Red Team Exercise Overview

Threat intelligence and open source intelligence

What is my attack surface and threats?

- Vulnerable external infrastructure and applications
- Industry and client specific threats
- Sensitive information and data Leaks
- Employees Information
- Remote access services
- Physical locations

Sources

Initial foothold and advanced implant execution

How can an attacker use those threats to access my environment?

Identify attack vectors and realistic scenarios:

Targeted phishing

- Delivery of a bespoke implant
- Credential harvesting and MFA tokens

External perimeter vulnerabilities

- Access to on-premises servers
- Access to cloud infrastructure

Physical social engineering

- Badge cloning
- Tailgating
- In person social engineering
- Physical wiretap installation

Internal network access and establishing a command and control channel

Lateral movement and privilege escalation

What can an attacker do before we detect and contain the compromise?

Identify and bypass security controls

Establish persistence

Stealth lateral movement and privilege escalation

Achieve agreed objectives

- Cloud tenant compromise
- Access inbox of c-suite executive
- Exfiltration of large amounts of data
- Locate sensitive intellectual property

Reporting

What are the security gaps in prevention, detection, and response that resulted in the breach?

Clean up and debrief

Detailed report

- Detailed attack path, findings and recommendations
- Timelines of TTP activities

Workshop with the Blue Team

Contact us:

IE/International
Call: +353 1 210 1711
Email: digitaltrust.consulting.ie@bsigroup.com
Visit: bsigroup.com/digital-trust-ie

UK
+44 345 222 1711
digitaltrust.consulting@bsigroup.com
bsigroup.com/digital-trust-uk

US
+1 800 862 4977
digitaltrust.consulting.us@bsigroup.com
bsigroup.com/digital-trust-us