SAPPHIRE™

Breach Attach Simulation

Service Definition

Classification: Public

Contents

Proprietary Notice

Overview

Breach Attack Simulation (BAS) assessments compliment penetration testing and red and purple teaming exercises, by validating your organisations security posture through specific simulated advanced attacks that are known to be carried out by significant threat actors. In simple terms, simulating the attack paths and techniques that are likely to be used by malicious actors.

Service features:

- Understand your security vulnerabilities by automating testing of threat vectors
- Attempt lateral movement and data exfiltration
- Scale up your cyber defences by running scenarios and emulations
- Strengthen defences by emulating real attacks and tuning SIEMs/SOCs
- Full Purple team testing, allowing real time testing
- Customised methods leveraging real-world Tactics, Techniques and Procedures (TTPs)
- Advance Persistent Threat (APT) approach and analysis
- The attack simulation follows the MITRE ATT&CK Framework
- Emulate techniques used by ransomware threat actors for data exfiltration
- Assess vulnerability to deliver custom payloads and scripts.

Service benefits:

- Enables organisations to assess the effectiveness of their cybersecurity defences
- Simulations help fine-tune incident response plans and assess SOC efficacy
- Completing and understanding breaches allows prioritisation of security investments effectively
- Prioritise remediation efforts based on the risk and threat level
- Assess maturity of detection and response capabilities in safe fire-drill
- Assessment and simulations provide advanced planning to prepare your responses

Functional and Non-Functional Detail

The service is a scenario based external and/or internal simulated assessment. We start from an 'assumed breach' position from an agreed starting point. This can be an external host, endpoint machine or connected to the internal network. This enables us to focus the simulation on post-compromise activity detection, prevention and response capabilities from your internal teams, external providers if applicable and technology in place.

The assessment is based on a grey-box scenario, and we will search for defects due to improper structure or use of insecure applications or services. The attack simulation will follow the MITRE

ATT&CK Framework and leverage threat intelligence to emulate the attacker tradecraft (tools, techniques and procedures) most likely to target your organisation.

Sapphire will attempt to gain a foothold into your network to see how easily we can use common tools, tactics and processes to laterally move within your environment, escalate privilege and ultimately deliver a payload via a benign mechanism. The results enable you to identify what additional controls you need to consider mitigating the risks of a threat actor gaining access to your environment. The goal is data exfiltration to mirror a ransomware-based attack. First, we will attempt to attack the network with no credentials and see if data can be exfiltrated. Then with credentials (found or provided) to see if it is possible to traverse the network.

A Breach Attack Simulation (BAS) focuses on 'assumed breach' due to the likelihood of a social engineering attack (such as phishing) to be successful in convincing an end user to click a link and have some form of malware installed on the host. A truly resilient organisation must keep this 'blast-radius' as small as possible and prevent lateral movement and broad scale malware/ransomware spread. A BAS quantifiably measures your susceptibility to this lateral movement and identifies weak points to be improved to increase your overall security resilience.

The breach attack simulation will help you fine-tune your incident response plans. By completing and understanding breaches it allows prioritisation of your security investments effectively by assessing the effectiveness of your cybersecurity defences. Additionally, it can be performed either in collaboration or blind of the Security Monitoring function to assess effectiveness of your detection and response capabilities in a safe and secure but effective manner.

A BAS from Sapphire answers the question "What is my organisations response if a user did click on a phishing link and a piece of malware breached my initial defences? Can I detect and mitigate it and keep the blast radius as small as possible?".

Sapphire's Certifications and Associations