

# Attack & Response: 3 Common Scenarios & What To Do About Them

November 16, 2020

---

**INNOVATE. TRANSFORM. SUCCEED**

Adapt to the new business reality.



**protiviti**<sup>®</sup>  
*Face the Future with Confidence*

**\*Note: To ensure the best webinar experience, we recommend that you use Google Chrome as your web browser.\***

## A FEW REMINDERS

#ProtivitiTech

1

Audio will be streamed through your computer.

2

If you are experiencing technical difficulties during the webcast or you have a question during the webinar, let us know by submitting your questions through the Q&A area of your screen.

3

We are recording today's webinar and it will be available for on-demand viewing following the live event.

4

Chrome is the recommended browser. Earlier versions of IE are no longer supported so if you are experiencing issues, please update IE or download Chrome.

5

CPE credits are available for this webinar.



**Sean Webb**

Managing Director  
Security & Privacy  
Protiviti

[Sean.webb@protiviti.com.au](mailto:Sean.webb@protiviti.com.au)

### **2020 Trends**

### **Scenario 1: “Assumed Breach” Penetration Test**

### **Scenario 2: Cloud Compromise**

### **Scenario 3: Ransomware and Medical Devices**



## 2020 Trends



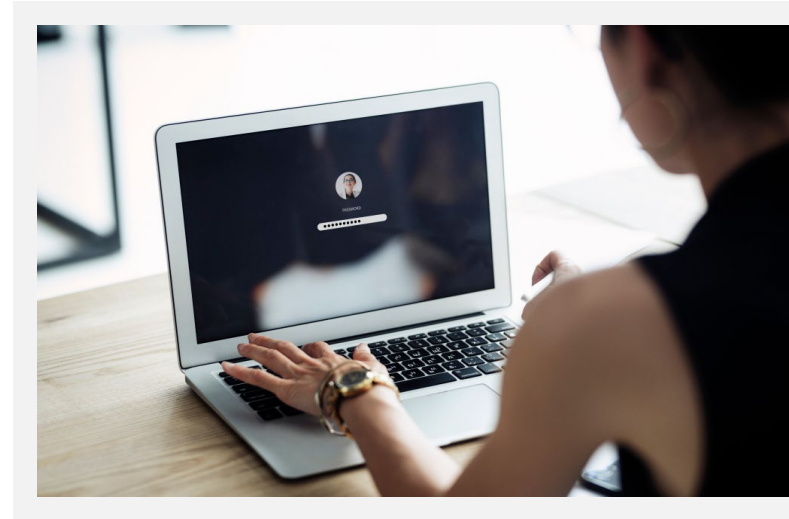


- Phishing
- Ransomware
  - Uptick on attacks on public sector
  - Failure to pay results in release of data
- Credential Stuffing
- Accidental Data Exposure
  - Databases
  - Cloud storage





- Password guessing is getting harder
  - Effective deployment and configuration of blocklist solutions
  - ... although not impossible
    - Training still doesn't appear to have an impact
- Directly exploitable issues are still there, but much less frequent
  - Continued decline over the past couple of years
- Phishing requires a more targeted approach
  - E-mail security solutions have upped their game
    - URL scanning and sandboxing technologies
  - Routine training is effective





- Remote work is here to stay
  - Will be more prevalent, even after pandemic
- Less or no folks in offices means:
  - Reduced traffic on internal and wireless networks
  - Higher bar for physical social engineering
- Scenario-based testing
  - Stolen laptops
  - “Assumed Breach”







- Tailored threat emulation scenarios
- Perspectives on impact potential based on access provided
  - Simulation of credential compromise
    - Employees
    - Vendors
  - Malware infection
    - EDR resilience
    - SOC/NOC/IR team response



When is your organization planning on returning to your office(s)?

a) Already returned



b) In less than 6 months



c) Beyond 6 months



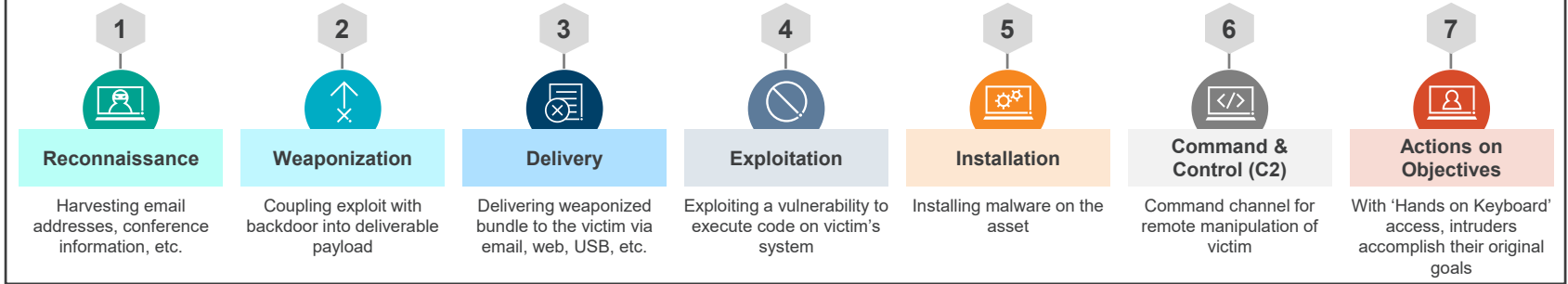
d) Unsure, and unlikely to return in normal state



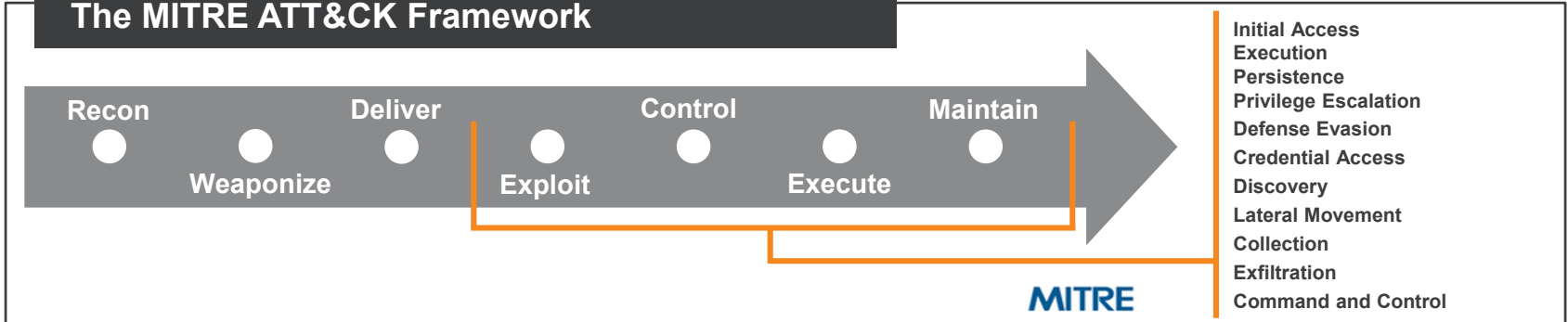
A snowy owl is perched on a branch in a snowy forest. The entire image is overlaid with a teal color. A white rectangular box is positioned in the center, containing the text "Scenario 1: Assumed Breach Penetration Test".

## Scenario 1: Assumed Breach Penetration Test

## The Cyber Kill Chain



## The MITRE ATT&CK Framework

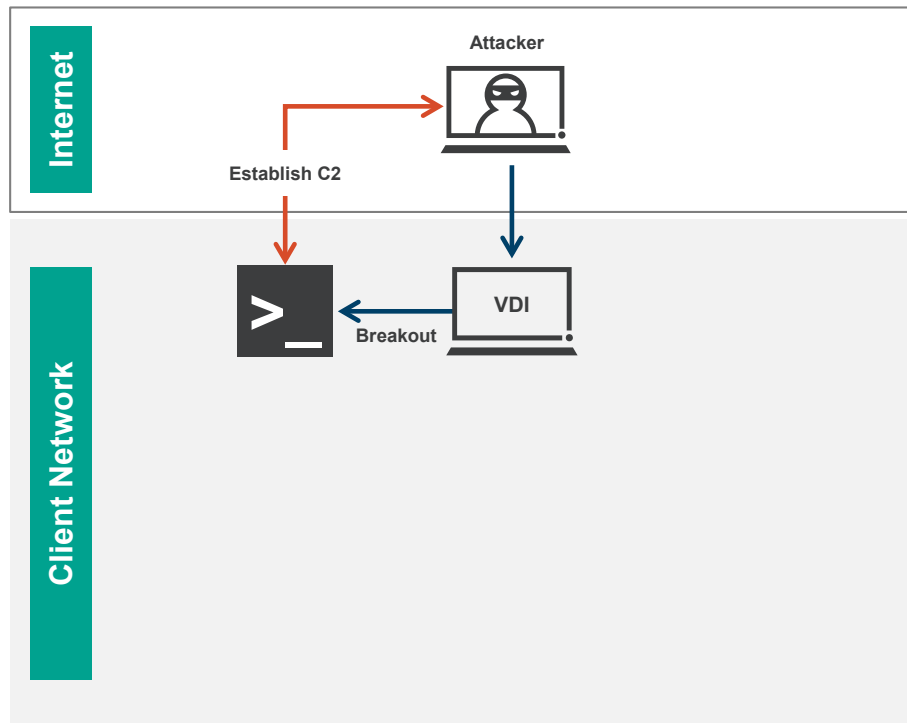


1 Access VDI environment

2 “Break out” of VDI

3 Access command line

4 Download and execute C2 payload



1

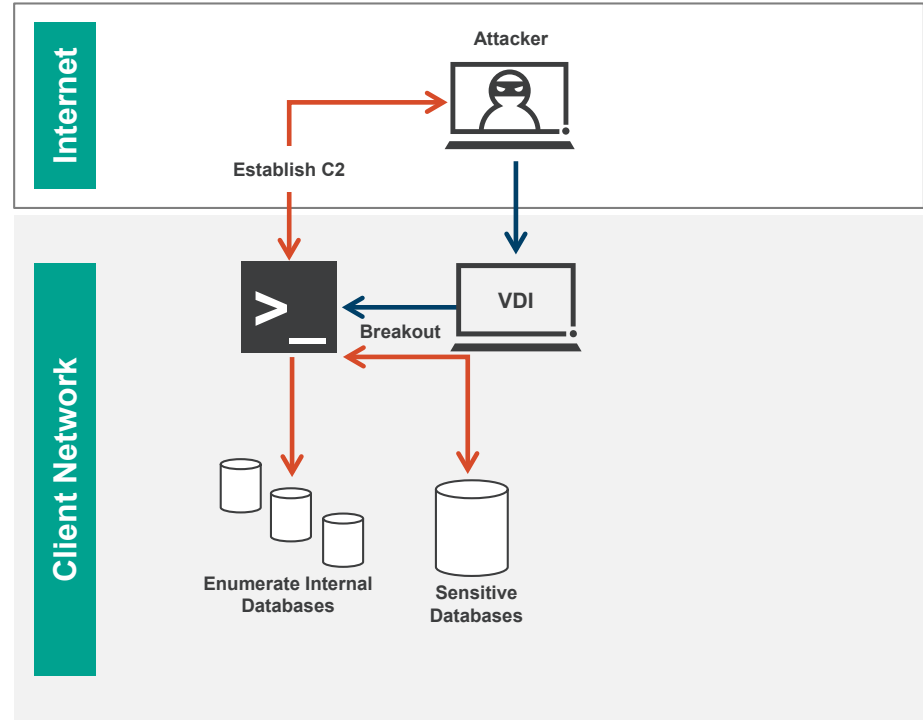
Load tooling into memory

2

Hunt for data

3

Obtain access



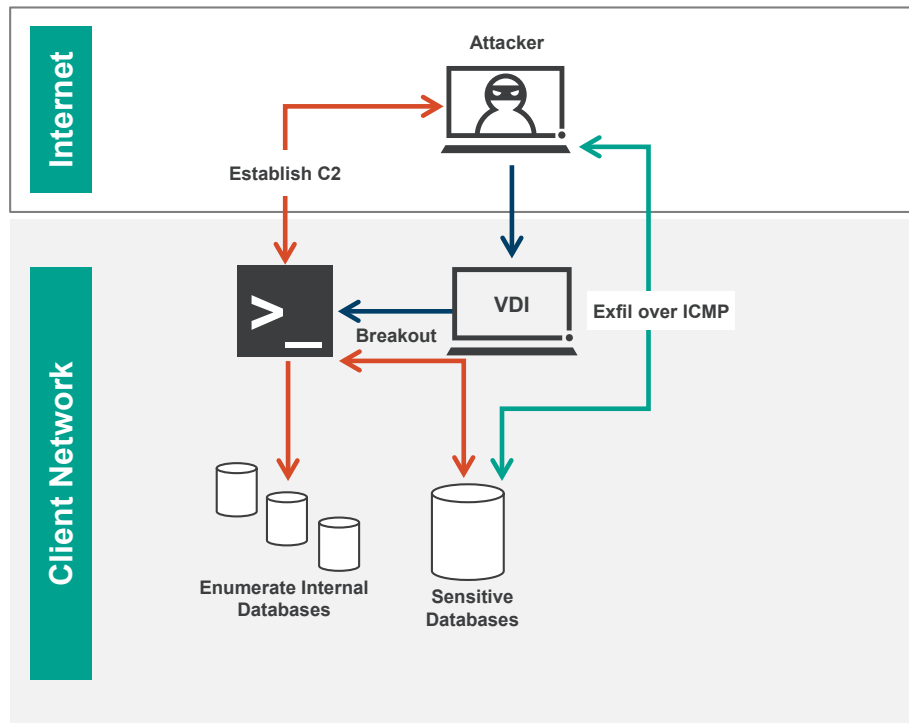


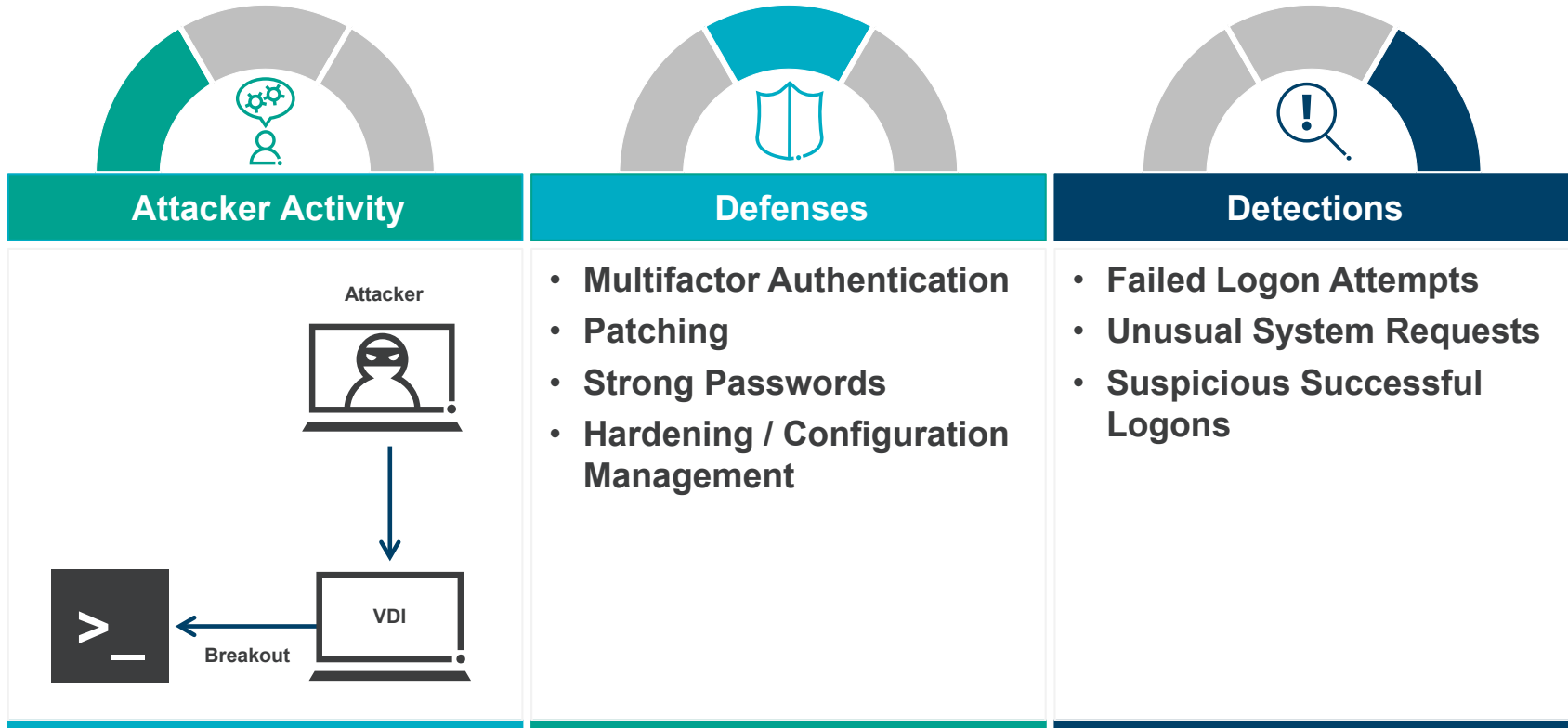
1 Test outbound policies

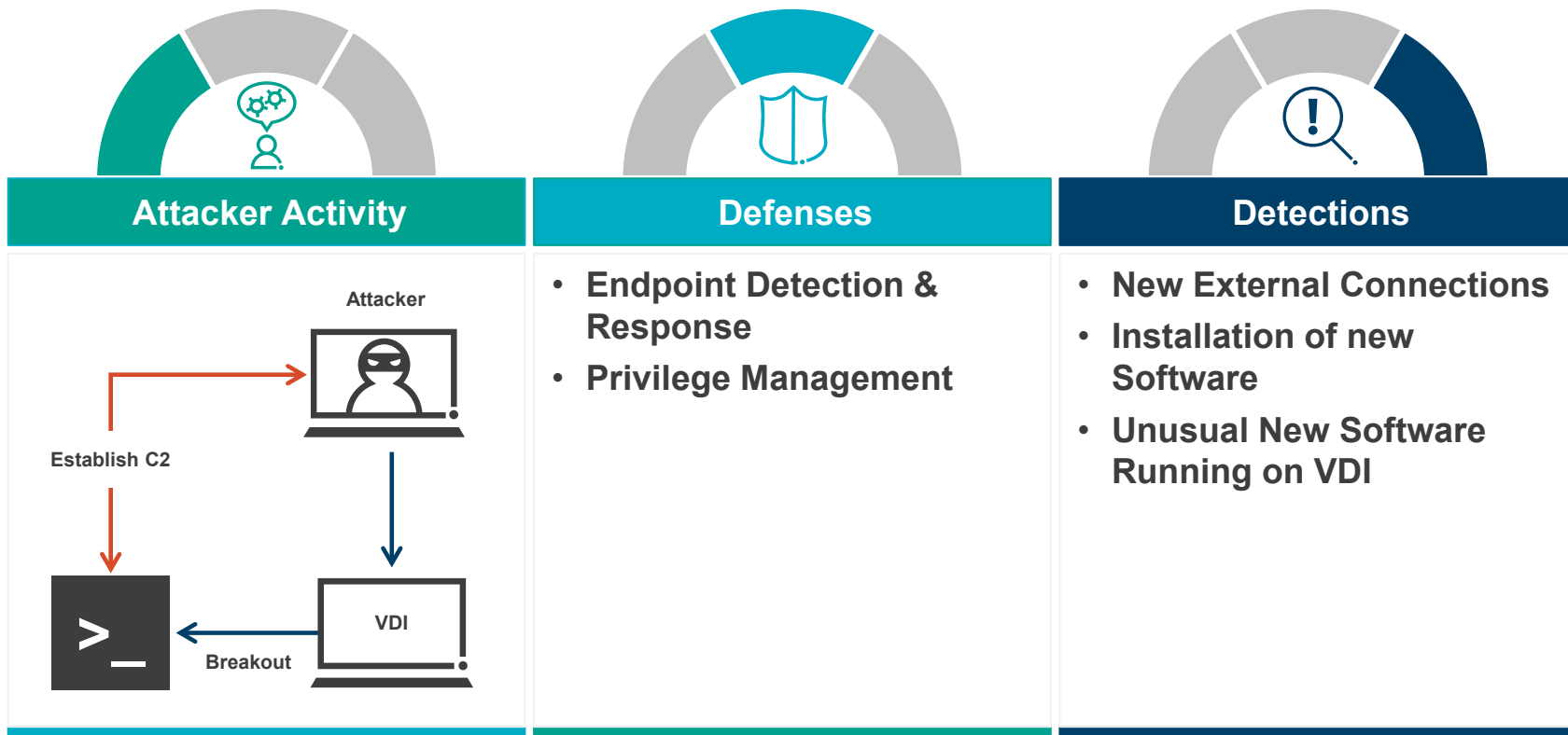
2 Find a method that works

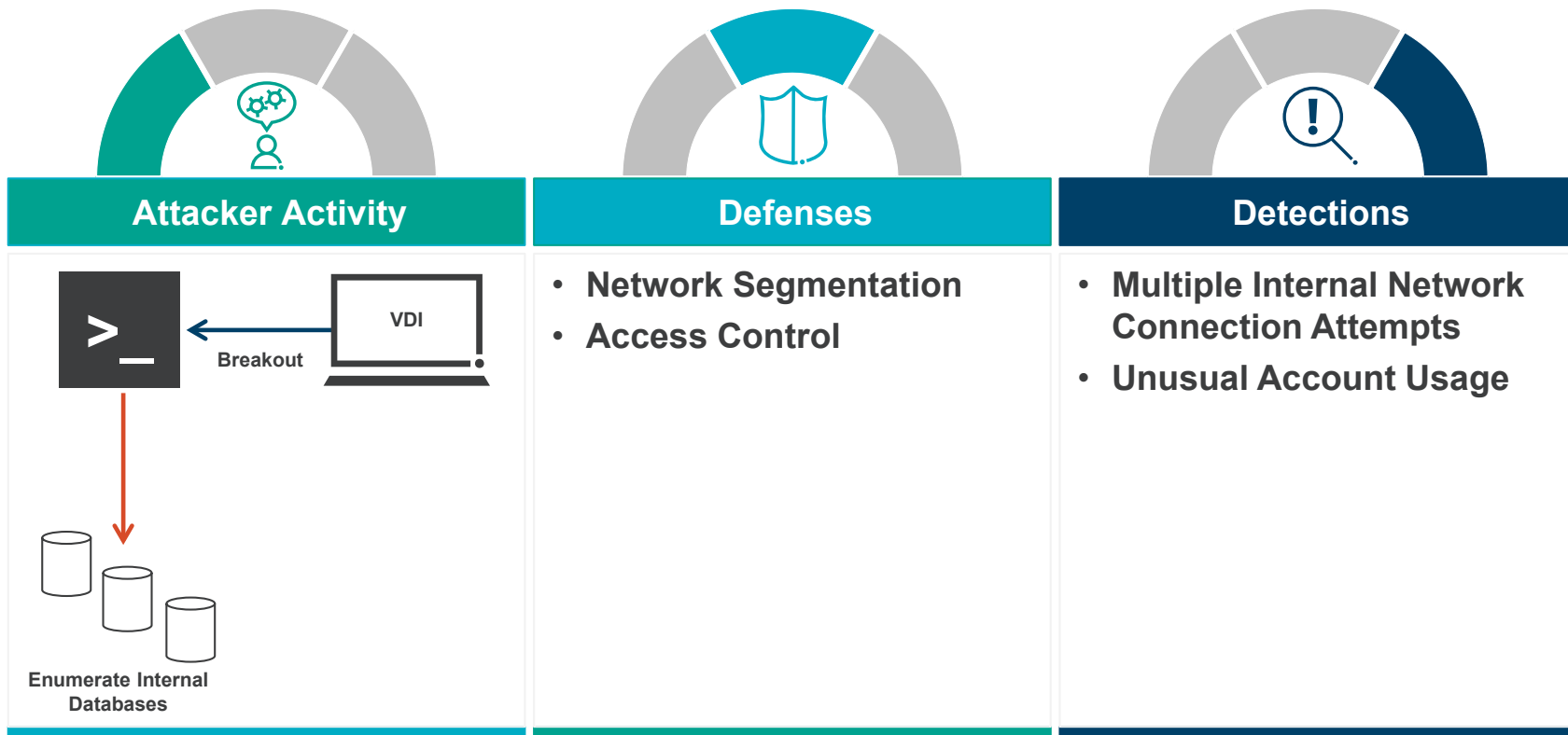
3 Transfer data out

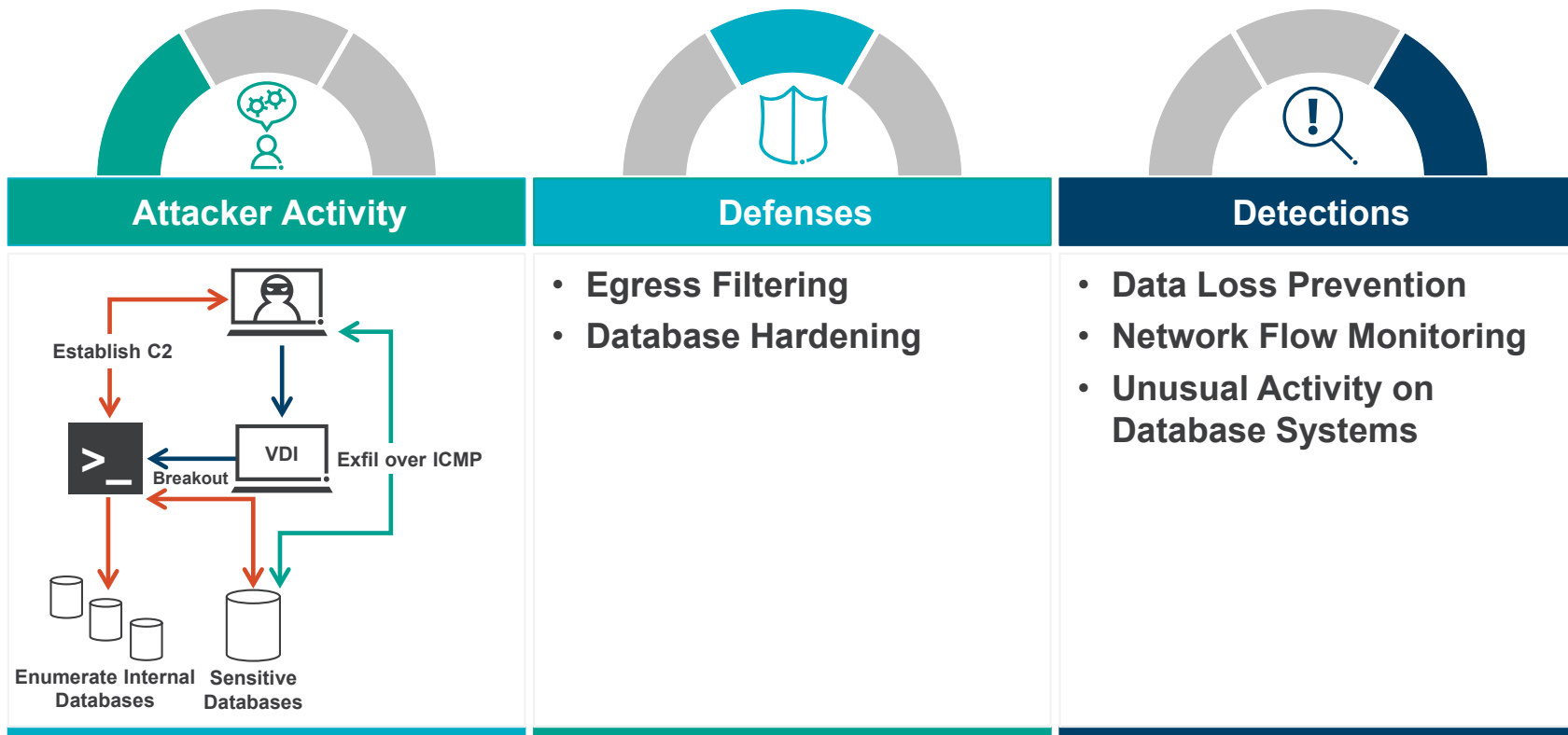
4 \$\$\$













Frameworks can be used to model threat actor behavior and design defenses



Being able to discern normal from anomalous activity is crucial



Multiple opportunities during the attack to defend or detect the attack



This approach can apply to any environment or scenario in your threat model





## Scenario 2: Cloud Compromise

What is your experience with assumed breach testing?

a) We're not ready for one yet



b) We're ready, but haven't done one yet



c) We've performed them, but haven't reviewed all possible scenarios



d) Unsure



```
2020-09-23 09:39:06 EDT [REDACTED] ~> aws s3 --profile awscli cp s3://[REDACTED]2020/passwords.txt .  
download: s3://[REDACTED]2020/passwords.txt to ./passwords.txt  
2020-09-23 09:39:34 EDT [REDACTED] ~> cat passwords.txt  
password123
```



- Reconnaissance sometimes reveals much more than expected
- Misconfiguration and excessive permissions expose more than you realize
- Code repos are a treasure trove
  - Often contain secrets used to access cloud infrastructure

## Common Challenges



Hard-coded Secrets / Credentials  
Committed to Public Code Repositories



Retention and Storage of Secrets in  
Unencrypted Tools



## Potential Solutions

Utilize Cloud Native Secrets Management  
Services



Integrate Pre-Commit Security Solutions to  
Scan for Secrets (e.g., API keys, SSH keys)



**SEDATED**  
Sensitive Enterprise Data Analyzer To Eliminate Disclosure

## Common Challenges



Ad-hoc deployments of cloud resources and policy alignment



Configuration drift across enterprise cloud accounts



## Potential Solutions

Deploy Cloud Access Security Broker (CASB) to monitor cloud posture



Utilize Cloud Native Infrastructure as Code (IaC) service that incorporates leading security standard (CIS Benchmarks)



Integrate CaC Scanning Solutions



CHEF INSPEC™

## Common Challenges



Unpatched public cloud resources with known vulnerabilities



Inappropriate access to cloud resources and underlying data



## Potential Solutions

Timely Patch Public Cloud Resources

Deploy Cloud Native Web Application Firewalls (WAFs)



Deploy Cloud Native API Gateways







Implement Cloud Native Secrets Management Solutions



Utilize Cloud Native IaC Services to Standardize Cloud Infrastructure Deployments



Patch Public Cloud Resources and Deploy Cloud Native WAF and API Gateway Services



Deploy a Cloud Access Security Broker (CASB) to monitor cloud posture



## Scenario 3: Ransomware and Medical Devices



- Broad application of these issues
  - Seeing variation of these in all environments
    - Not just IoT and Medical Devices
- Broad application of controls
  - Same mitigation/response applies to most systems/environments





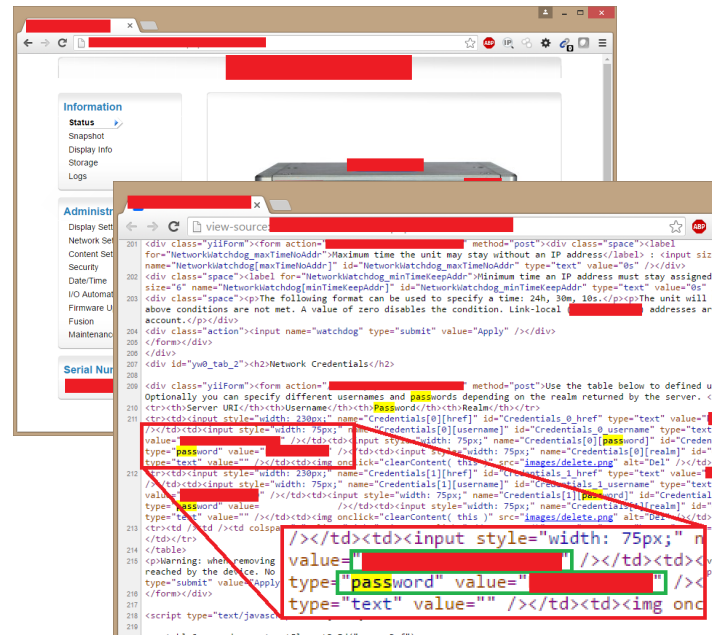
- Medical records are worth more on the black market
  - (roughly \$1 instead of cents like credit card data)
- Hospitals react reflexively because time is often very precious in a hospital setting
- Medical devices are attacked both incidentally & directly
  - Incidentally because they are often difficult to secure in HDO environments
  - Directly because they are an appealing target to bad actors



© picture-alliance/idpa/R. Bonss



- Devices have an extremely long life span (years-decades) - security changes rapidly (months)
- Actors are increasingly sophisticated
- Platforms - exploits are abundant
  - Windows
  - Android
  - Linux
- MDs/Hospitals need 'always working' capabilities
  - Common controls like 2FA don't make sense



1

Obtain access to network

- Stolen/stuffed credentials

2

Focused search for medical imaging devices

- Listen for broadcasted DICOM traffic
- Specific services/ports (TCP and UDP 104)

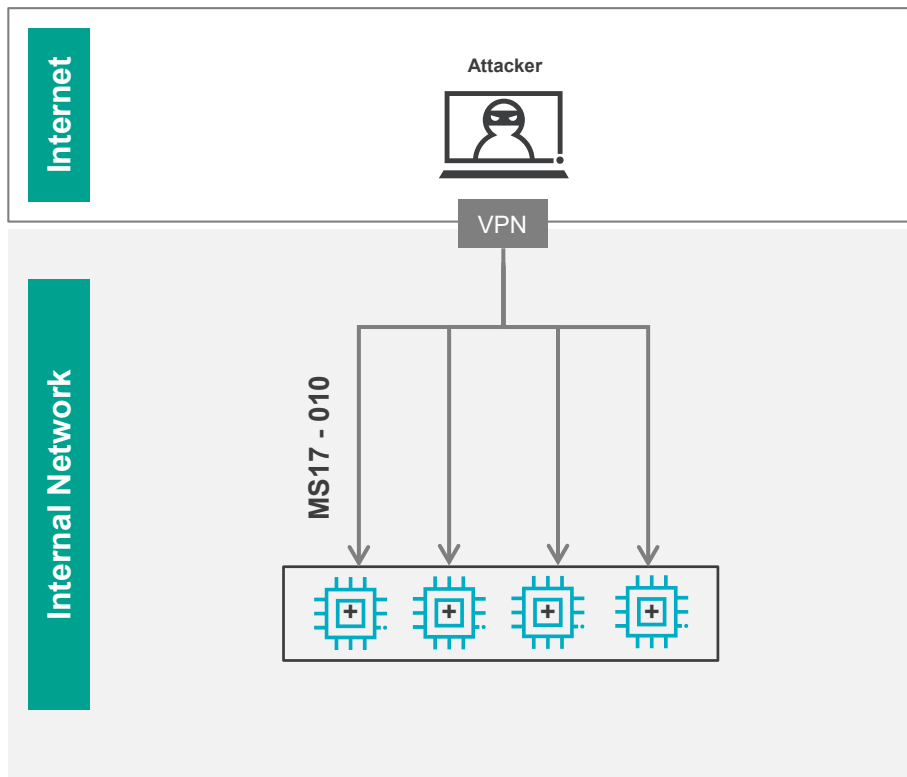
3

Exploit via...

- Default credentials
- Missing patches

4

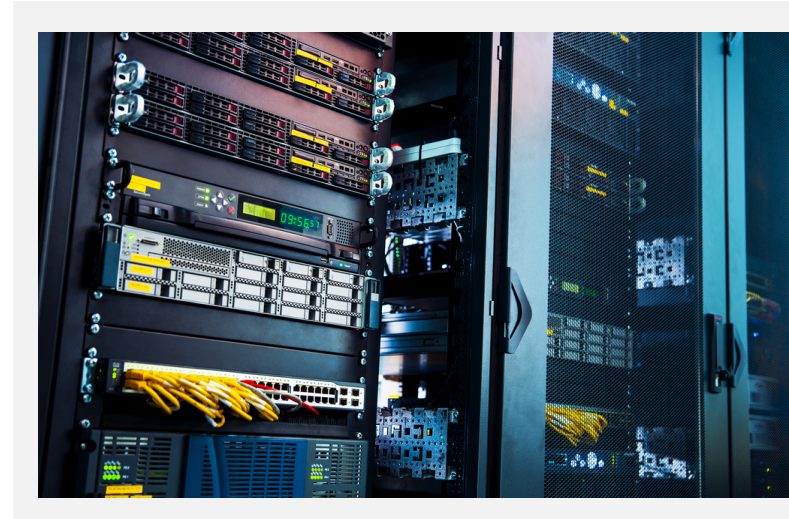
Encrypt and Ransom!







- Device isolation/micro-segmentation
- Updateability/Patching (FDA requirement)
- Device lockdown (change default passwords)
- Specialized device security scan engines
  - Medigate
  - Ordr





IoT & Medical devices can and will be attacked



These devices are traditionally more vulnerable



Off-device (network based) controls should be used



Ask about device security during the procurement process





Q&A

# RECOMMENDED RESOURCES

#ProtivitiTech

## [Source Code Repositories and Mishandled Secrets](#)

## [Protiviti Perspective: Verizon 2020 Data Breach Investigations Report](#)

## [Is Software Defined Perimeter the Best Method for Adopting a Zero Trust Strategy?](#)

## [Five C's for Cost Savings in the Cloud](#)



**Source Code Repositories and Mishandled Secrets**

by I.D. Morris | September 14, 2020 | 4 min read

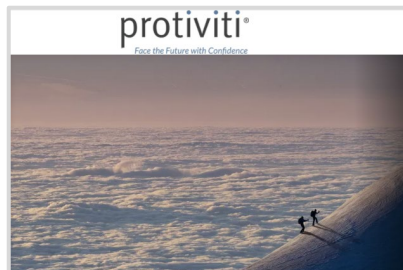
As the DevOps revolution continues to sweep across the IT landscape, source code repositories have become a prominent resource for most organizations. They provide a centralized place to track, document and collaborate on changes to applications, a critical component of modern continuous integration/continuous delivery (CI/CD) workflows. The automation of the technology stack necessary to support an application is a key facet of the DevOps model and the Infrastructure as Code (IaC) paradigm has extended the usefulness of DevOps and source code repositories to "traditional" applications.



**Protiviti Perspective: Verizon 2020 Data Breach Investigations Report**

by Roger Delph | August 27, 2020 | 4 min read

Security data nerds look forward to the annual release of the Verizon Data Breach Investigations Report (DBIR). The report contains a breakdown of the prior year's security incidents and breaches and provides trending data that mature security programs can benchmark against. One of the surprises in this year's report is that organizations are discovering 60 percent of data breaches in days or less and containing 80 percent of breaches in the same timeframe. Most organizations think this is due to more breaches being



**Is Software Defined Perimeter the Best Method for Adopting a Zero Trust Strategy?**

by Megha Kadi | September 10, 2020 | 6 min read

Enterprise networks have been described as being like an egg, with a hard shell on the outside and soft on the inside. There have been heated dialogues between security professionals that treat the "intruders" as trusted and anything outside the network as a threat. However, this thought process begins to change after the introduction



**Five C's for Cost Savings in the Cloud**

by Teri Dye, Randy Aminech | April 6, 2020 | 3 min read

In Protiviti's most recent [Finance Trends survey](#), more than half (58%) of the respondents said they plan to increase their spending on cloud applications in 2020. Considering this number includes those who are contemplating migration or have already migrated to the cloud, the adoption of these technologies is not just a possibility but rather, a reality.

For many, the business drivers to utilize cloud technologies was built on a few basic premises – availability, accessibility, modernization and of course, decreased cost.

[Looking for more? Check out our Tech Insights Blog](#)

*Face the Future with Confidence*