GOAL-ORIENTATED PENETRATION TESTS

SERVICE DESCRIPTION

Significantly more sophisticated than a standard Penetration Test, Goal Orientated Penetration Testing, also known as Red Team Assessments, assessments simulate real-world, covert, multi-phase attacks as they would be performed by real and persistent criminals.

These assessments are based around certain "goals" agreed up front. These goals are designed around possible critical failures of your most important business functions. For example, a goal could be to gain access to a material amount of money, or secret business information, or large amounts of data under regulatory scrutiny. These goals are important for replicating a real-world attack, as real criminals have such motives. The methods used to attain these goals are as unrestricted as feasible, allowing likely attack scenarios to be played out. The results of the assessment are vital to escalate cyber risk to a business level by demonstrating the business risk of such an attack. Additionally, knowing the full attack chain enables intelligent defences to be placed along it, rather than focusing on initial vectors only.

Modern adversaries can take several forms. SensePost studies the behaviour of attack groups to impersonate the style and expertise of attack an organisation may face. Broadly, they fall into the following categories.

Opportunists are looking for easy opportunities and “low hanging fruit.” They either do not possess the skill for more advanced attacks, or do not have a need for utilising such skill. Examples here are website defacements, or petty theft.

Insiders are the traditional “white collar criminals” who know the business systems well enough to bypass their rules. Examples here are “ghost employees” or supplier payment fraud.

Hackers are skilled at technically manipulating systems in ways no one intended. Examples here are banking trojan authors, custom ransomware or some organised criminals.

Advanced attackers are typically cross-functional teams of both skilled technical hackers as well as highly knowledgeable business users. These range from organised crime to nation states.

KEY BENEFITS & DELIVERABLES

- **Ongoing, real-world attack:** Our Ethical hackers attack an organisation’s users, web estate, public-facing applications and perimeter exactly as determined and directed attackers would
- **Post-exploitation manoeuvring:** Once we have gained access to the internal network, we will establish a persistent presence and explore the network’s assets for further compromise
- **Exfiltration:** We will find the agreed trophies -most critical assets- and seek to compromise the organisation’s access to them or remove copied data

KEY SERVICE COMPONENTS

Armed with appropriate modus operandi for the range of adversaries your organisation is likely to face, we will take one or many of the following approaches.

- Reconnaissance involves hunting for public information to be used to choose targets, or appear as a legitimate business entity. These activities include gathering technical information (such as e-mail addresses, or Wi-Fi network names) to business relevant information (such as job roles or business functions).
- The Perimeter Breach serves as the initial entry vector onto the network. This is most often via malware delivered through phishing exercises, exploiting vulnerabilities in Internet-facing systems, or via physical co-location attacks against Wi-Fi or unprotected network ports.
- Lateral Movement is the stage of the attack where further reconnaissance of internal user behavior is conducted and relevant privileged access is obtained. A beachhead will be established, and redundant and persistent channels are covertly established to maintain access. In some cases, this will include compromise of the Microsoft Active Directory domain, but frequently, critical business systems can be accessed via other means.
- Action on Technical Objectives once objective-appropriate target systems and users within the relevant business unit have been identified, this phase will include the exploitation of the specific target systems and infrastructure
- Action on Business Objectives i s where the target business systems and processes are exploited to achieve the overall objectives. Examples include learning entity-specific SWIFT codes in order to conduct transactions, or creating false suppliers and payments in a manner that passes business-specific rules.

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com