IS YOUR ORGANIZATION PREPARED FOR A BREACH?

February 15, 2023 • Sean D. Goodwin, GSE

Introduction

Sean D. Goodwin, GSE

CCSP, CISA, CISSP, GCCC, GCIA, GCIH, GCUX, GCPM, GCWN, GDAT, GSEC, PCIP, QSA

Senior Manager – DenSecure

✉ sdgoodwin@wolfandco.com

☎ 617.261.8139

OVERVIEW

Sean is a Senior Manager in Wolf's Advisory Group leading the team of cybersecurity experts, DenSecure™. Wolf's DenSecure boasts a team of cyberthreat experts with a diverse knowledge base. Our team's wide array of certifications means they're prepared to address a variety of defense scenarios and offer outstanding guidance customized to your needs. Our team works with internationally recognized databases and frameworks like Penetration Testing Execution Standard (PTES), MITRE ATT&CK®, and OWASP to ensure we offer comprehensive strategies.

Sean resides in Western Massachusetts with his family and can usually be found with his dog within arms reach.

HOW TO PREPARE FOR A BREACH

EXECUTIVE BUY-IN

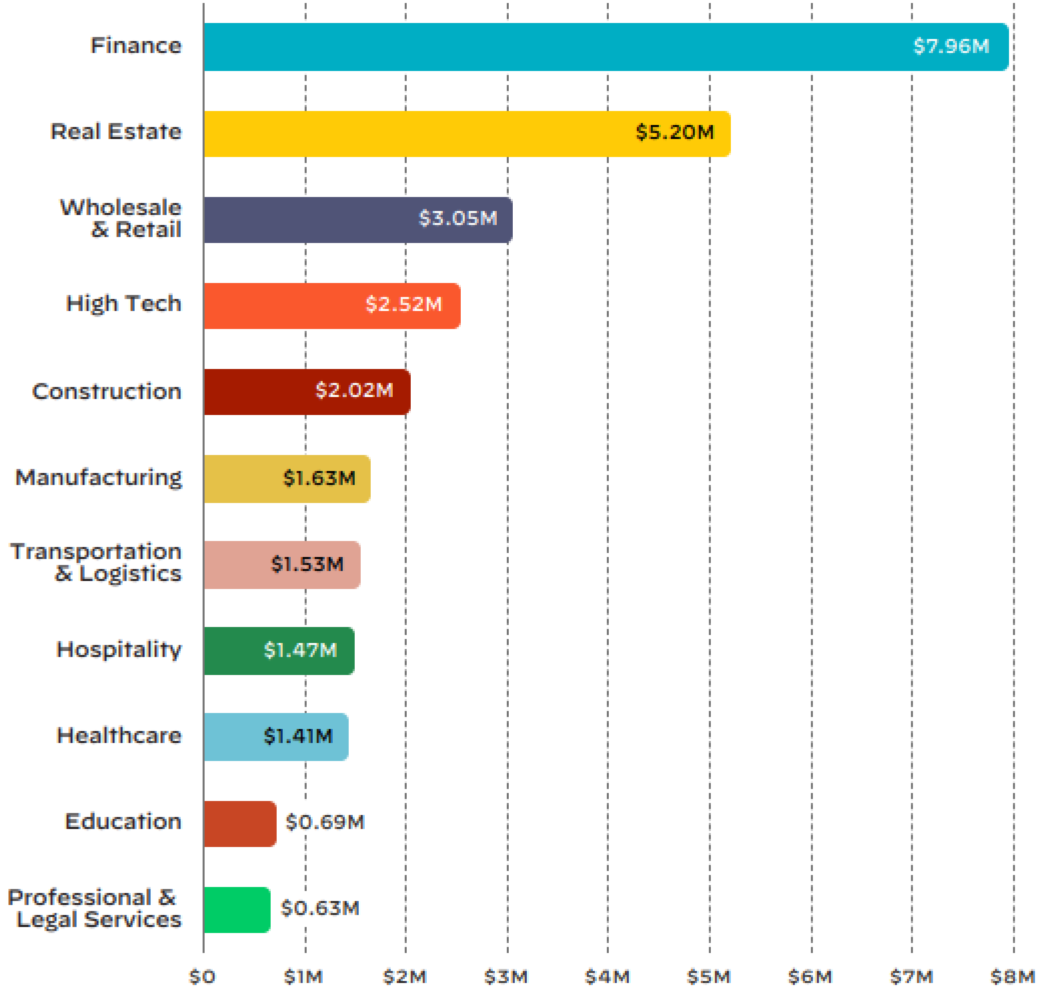


Figure 6: Average Ransom Demand by Industry

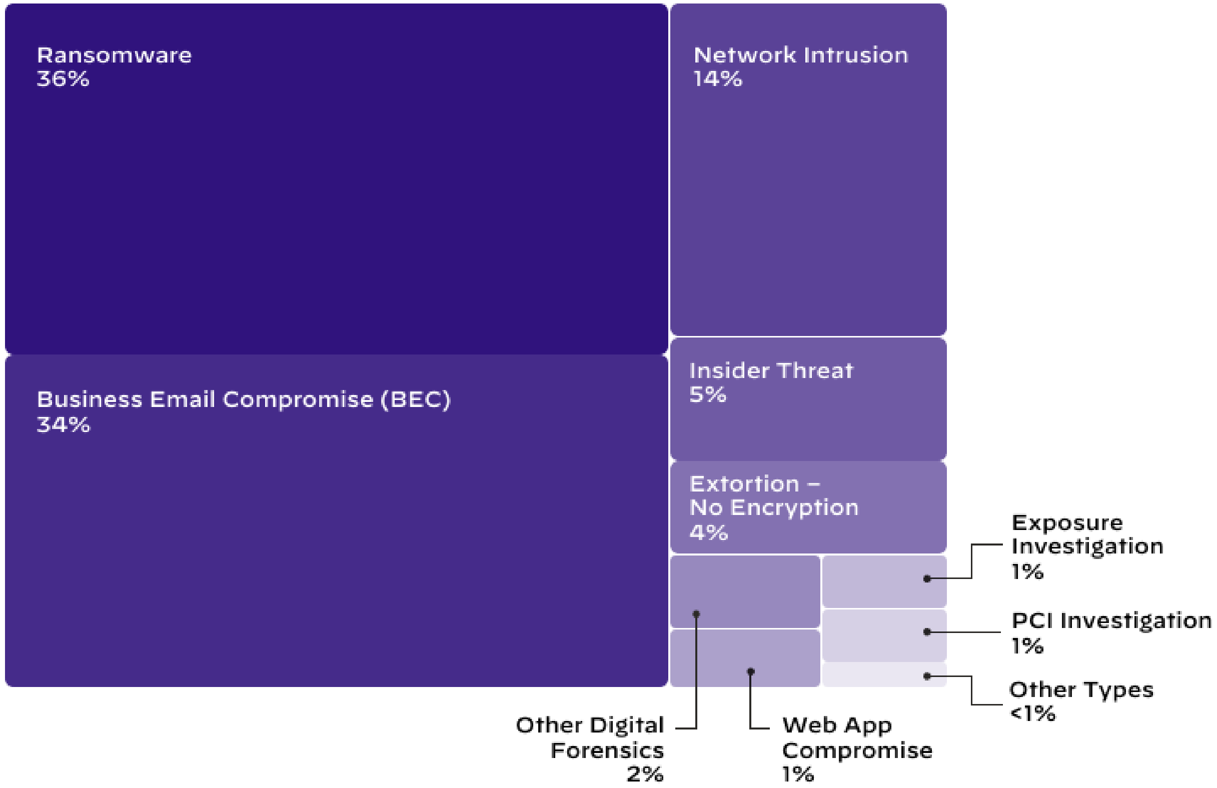


Figure 1: Types of Investigations Conducted by Unit 42 in 2022

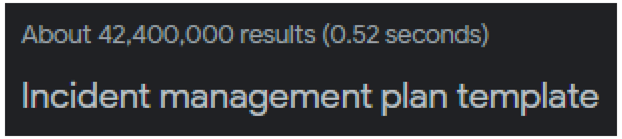
https://start.paloaltonetworks.com/2022-unit42-incident-response-report

BEST PRACTICE GUIDANCE

- CIS CSC #17 *Incident Response and Management*
- *NIST SP 800-53r5* Security and Privacy Controls for Information Systems and Organizations
- NIST 800-61r2 Computer Security Incident Handling Guide

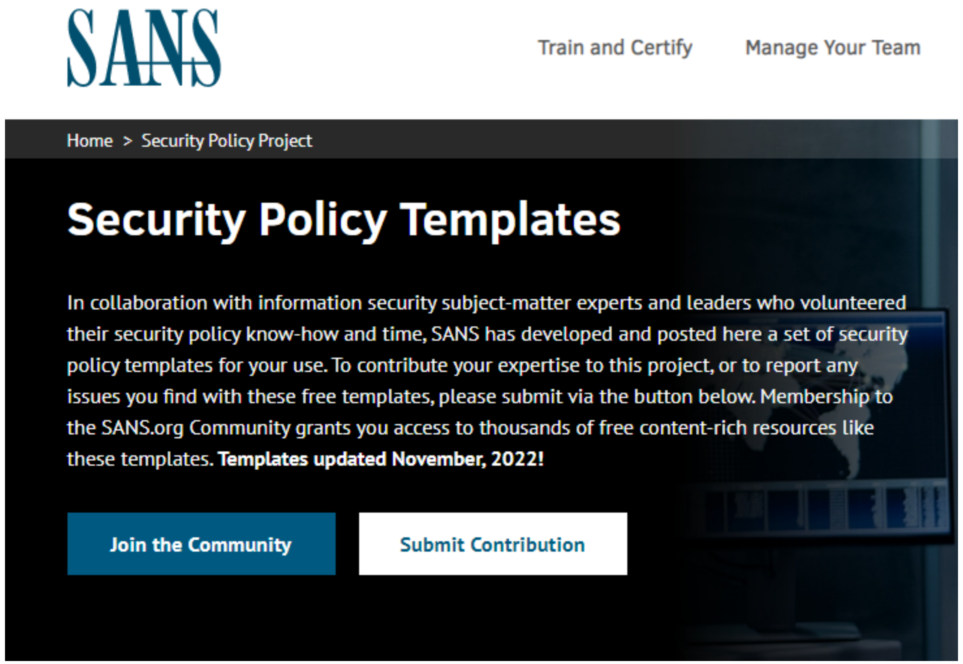
DOCUMENT YOUR PLAN

- Start small and get something in place
  - Plan for it to be a living document
- Don't boil the ocean
  - Focus on High-Likelihood incidents first



About 42,400,000 results (0.52 seconds)

Incident management plan template



Security Policy Templates

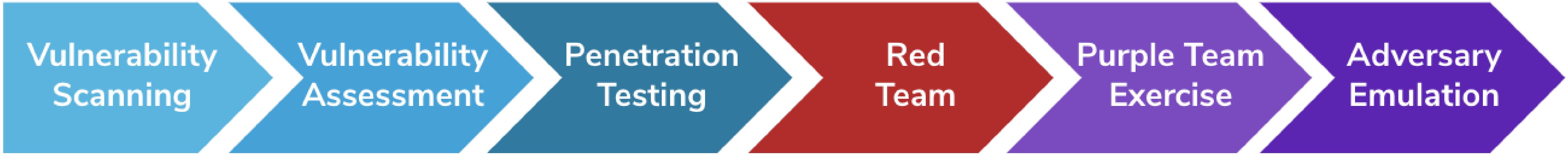
In collaboration with information security subject-matter experts and leaders who volunteered their security policy know-how and time, SANS has developed and posted here a set of security policy templates for your use. To contribute your expertise to this project, or to report any issues you find with these free templates, please submit via the button below. Membership to the SANS.org Community grants you access to thousands of free content-rich resources like these templates. **Templates updated November, 2022!**

TABLETOP TESTING

- Start small (both in team and scenario details)
- Identify the expected outcomes & get buy-in early
- Scenario Inspirations:
  - CISA Tabletop Scenarios
  - NARUC Cybersecurity Tabletop Exercise Guide
  - Backdoors & Breaches (DnD for IR)
  - CIS Six Tabletop Exercises to Help Prepare Your Cybersecurity Team

LIVE TESTING

- Don’t wait until you are ready for a formal Red Team – you can try to “catch” your regularly scheduled penetration tests
  - Which attacker techniques can you identify (alerts, logs, etc.)?
  - Which attacker techniques will you be unable to prevent?
  - What would your response look like (start creating runbooks)?



SCYTHE’s Ethical Hacking Maturity Model

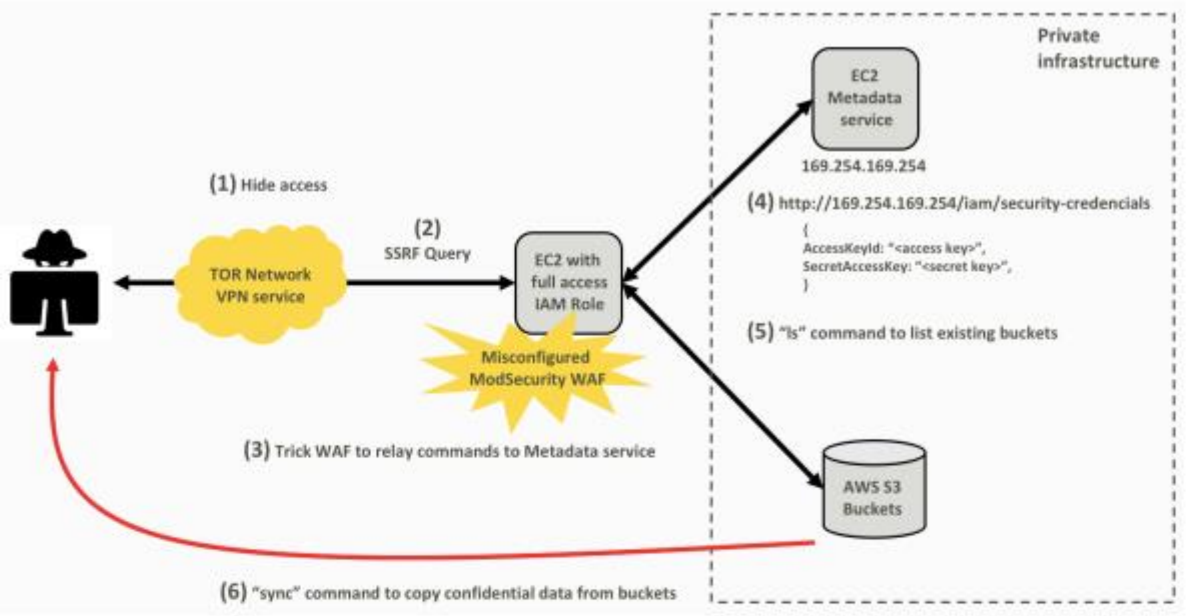
WHAT DOES A BREACH LOOK LIKE

CAPITAL ONE CASE STUDY

- “On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information from Capital One credit card customers and individuals (…).”
  - Capital One’s public report released on July 29, 2019
- According to the FAQ published by Capital One, the company discovered the incident thanks to their Responsible Disclosure Program on July 17, 2019, instead of being discovered by regular cybersecurity operations.

CAPITAL ONE CASE STUDY

- The FBI and Capital One identified several accesses through anonymizing services such as TOR Network and VPN service provider IPredator, both used to hide the source IP address of the malicious accesses;
- The SSRF attack allowed the criminal to trick the server into executing commands as a remote user, which gave the attacker access to a private server;


Private infrastructure
EC2 Metadata service
169.254.169.254
(1) Hide access
(2) SSRF Query
TOR Network VPN service
EC2 with full access IAM Role
Misconfigured ModSecurity WAF
(3) Trick WAF to relay commands to Metadata service
(4) http://169.254.169.254/iam/security-credencials
(5) "ls" command to list existing buckets
AWS S3 Buckets
(6) "sync" command to copy confidential data from buckets

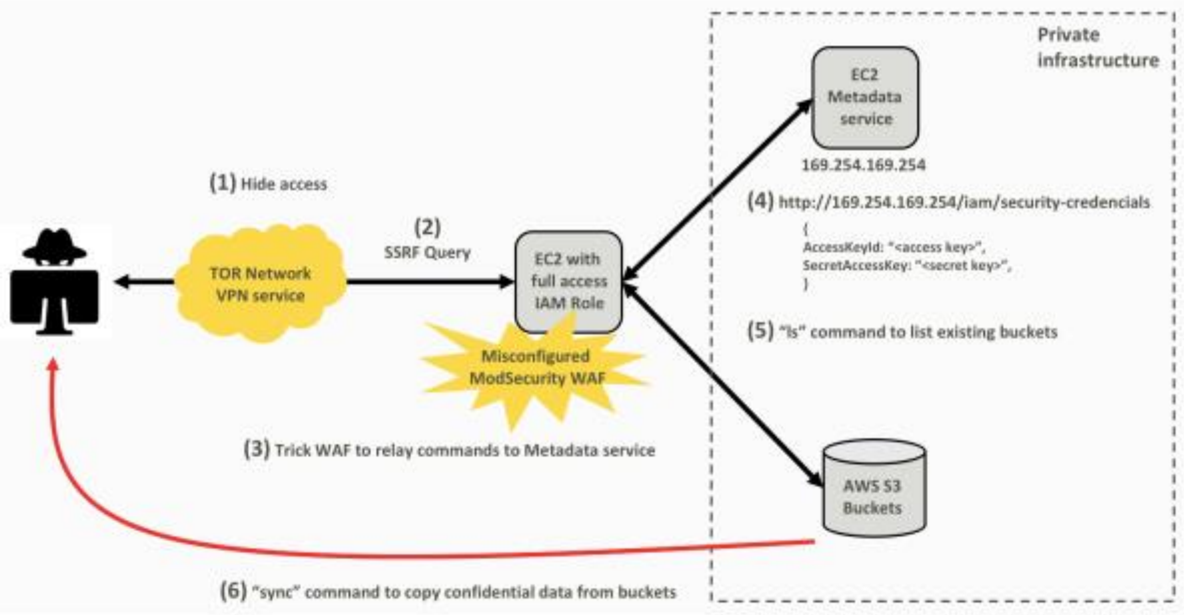
```
{
AccessKeyId: "<access key>",
SecretAccessKey: "<secret key>",
}
```

Figure 2: Diagram of the attack: Capital One case study

https://web.mit.edu/smadnick/www/wp/2020-07.pdf

CAPITAL ONE CASE STUDY

- The WAF misconfiguration allowed the intruder to trick the firewall into relaying commands to a default back-end resource on the AWS platform, known as the metadata service (accessed through the URL http://169.254.169.254);


Private infrastructure
EC2 Metadata service
169.254.169.254
(1) Hide access
TOR Network VPN service
(2) SSRF Query
EC2 with full access IAM Role
Misconfigured ModSecurity WAF
(3) Trick WAF to relay commands to Metadata service
(4) http://169.254.169.254/iam/security-credencials
(5) "ls" command to list existing buckets
AWS S3 Buckets
(6) "sync" command to copy confidential data from buckets

```
{
AccessKeyId: "<access key>",
SecretAccessKey: "<secret key>",
}
```

Figure 2: Diagram of the attack: Capital One case study

https://web.mit.edu/smadnick/www/wp/2020-07.pdf

CAPITAL ONE CASE STUDY

- By combining the SSRF attack and the WAF misconfiguration with the access to the metadata service containing temporary credentials for such environment, the attacker was able to trick the server into requesting the access credentials. The attacker then used the URL “http://169.254.169.254/iam/securitycredentials”, to obtain the AccessKeyId and SecretAccessKey from a role described in the FBI indictment as “*****-WAF-Role” (name was partially redacted). The resulting temporary credentials allowed the criminal to run commands in AWS environment via API, CLI or SDK;

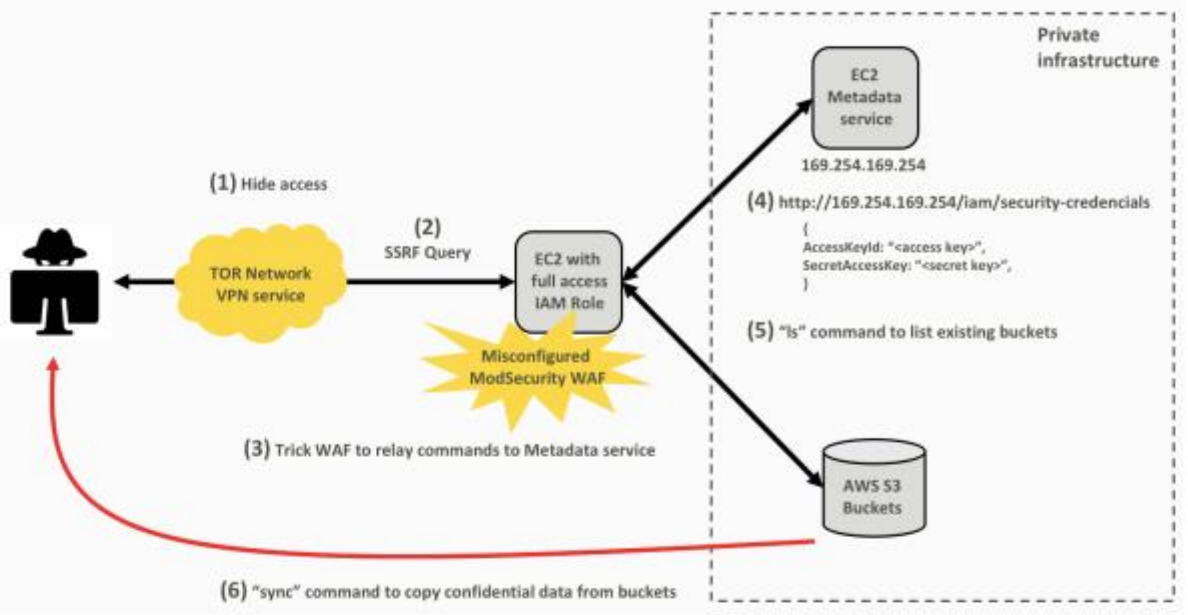

Private infrastructure
EC2 Metadata service
169.254.169.254
(1) Hide access
(4) http://169.254.169.254/iam/security-credencials
{
AccessKeyId: "<access key>",
SecretAccessKey: "<secret key>",
}
(2) SSRF Query
TOR Network VPN service
EC2 with full access IAM Role
(5) "ls" command to list existing buckets
Misconfigured ModSecurity WAF
(3) Trick WAF to relay commands to Metadata service
AWS S3 Buckets
(6) "sync" command to copy confidential data from buckets

Figure 2: Diagram of the attack: Capital One case study

https://web.mit.edu/smadnick/www/wp/2020-07.pdf

CAPITAL ONE CASE STUDY

- By using the credentials, the attacker ran the "ls” command multiple times, which returned a complete list of all AWS S3 Buckets of the compromised Capital One account ("$ aws s3 ls");
- Lastly, the attacker used the AWS sync command to copy nearly 30 GB of Capital One credit application data from these buckets to the local machine of the attacker ("$ aws s3 sync s3://bucketone."). This command gave the attacker access to more than 700 buckets, according to the FBI report.

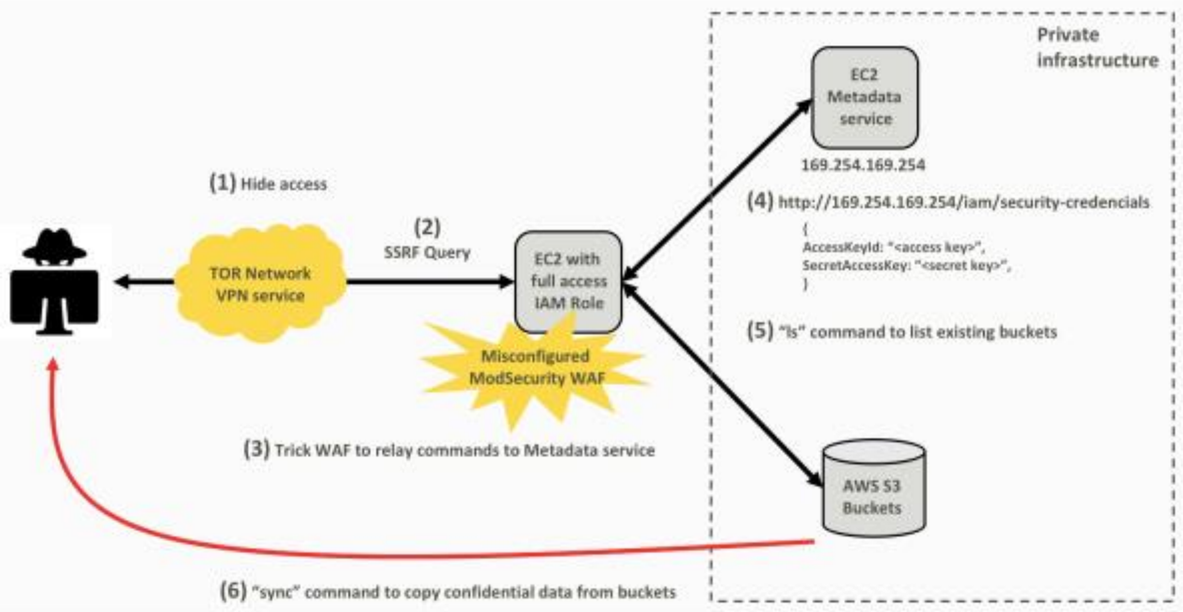

Private infrastructure
EC2 Metadata service
169.254.169.254
(1) Hide access
(4) http://169.254.169.254/iam/security-credencials
{
AccessKeyId: "<access key>",
SecretAccessKey: "<secret key>",
}
(2) SSRF Query
TOR Network VPN service
EC2 with full access IAM Role
(5) "ls" command to list existing buckets
Misconfigured ModSecurity WAF
(3) Trick WAF to relay commands to Metadata service
AWS S3 Buckets
(6) "sync" command to copy confidential data from buckets

Figure 2: Diagram of the attack: Capital One case study

https://web.mit.edu/smadnick/www/wp/2020-07.pdf

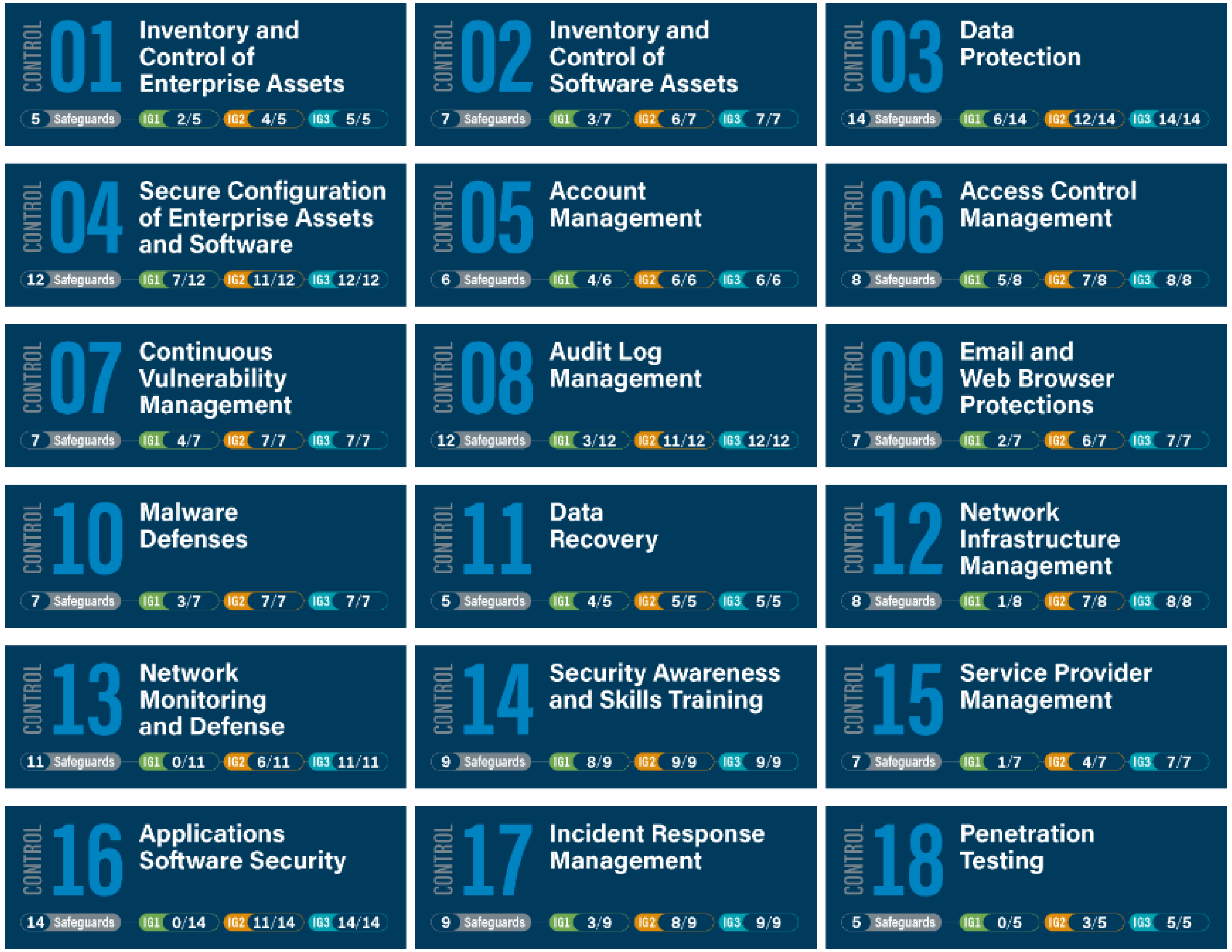
WHAT SENIOR LEADERSHIP CAN DO

SET THE TONE

- What are the current security initiatives and priorities
  - Compliance vs. Security as the end goal
- When was the IRP last reviewed and tested?
  - You do have one, right?
- What attention does the “lessons learned” phase receive?
- Identify your resources
  - In-house skills
  - Legal/Insurance benefits & responsibilities
  - Trustworthy partners

VALIDATE FUNDAMENTAL CONTROLS

- Follow a framework, don’t play Whack-a-Mole, specifically:
- Secure Authentication
  - Multi-Factor Authentication (MFA)
  - Brute-Force/Password-Spray Mitigations
- Endpoint Detection and Response (EDR)
- Logging, alerting, and detection abilities



CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7

CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12

CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6

CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8

CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7

CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12

CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7

CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7

CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5

CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8

CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11

CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9

CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7

CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14

CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9

CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

QUESTIONS

Sean D. Goodwin, GSE

CCSP, CISA, CISSP, GCCC, GCIA, GCIH, GCUX, GCPM, GCWN, GDAT, GSEC, PCIP, QSA

Senior Manager – DenSecure

✉ sdgoodwin@wolfandco.com

☎ 617.261.8139

Back to Home ⟶

ABOUT WOLF & COMPANY, P.C.

1911 WOLF & CO. ESTABLISHED

300+ PROFESSIONALS

3 OFFICES IN:

- ✓ Boston, MA
- ✓ Springfield, MA
- ✓ Livingston, NJ

SERVICES OFFERED IN:

- ✓ Audit
- ✓ Tax
- ✓ Risk Management

ABOUT WOLF & COMPANY, P.C.

111

YEARS IN BUSINESS

- Established in 1911
- Built on quality and integrity
- Succession strategy to remain independent allows us to be with you throughout your business lifecycle

300+

EXPERIENCED, HIGHLY TRAINED PROFESSIONALS

- Lower-than-industry-average staff turnover means a consistent team structure year after year
- Niche team dedicated to your industry

RESOURCES TO LEARN MORE

- Cultures & Values
- Inclusion & Diversity
- Our History
- Social Responsibility
- Thought Leadership
- Wolf Global

Wolf & Company ranked

#2 BEST LARGE FIRM TO WORK FOR

nationwide

accountingTODAY

WOLF & COMPANY, P.C.

den secure by wolf & company, p.c.

ABOUT WOLF & COMPANY, P.C.

SERVICES WE OFFER

We combine industry expertise with service specialization to provide your organization with insight, opportunities, and solutions allowing you to address your unique business needs.

ADVISORY

- Business Continuity Planning
- Cybersecurity
- Enterprise Risk Management
- Environment, Social & Governance
- Internal Audit
- IT Audit
- Model Risk Management
- Outsourced Accounting Solutions
- Penetration Testing
- Regulatory Compliance
- Strategic Planning

ASSURANCE

- Employee Benefit Plan Audits
- Financial Statements Audits
- HITRUST
- PCI DSS
- SOC Reporting

TAX

- Business Tax
- Federal
- International
- State & Local
- Private Client Group

vSUITE

- Virtual Consulting Services
  - Business Continuity Planning (BCP)
  - Virtual Chief Information Security Officer (vCISO)
  - Virtual Chief Privacy Officer (vCPO)
  - Virtual Chief Risk Officer (vCRO)
  - Virtual Vendor Management

WOLFPAC

- Integrated risk management SaaS suite

WOLF & COMPANY, P.C.

den secure by wolf & company, p.c.

WOLF ACCOLADES

Wolf is pleased to have received recognition from a variety of sources for our efforts at providing responsive client service and development of our professionals. Examples of this recognition include:

INSIDE Public Accounting

TOP 100
Accounting Firms

accountingTODAY

TOP 100
Accounting Firms

#2 BEST LARGE FIRM to
Work For Nationwide

TOP FIRMS:
New England

BOSTON BUSINESS JOURNAL

- ✓ Area's Best Places to Work
- ✓ Area's Most Admired Companies
- ✓ Area's Fastest Growing Private Companies
- ✓ Area's Largest I.T. Consulting Firms

Forbes

America's Best
Tax and Accounting
Firms of 2022, 2021

WOLF & COMPANY, P.C. den secure by wolf & company, p.c.

ABOUT DENSECURE

Wolf & Company's IT Assurance & Advisory team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.

DenSecure's core services include:

- Advanced Security Assessment
- Application Penetration Testing
- Network Penetration Testing
- Social Engineering
- Threat Emulation