Test the Efficacy of Your Security Controls with Cortex XDR™ and SafeBreach

Cortex® XDR™
+
SafeBreach

Joint Solution Brief

CISOs and security teams seek to maximize the impact of their security controls and proactively manage their risk and security posture. The biggest reason security controls fail today is that they are improperly configured or have drifted over time. SafeBreach automatically executes tens of thousands of attacks, safely and continuously, from its extensive and growing Hacker's Playbook™ to validate the effectiveness of an organization's security controls. The attacks are presented in several perspectives for fast, full comprehension of the attack sequence and focus on the relevant security gaps. Additionally, outcome-driven results are presented in the form of SafeBreach Insights to holistically remediate security controls for highly effective hardening of the enterprise defenses.

The integration of SafeBreach with Cortex XDR empowers security teams to maximize the efficiency and effectiveness of the security controls by analyzing how they perform against known attacks, identifying any gaps, and enabling close remediation of those gaps. Continuous validation of security controls provides a baseline and aides security teams to manage risk over time. The solution even goes one step further by allowing security teams to score, visualize and operationalize MITRE ATT&CK® reporting.

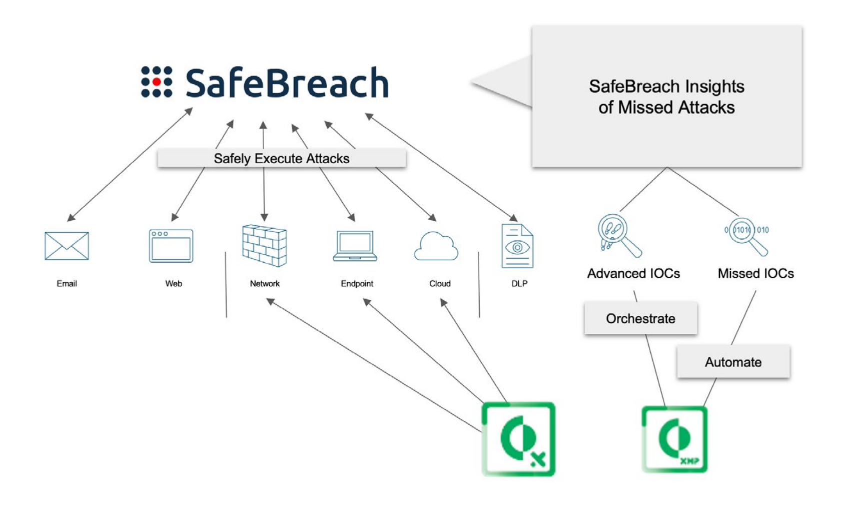
Challenge

In the quest to defend the enterprise amid the ever-changing threat landscape, security teams have implemented numerous tools and processes to prevent devastating attacks that could jeopardize the business. No matter how sophisticated the security stack, there is a clear lack of visibility into the performance of all security controls. Teams struggle to understand if the many controls deployed are configured correctly, which controls will prevent, detect, or completely miss an attack, and how the controls will work together against threat groups that pose a risk to the business.

Use Case 1
Closed-loop remediation of indicators of compromise (IOCs)

Solution

SafeBreach executes attacks from known threat groups, safely and continuously, to bring visibility into which controls prevented an attack and which attacks sailed past security controls. The dedicated SafeBreach Labs team monitors the threat landscape for the changes in IOCs to ensure the SafeBreach Hacker's Playbook is safely executing attacks with the latest IOCs. The integration with Cortex XDR tests the attacks against your Cortex XDR endpoint protection controls to validate attacks that Cortex XDR blocked, and identify which IOCs were not blocked. In the case of any attack being missed, SafeBreach, Cortex XDR and Cortex XSOAR work in combination to ensure that indicators of compromise (IOCs) that were not blocked will be automatically remediated. The tight integration also reruns the attacks to ensure closed-loop remediation of security gaps and misconfigurations.

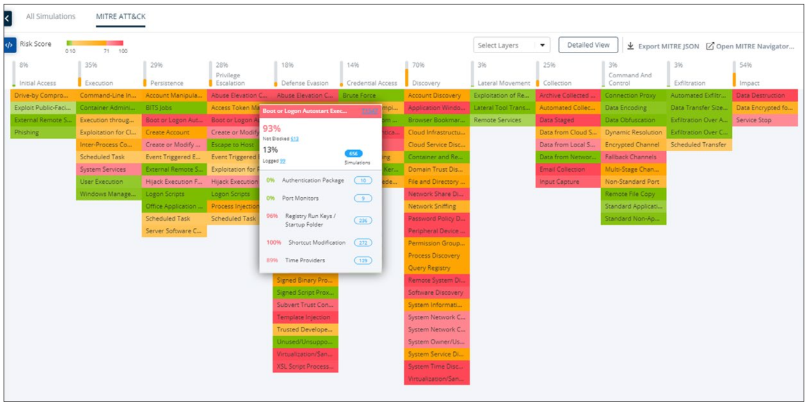


SafeBreach, Cortex XDR, and Cortex XSOAR help automate remediation of behavioral and non-behavioral IOCs

Use Case 2
Operationalize MITRE ATT&CK® Reporting & Remediation

Solution

SafeBreach Hacker's Playbook contains tens of thousands of breach and attack methods that continuously tests your email, web, network, endpoint, data leak, cloud, and container controls. The integration of Cortex XDR with SafeBreach enables customers to identify which attacks were blocked, detected, or missed on endpoint controls. The insights from validating controls are heat mapped to the MITRE ATT&CK framework enabling security teams to focus their efforts on the highest priority gaps. SafeBreach also prioritizes the remediation insights enabling the most efficient responses to improve your risk posture. The remediation insights can be further automated with the Cortex XOSAR integration with SafeBreach where Cortex XSOAR will ingest the missed IOCs and build playbooks to automatically update endpoint and network controls to reduce dwell time of attacks that have been proven to breach your environment.



8% Initial Access	35% Execution	29% Persistence	28% Privilege Escalation	18% Defense Evasion	14% Credential Access	70% Discovery	3% Lateral Movement	25% Collection	3% Command And Control	3% Exfiltration	54% Impact
Drive-by Compro...	Command-Line In...	Account Manipula...	Abuse Elevation C...	Abuse Elevation C...	Brute Force	Account Discovery	Exploitation of Re...	Archive Collected ...	Connection Proxy	Automated Exfiltr...	Data Destruction
Exploit Public-Faci...	Container Admini...	BITS Jobs	Access Token Ma	[illegible]	mpi...	Application Windo...	Lateral Tool Trans...	Automated Collec...	Data Encoding	Data Transfer Size...	Data Encrypted fo...
External Remote S...	Execution throug...	Boot or Logon Aut...	Boot or Logon A	[illegible]	om ...	Browser Bookmar...	Remote Services	Data Staged	Data Obfuscation	Exfiltration Over A...	Service Stop
Phishing	Exploitation for Cl...	Create Account	Create or Modify	[illegible]	tica...	Cloud Infrastructu...		Data from Cloud S...	Dynamic Resolution	Exfiltration Over C...	
	Inter-Process Co...	Create or Modify ...	Escape to Host	[illegible]	[illegible]	Cloud Service Disc...		Data from Local S...	Encrypted Channel	Scheduled Transfer	
	Scheduled Task	Event Triggered E...	Event Triggered	[illegible]	ng	Container and Re...		Data from Networ...	Fallback Channels		
	System Services	External Remote S...	Exploitation for	[illegible]	Ker...	Domain Trust Dis...		Email Collection	Multi-Stage Chan...		
	User Execution	Hijack Execution F...	Hijack Execution	[illegible]	ede...	File and Directory ...		Input Capture	Non-Standard Port		
	Windows Manage...	Logon Scripts	Logon Scripts	[illegible]		Network Share Di...			Remote File Copy		
		Office Application ...	Process Injection	[illegible]		Network Sniffing			Standard Applicati...		
		Scheduled Task	Scheduled Task	[illegible]		Password Policy D...			Standard Non-Ap...		
		Server Software C...		[illegible]		Peripheral Device ...					
				[illegible]		Permission Group...					
				[illegible]		Process Discovery					
				[illegible]		Query Registry					
				Signed Binary Pro...		Remote System Di...					
				Signed Script Prox...		Software Discovery					
				Subvert Trust Con...		System Informati...					
				Template Injection		System Network C...					
				Trusted Develope...		System Network C...					
				Unused/Unsuppo...		System Owner/Us...					
				Virtualization/San...		System Service Di...					
				XSL Script Process...		System Time Disc...					
						Virtualization/San...					

Boot or Logon Autostart Exec... T1547

93%
Not Blocked 613

13%
Logged 99

656 Simulations

0%	Authentication Package	10
0%	Port Monitors	9
96%	Registry Run Keys / Startup Folder	236
100%	Shortcut Modification	272
89%	Time Providers	129

MITRE ATT&CK board in the SafeBreach Platform

Integration Benefits

Together, SafeBreach and Palo Alto Networks Cortex XDR:

Provide unparalleled levels of visibility into endpoint security control performance

Continuously execute attacks to baseline, monitor and detect any deviation in coverage

Optimize endpoint configurations with SafeBreach Insight remediations

Automate remediation of behavioral and non-behavioral indicators of compromise with Cortex XSOAR

SafeBreach

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

About SafeBreach

SafeBreach safely and continuously executes thousands of attack behaviors covering the full kill chain to provide a hacker's view into the enterprise security controls and provides a prioritized remediation plan to improve the organization's risk profile. SafeBreach is privately held and is headquartered in Sunnyvale, California with an office in Tel Aviv, Israel.

For more information, visit safebreach.com

About Cortex® XDR™

Cortex® XDR™ is the world's first extended detection and response platform that integrates endpoint, network, and cloud data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency.

For more information,
visit paloaltonetworks.com/cortex/cortex-xdr