Validating Security Controls of Microsoft Defender for Endpoint with SafeBreach

Microsoft + SafeBreach

Joint Solution Brief

To make the business case for acquiring a new security tool, it's critical to run realistic proofs of concept (PoCs) to instantly test and validate the technical efficacy of endpoint security capabilities against leading threats.

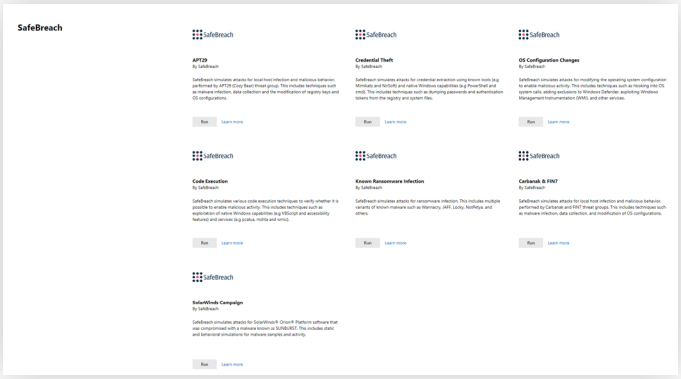
It can be logistically and technically challenging and time consuming for security teams to run PoCs that represent real-world scenarios that accurately mimic their organization's production security stance as precisely as possible.

SafeBreach has partnered with Microsoft to bring a select set of advanced attack simulation methods, from over 20,000 breach and attack methods in the SafeBreach Hacker's Playbook to the Microsoft Defender for Endpoint Evaluation Lab. The addition of these simulation methods will improve the quality of evaluations and simplify determinations of the efficacy of Microsoft Defender for Endpoint product against known attacks in the wild.

The Lab Reports Summarize the Results of the Simulations Conducted on the Machines

At a glance, you'll quickly be able to see:

- Incidents that were triggered
- Generated alerts
- Assessments on exposure level
- Threat categories observed
- Detection sources
- Automated investigations



SafeBreach Advanced Attack Simulations in Microsoft Defender for Endpoint Evaluation Lab.

How Microsoft Defender for Endpoint Evaluation Lab Works

Microsoft created the Microsoft Defender for Endpoint Evaluation Lab to simplify and improve PoCs. The lab is designed to eliminate the complexities of creating the right machine and environment configurations to accurately evaluate the capabilities of the Microsoft Defender for Endpoint platform.

To improve the capabilities of the lab, SafeBreach is automatically deployed on the Carbanak & FIN7, SolarWinds Campaign Software Compromise, APT29, Credential Theft, OS Configuration Changes, Code Execution, and Known Ransomware Infection scenarios, which include a limited set of attacks methods from the SafeBreach Hacker's Playbook.

The built-in attack simulations that can clearly demonstrate the effectiveness of various Microsoft Defender for Endpoint configurations, allowing testers to observe prevention, detection, threat hunting and remediation features in action.

Testers will be able to choose scenarios that include SafeBreach breach and attack simulations:

Carbanak & FIN7 Scenario

This includes techniques such as malware infection, data collection, modification of OS configurations, and communication with C&C servers. The attack types simulated by SafeBreach include:

- Write Malware to Disk—Verify whether the malware can be written to disk.
- System Information Dump—Verify whether system data, credentials and other information can be collected.
- OS Configuration Change—Verify whether the operating system configuration can be changed to allow malicious activity.
- Code Execution—Verify whether code execution is possible to enable malicious activity.

SafeBreach simulates attacks for local host infection and malicious behavior, performed by Carbanak and FIN7 threat groups.

SolarWinds Campaign Scenario

This includes static and behavioral simulations for malware samples and activity. The attack types simulated by SafeBreach include:

- Write Malware to Disk—Verify whether the malware can be written to disk and executed.
- System Information Dump—Verify whether system data, credentials and other information can be collected.
- OS Configuration Change—Verify whether is it possible to start or modify services.

SafeBreach simulates attacks for SolarWinds Orion® Platform software that was compromised with a malware known as SUNBURST.

APT29 Scenario

This includes techniques such as malware infection, credential theft, data collection and the modification of registry keys and OS configurations. The attack types simulated by SafeBreach include:

- Write Malware to Disk—Verify whether the malware can be written to disk.
- Code Execution—Verify whether code execution is possible to enable malicious activity.
- OS Configuration Change—Verify whether the operating system configuration can be changed to enable malicious activity.
- System Information Dump—Verify whether system information or credentials can be dumped by a malicious entity.

SafeBreach simulates attacks for localhost infection and malicious behavior, performed by the APT29 (Cozy Bear) threat group.

Credential Theft Scenario

This includes techniques such as dumping passwords and authentication tokens from the registry and system files. The attacks simulated by SafeBreach include:

- Collect login information using the Mimikatz tool.
- Write NirSoft password extraction tools to disk.
- Extract credentials using reg.exe commands.
- Extract NTLM hashes using Invoke-Kerberoast PowerShell script.
- Extract security packages using Get-SecurityPackages PowerShell script.
- Extract credentials from the group policy using Get-GPPPassword PowerShell script.
- Extract password policy using the 'net accounts' command.

SafeBreach simulates attacks for credential extraction using known tools and native Windows capabilities.

OS Configuration Changes Scenario

This includes techniques such as hooking into OS system calls, adding exclusions to Windows Defender, exploiting Windows Management Instrumentation (WMI), and other services. The attacks simulated by SafeBreach:

- Hooking into GetSystemTime function using mavinject.exe with a custom DLL.
- Add a file exclusion to Windows Defender using PowerShell.
- Write data into an Alternate Data Stream.
- Add an executable path to a registry associated with accessibility features (Image File Execution Options).
- Subscribe to a Windows Management Instrumentation event.

SafeBreach simulates attacks for modifying the operating system configuration to enable malicious activity.

Code Execution Scenario

This includes techniques such as exploitation of native Windows capabilities and services. The specific attacks simulated by SafeBreach include:

- Run an executable indirectly using pcalua (Program Compatibility Assistant).
- Execute a VBScript using XSL with wmic.exe (command line foe WMI).
- Run an executable using mshta.exe (a utility that executes Microsoft HTML Applications).
- Run the rundll32.exe masquerading as a different process.

SafeBreach simulates various code execution techniques to verify whether it is possible to enable malicious activity.

Known Ransomeware Infection Scenario

This includes multiple variants of known malware such as Wannacry, JAFF, Locky, NotPetya, and others.
Ransomware infections simulated by SafeBreach:

- WannaCry 2.0 ransomware
- Trojan-Ransom.Win32.Locky bl
- JAFF ransomware
- JAFF ransomware dropper
- NotPetya
- Ryuk ransomware
- Ryuk ransomware dropper
- Nemty ransomware
- Ransom.BitPaymer

SafeBreach simulates attacks for ransomware infection.

Summary

The joint integration of SafeBreach, the market-leading security control validation solution, with the Microsoft Defender Evaluation Lab includes a select group of highly relevant attacks against a fully configured Microsoft Defender for Endpoint instance. The PoC capabilities now deliver:

- Free virtual environments that are simple to configure to match most common IT environments and system topologies.
- A risk-free way to evaluate and report on the performance of Microsoft Defender for Endpoint against advanced attacks.
- Push-button deployment with no code or config changes required to run the tightly integrated advanced attack scenarios.

Incorporating these capabilities and SafeBreach simulated attacks delivers a superior user experience for creating full-featured PoCs in Microsoft Defender for Endpoint Evaluation Lab.

The integration enables faster, easier, and more accurate evaluation of the Microsoft Defender for Endpoint platform's efficacy in a wide range of techniques and attack scenarios.

SafeBreach

111 W. Evelyn Avenue Suite 117
Sunnyvale, CA 94086 408-743-5279
safebreach.com

About SafeBreach

SafeBreach is the world's most widely used continuous security validation platform for enterprise companies. The company's patented platform empowers CISOs and their teams to validate security controls, maximize their effectiveness, and drive down risk. SafeBreach provides a "hacker's view" of an enterprise's security posture by continuously validating security controls and presenting findings in customized dashboards to enable stakeholders to cleanly focus on the biggest risks to the organization. SafeBreach automatically and safely executes thousands of attack methods to validate network, endpoint, cloud, container and email security controls against its Hacker's Playbook™, the world's largest collection of attack data broken down by methods, tactics and threat actors. Data from SafeBreach validations can improve SOC team responses and inform management teams to make smarter decisions to better manage risk and invest resources. SafeBreach is privately held and is headquartered in Sunnyvale, California with an office in Tel Aviv, Israel.

For more information, visit www.safebreach.com

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a market leading, unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response. The solution includes risk-based Threat & Vulnerability Management to discover, prioritize and automate mitigation of vulnerabilities and security misconfiguration. It provides security admins tools to surgically reduce the attack surface without limiting user's productivity. Its behavioral based and cloud-powered threat & malware protection prevents sophisticated and never-seen-before threats from impacting devices. Deep optics into the operating system, including memory and kernel, help to detect 0-days, advanced attacks, and data breaches. Microsoft Defender for Endpoint accelerates remediation by automatically investigating alerts and remediating threats—allowing security teams to go from alert to remediation in minutes—at scale. Finally, Microsoft Defender for Endpoint comes with a managed hunting service, which provides critical threat monitoring, expert level analysis, and support for Security Operations Centers.

Visit www.aka.ms/mdatp to learn more or start a free trial.