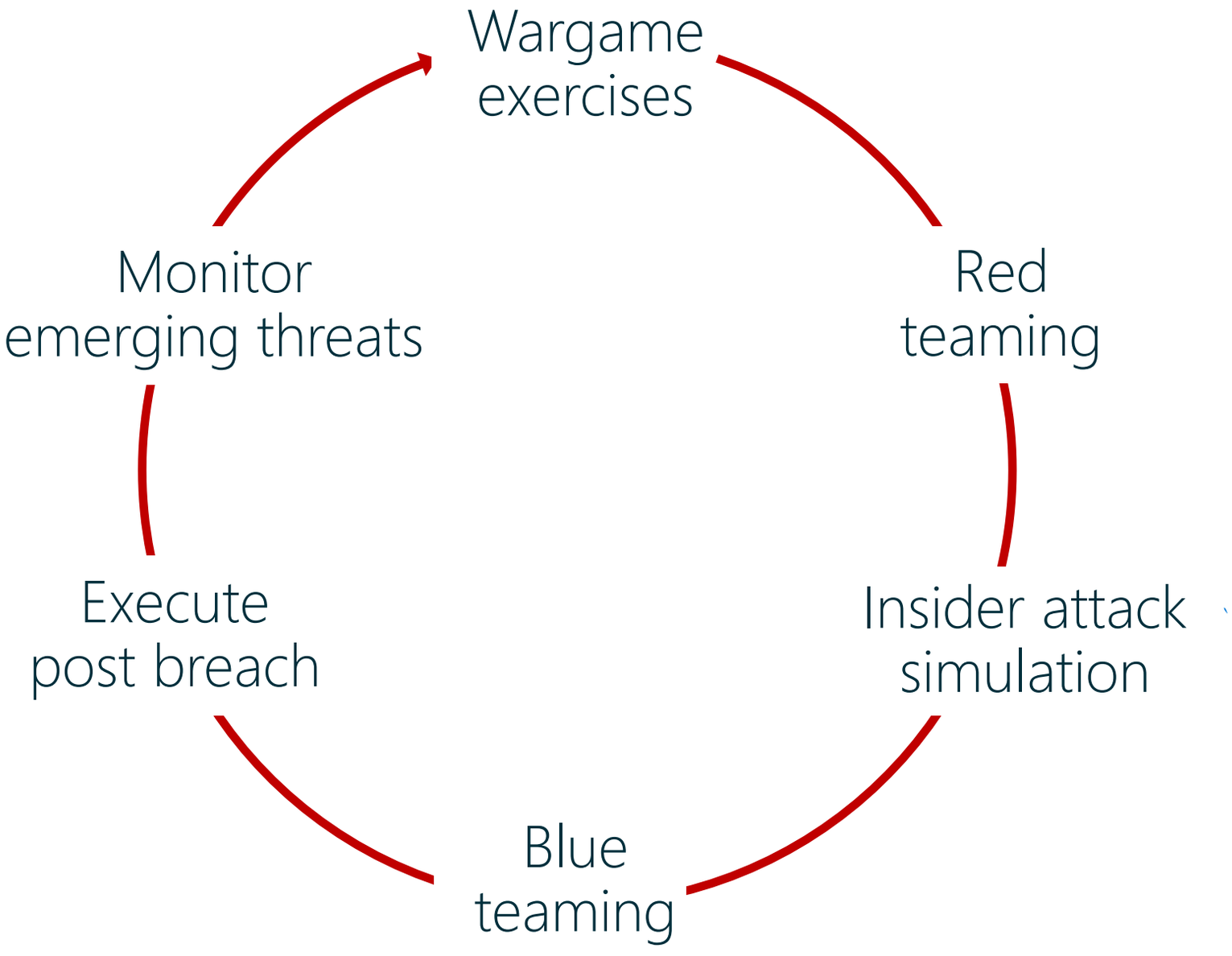
Lesson: Secure DevOps Practices

Lesson: Secure DevOps Practices

After completing this lesson, you will be able to:

- Understand the practices behind assuming breach
- Understand which practices can rely on automation and which practices rely manual processes
- List the supporting practices that enable the Prevent Breach methodology

Assume Breach execution



Wargames

Exercise ability to respond

- Like a **fire drill** vs. a real fire
- Standardized operating procedures & improve response
- Reduce **Mean Time To Detection (MTTD)**
- Reduce **Mean Time To Recovery (MTTR)**

Procedures

- Attack scenario
- Incident response process
- Post-mortem

Example scenarios

- Service compromise
- Inside attacker
- Remote code execution
- Malware outbreak
- Customer data compromised
- Denial of service

Red Teaming

Model real-world attacks

- Model **emerging threats** & use **blended threats**
- **Pivot** laterally & penetrate deeper
- **Exfiltrate** & leverage compromised data
- **Escape & Evade / Persistence**

Identify gaps in security story

- **Measures Time to Compromise (MTTC) / Pwnage (MTTP)**
- **Highlight security monitoring & recovery gaps**
- **Improves incident response tools & process**

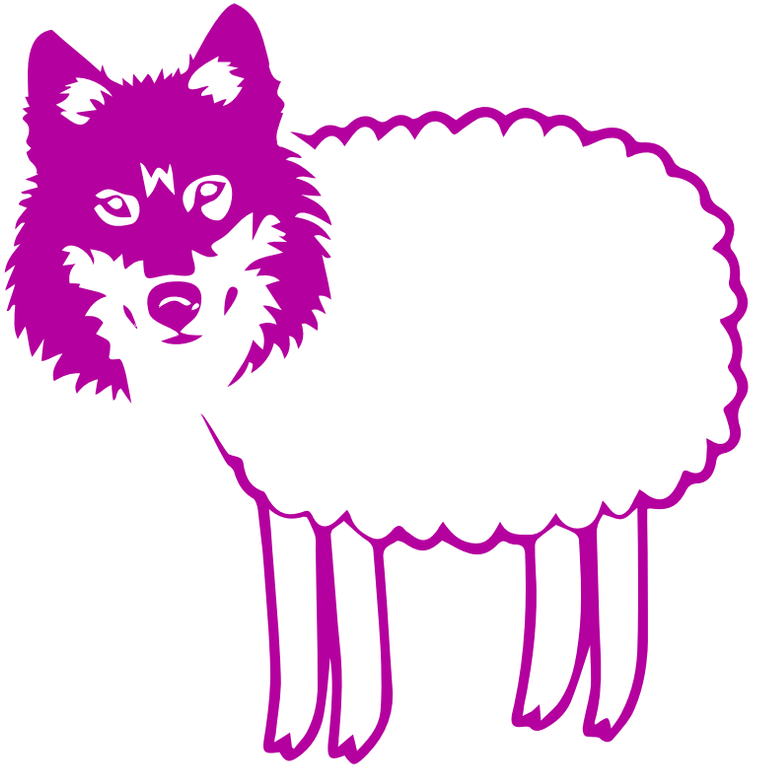
Demonstrable impact

- **Prove need for Assume Breach**
- **Enumerate business risks**
- **Justify resources, priorities, & investment needs**

Insider Attack Scenario

Insider attack scenario

- Talented & motivated attackers breach perimeter
- Attackers acquire insider privileges
- Emerging threat pattern
- Example: LinkedIn → DropBox compromise
- Restrict access to security bugs/findings
- Spear phishing = insider



Blue Teaming

Exercises ability to detect & respond

- **Detect** attack & penetration (MTTD)
- **Respond** & **recover** to attack & penetration (MTTR)
- **Practiced** incident response

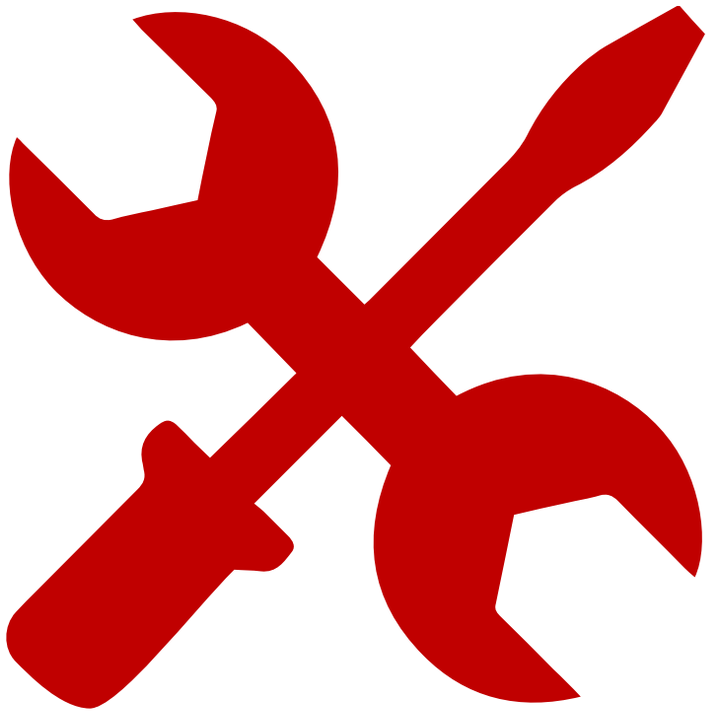
Enhances situational awareness

- Produces **actionable intelligence**
- **Full visibility** into actual conditions within environment
- **Data analysis** & **forensics** for attack & breach indicators

Measures readiness & impact

- **Accurately assesses** real-world attacks
- **Identifies** gaps & **investment needs**
- Focus on **slowing down attackers** & **speeding recovery**
- **Hardening** that prevents future attacks

Post Breach Execution



Establish security baselines

- Time to detect
- Time to contain
- Time to fix
- Time to recover

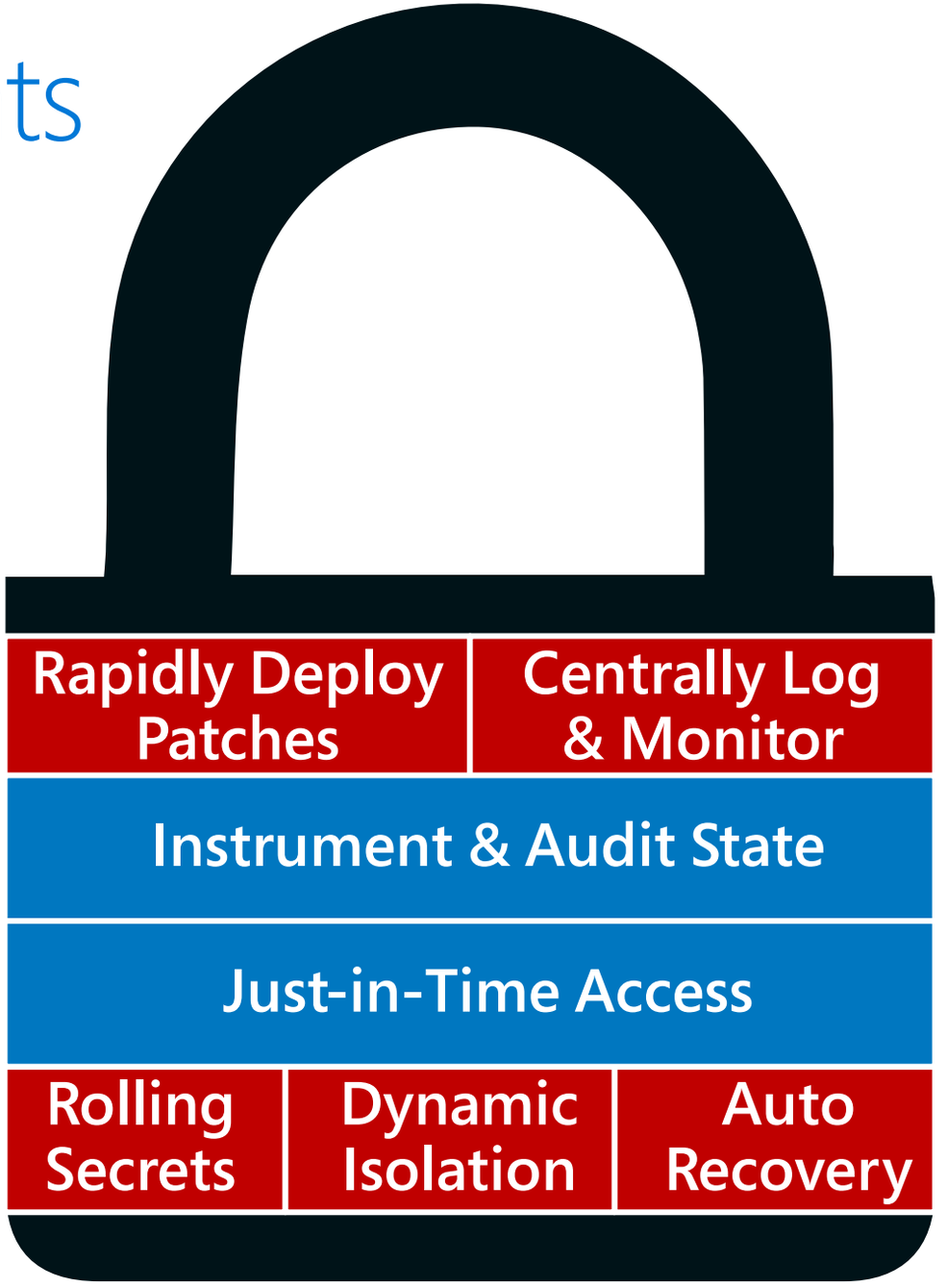
Framework to inventory damage

Identify reactive security investments

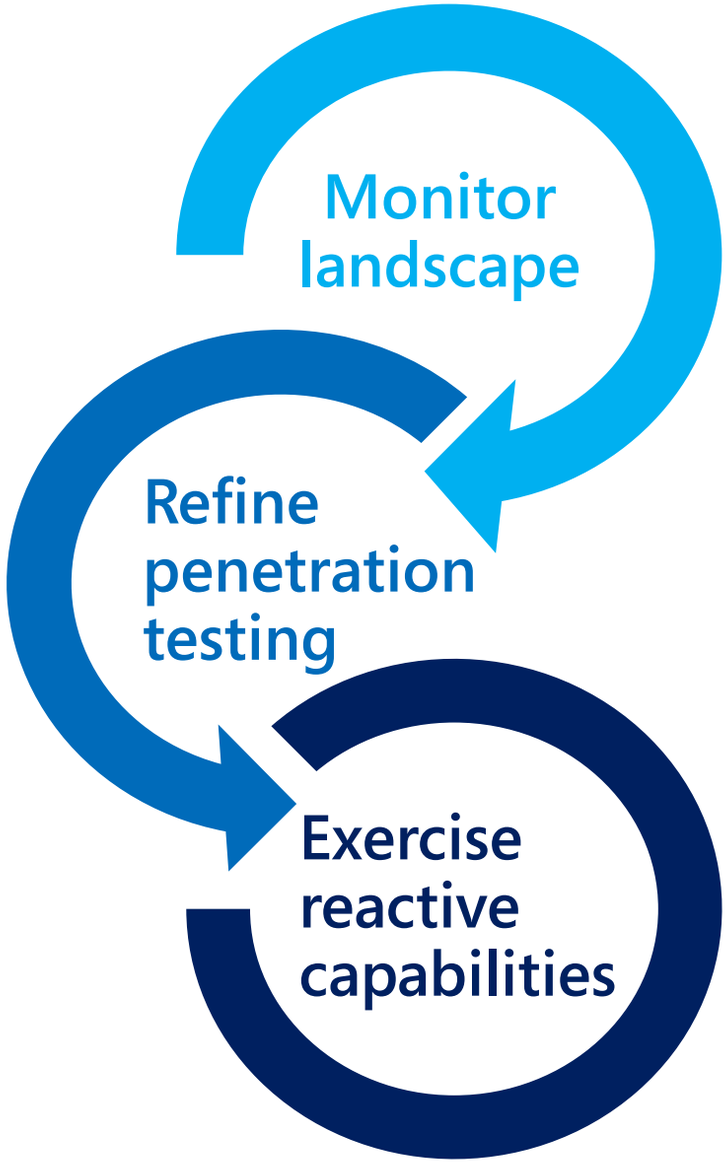
Update response plans

If you measure MTTR in WEEKS/MONTHS/YEARS instead of hours/days, then **YOU'VE FAILED!**

Reactive Security Investments



Principles



- Resist anchoring security strategy on **static attack scenarios** or assuming enemy will only come from **one fixed position**
- Utilize **defense-in-depth** – layers of complimentary security controls; effect is cumulative, increasing defense effectiveness
- **Number & distribution** of security controls is more important than individual efficiency of each
- Seek to **delay & respond** rather than **prevent** an attack

Discussion

- Think of what you are doing to help improve application security.

Lesson: Red/Blue Team Terminology

The Security Conversation

How real is the threat?

Our team is good, right?

I don't think that's possible.

We've never been breached.

Endless debates about value

Let's talk about how we change the conversation…

Lesson: Red and Blue Team Terminology

After completing this lesson you will be able to explain:

- How do Red/Blue team concepts differ from other InfoSec initiatives
- Know the differences between Red, Blue, Purple, and Green teams
- Microsoft's Evolution of Red vs Blue

Let's level-set terminology

- Red and Blue Team exercises are **not Cyberwar game exercises**
- Red and Blue Team exercises are **not Penetration Test exercises**
- Red and Blue exercises are **not Theoretical**
- Red and Blue exercises are **not disruptive to an organization**

Red Team

A Red team is an independent group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view.

https://en.wikipedia.org/wiki/Red_team

Blue Team

A **blue team** is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation.

https://en.wikipedia.org/wiki/Blue_team_(computer_security)

Other Definitions

Target –The environment you are testing

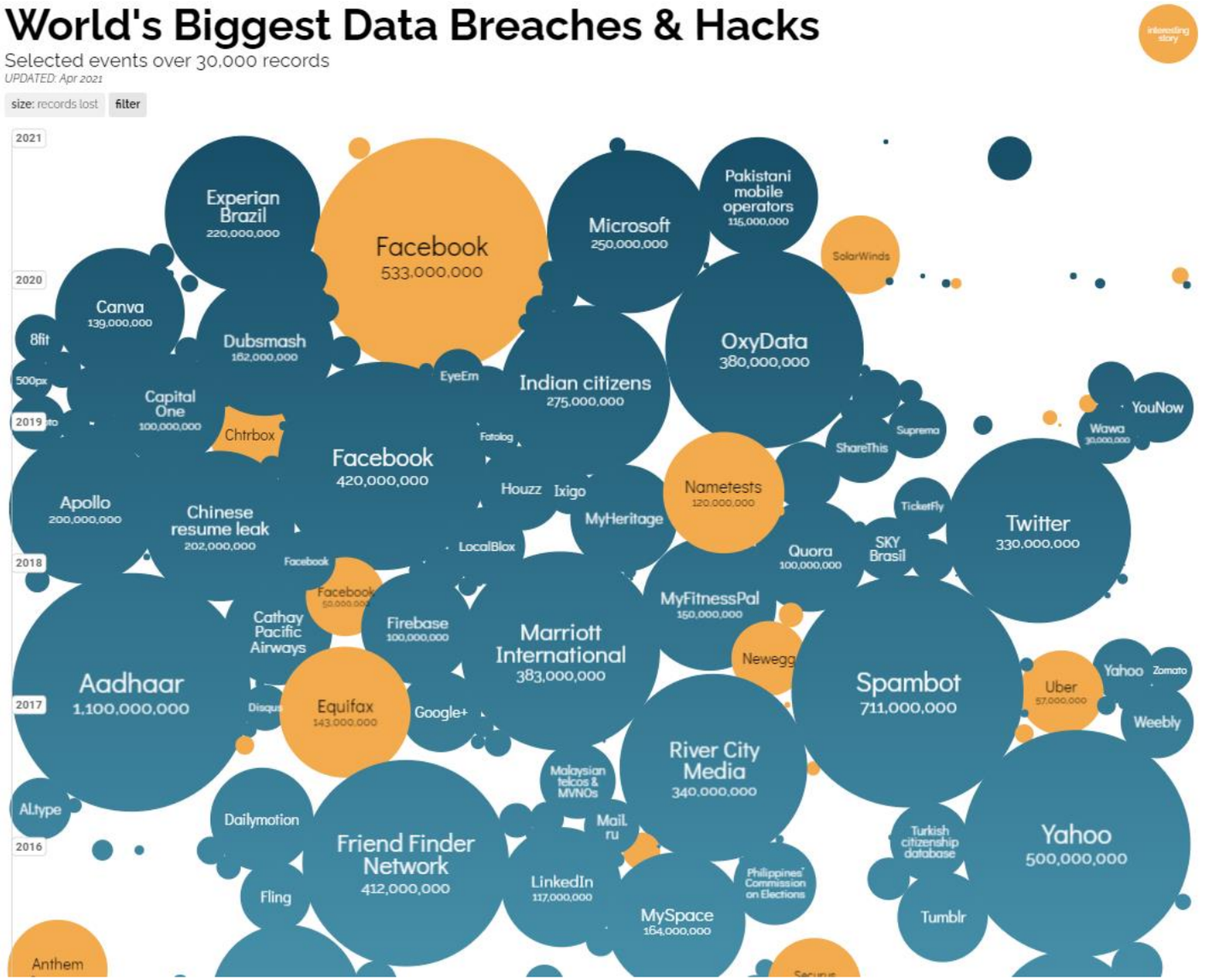
Security Guarantees – Security goals that a target needs to meet

Purple Team – Coordinated evaluation of target's security guarantees and monitoring story

Green Team - People that take systematic issues and solve them (address Bug Bar)

TTPS – Tactics, Tools, and Procedures (aka Playbook)

Consider this…



information is beautiful

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Microsoft's Evolution of Red vs. Blue

Earlier

- Identify vulnerabilities through manual code review
- Engage external pen testing company
- Report out to the team, fixes added to the backlog

2015

- Paired a handful of security-minded engineers with a pen tester (Red team)
- A few ops-minded engineers that understand the systems & logging available (Blue team)
- Attacks were successful due to poorly protected secrets, SQL injection & successful phishing campaigns

2016

- Augment both teams with outside experts (AD security and IT Security Incident Response experts)
- Comprehensive, centralized logging available for Blue team to do post-breach forensics
- Attacks were based upon Cross-site scripting (XSS), deserialization, & engineering system vulnerabilities

2017

- Red team taking longer to reach objectives. Forced to find & chain 5-6 different vulnerabilities together
- With enhancements to monitoring, Blue team is starting to catch Red team in real-time

2018

- Red Team still finding it difficult and forced to chain multiple vulnerabilities together
- Red and Blue partnering as Purple Team practice incident response & eviction
- More emphasis on supply chain security. CredScan is everywhere.

Lesson: Red Teaming

Lesson: Red Teaming

After completing this lesson you will be able to explain:

- The terms Recon, Exploit, Pivoting, Act, and Persist
- How are Recon, Exploit, Pivoting, Act, and Persist are used in Red Team activities
- A typical Red Team attack
- Rules of Engagement for Red Teams

Red Team Activities

Recon

Exploit

Pivoting

Act

Persist

Red Team: Exploit

- What vulns are out there?
  - 0-days are there
  - N-days are usually the focus
- Given enough surface, you will have a bug (and the Red team will find it)

"given enough eyeballs, all bugs are shallow" – Linus's Law

Red Team: Pivoting

- Active Directory environments are Chains of Trust
  - One account leads to another to another to a domain admin
  - Goal is to look for a High Value Asset
- Do you remember BloodHound?
  - Uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment

Red Team: Act

- Often interactive
- Where detection by Blue Team typically takes place
- Very “noisy” activities

Red Team: Persist

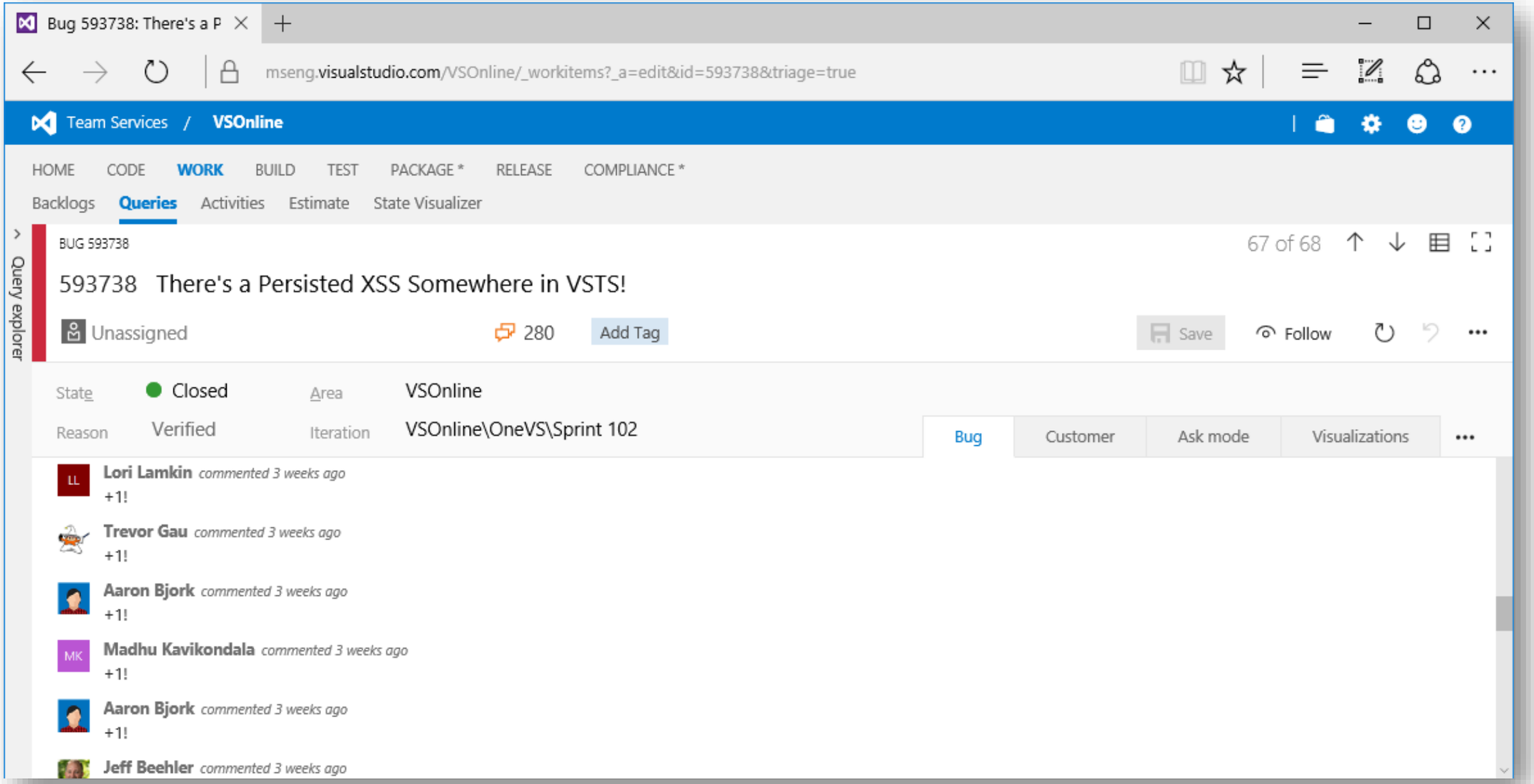
- Not standardized as it often depends on the environment you are operating in
- Evade defenses will be attempted in this stage
- Typically not as details as actual adversaries due to tooling challenges and “Rules of Engagement”

Prove it!

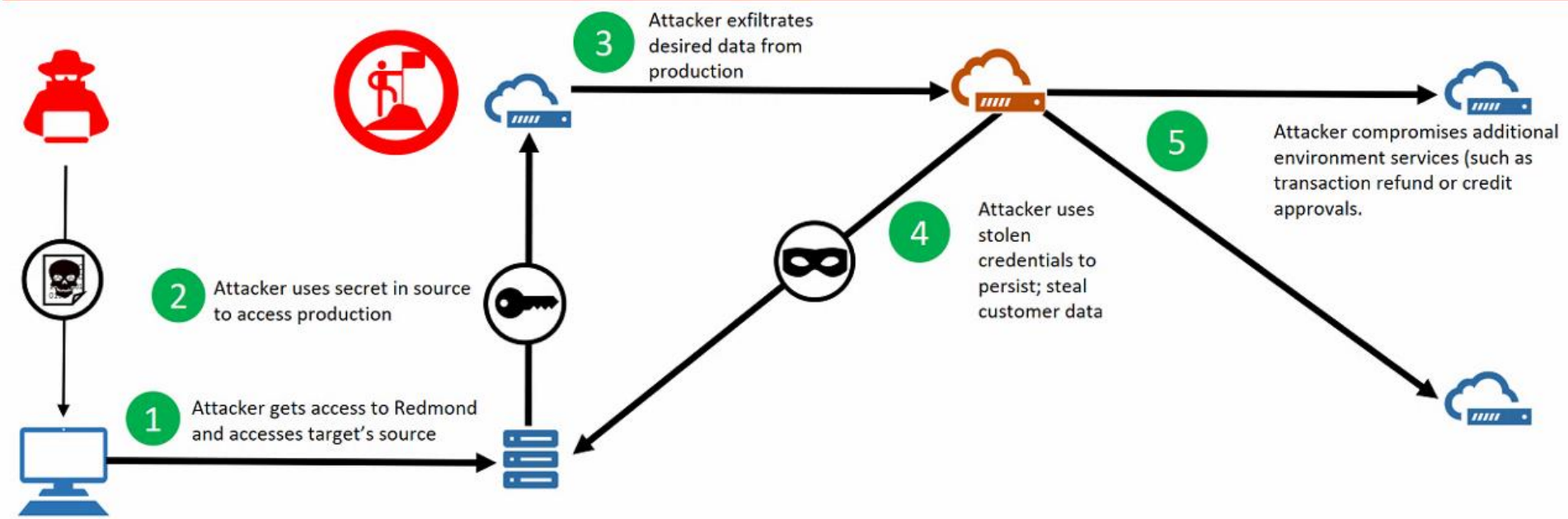
Show

Don’t tell

Every time someone viewed the dashboard…



Red Team Attack Decomposition



Event	Detection	Response	Impact & Lessons Learned
• Target's source code was pulled as part of standard recon activities and analyzed • Production Keyvault information was discovered inside source repository • Production Keyvault was accessed; all targets employees' usernames and password hashes were discovered and cracked out • Customer information was accessed, and read-write access was validated • Certificates for managing targets Azure subscriptions and targets Fabric were discovered and validated	• No actions were detected while on this engagement • Incident Response is engaged for cleanup of employee credentials and customer data	• Due to no detections; no response actions have been taken	• Implementation of automated credential scanning for places where high value data is a must • Environment separation between pre-production and production also is a must • A second look at target environment might be warranted at some time in the future (this was not planned or part of the roadmap)

https://gallery.technet.microsoft.com/Cloud-Red-Teaming-b837392e

Demo: Azure's Rules of Engagement

Review Azure's rules of engagement

Lesson: Establishing Teams

Determine your objectives

- Campaign length
- If defenses have been implemented, red teaming should be done regularly
- Consider red/blue team activities after the implementation of security measures
  - Ultimate test to determine your security posture
- Is a blue team necessary?
  - Robust IT organizations may be able to address blue team activities through existing processes

Recon and preparation

- Recon is the cornerstone of red teaming
- Make sure your team is well prepared
- The red team should understand their roles and activities
- Understand your High value assets (HVA)
- Know the attacks that real threat actors are using

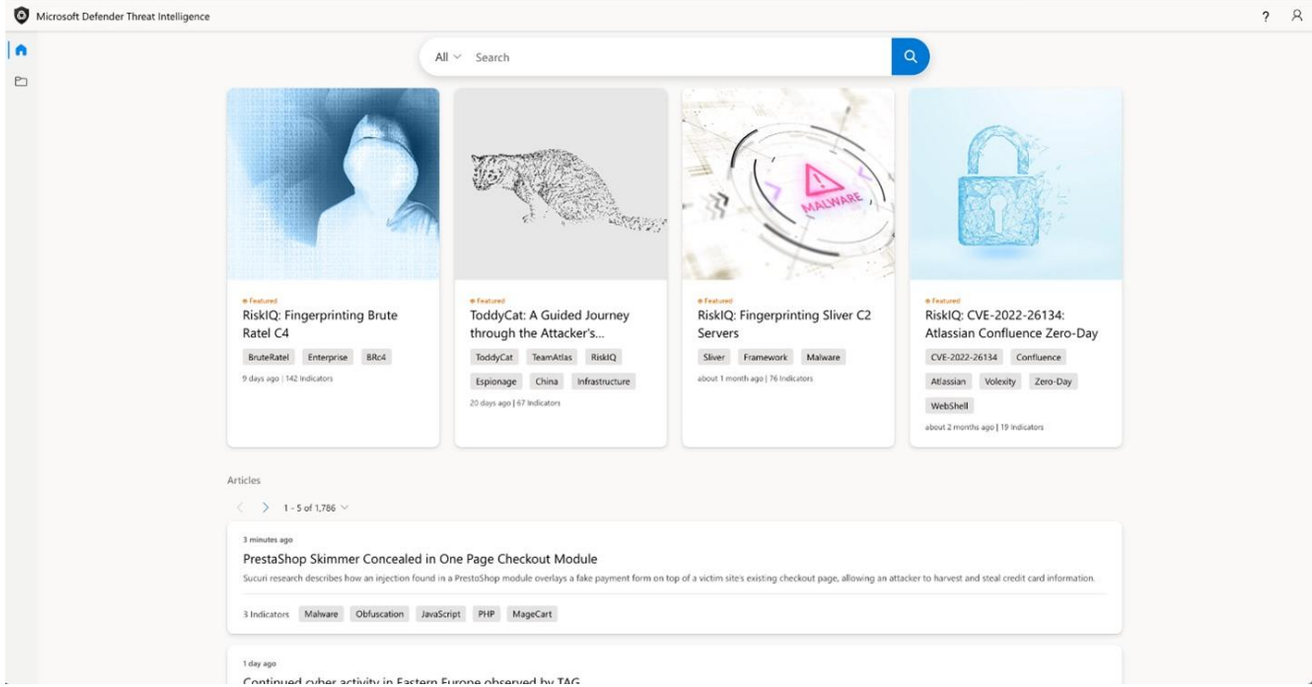
Establishing The Red Team

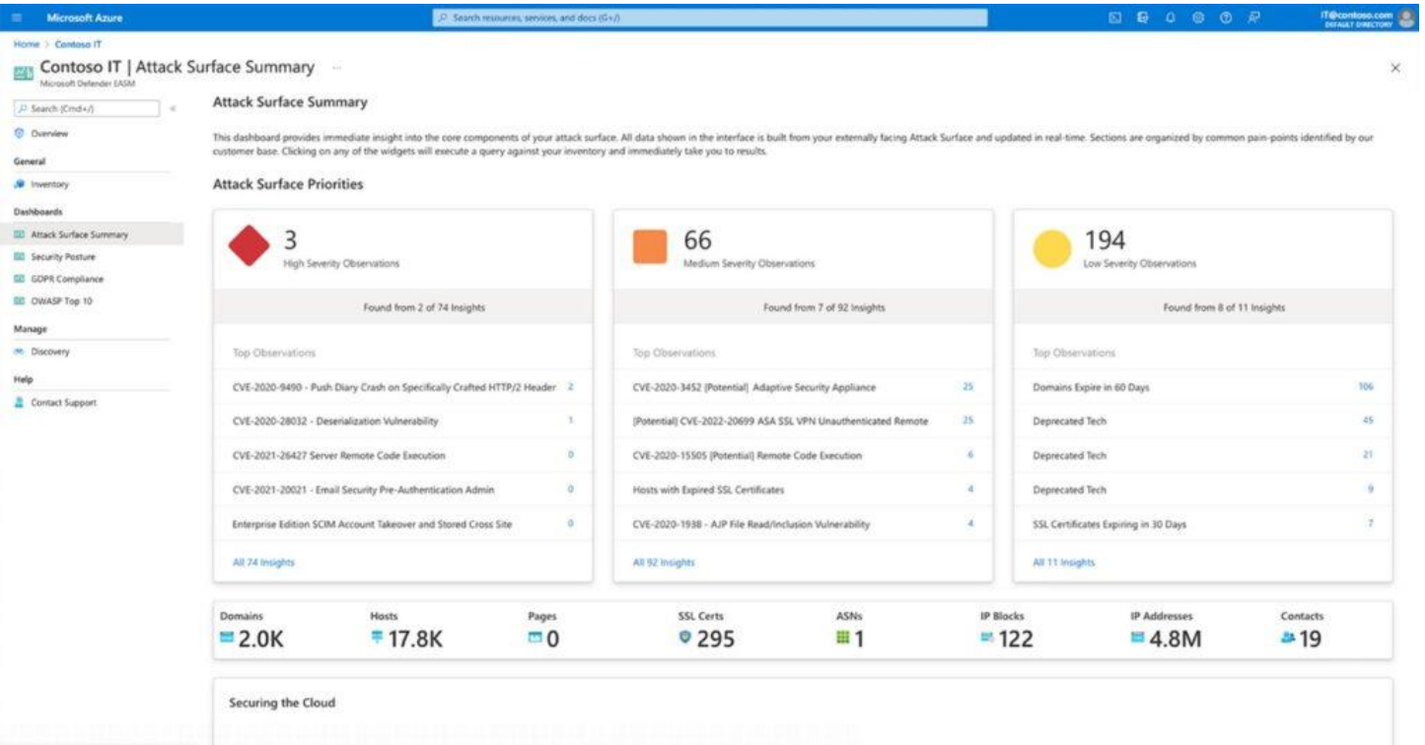
- Establish your security expertise
  - If you lack the expertise, partner with a security firm
  - Make sure testing with the security firm is inclusive
  - Ensure the security firm has reputable people in the security industry
- Learn from each exercise
- Keep up to date with the latest tools and attacks

Key things to consider

- Understand controls in the environment
- Collect and analyze your results
- Use the appropriate tools for the environment
- Assume there will be failures
- Findings need to be geared towards discovering gaps with Blue team activities
- Develop expertise and continue to learn

Unmask your adversaries with Microsoft Defender Threat Intelligence





Discover your vulnerabilities with Microsoft Defender External Attack Surface Management

Continued Education

- Measure your Time To Detect (TTD) and your Time To Mitigate (TTM)
- Leverage MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Matrix
  - https://mitre-attack.github.io/attack-navigator/enterprise/
- Know the tools:
  - **PenTesters Framework (PTF)** - Follows Penetration Testing Execution Standards (PTES) and provides all the tools (including Metasploit) in a packaged solution
  - **Red-Baron** - Red Baron is a set of modules and custom/third-party providers for Terraform for automating and creating resilient, disposable, secure and agile infrastructure for Red Teams.
  - **Cobalt Strike** - https://www.cobaltstrike.com Provides a post-exploitation agent and covert channels to emulate a quiet long-term embedded actor in your customer's network. Malleable C2 lets you change your network indicators to look like different malware each time

Demo: APT Groups and Operations Matrix

Knowledge Check

- How do Red Teams differ from Pen Testers?
  - Red teams build multi-week campaigns whereas Pen Testers are engaged for 1-2 weeks.
  - Pen testers ultimate goal is DA to the DC, whereas Red Teams outline their objectives when defining the scope of the campaign

Module Summary

- We determined why Red Teams are important
- Microsoft's journey with Red Teams and learnings
- Decomposition of a Red Team attack
- Guidelines that should be followed to help develop Red Teams