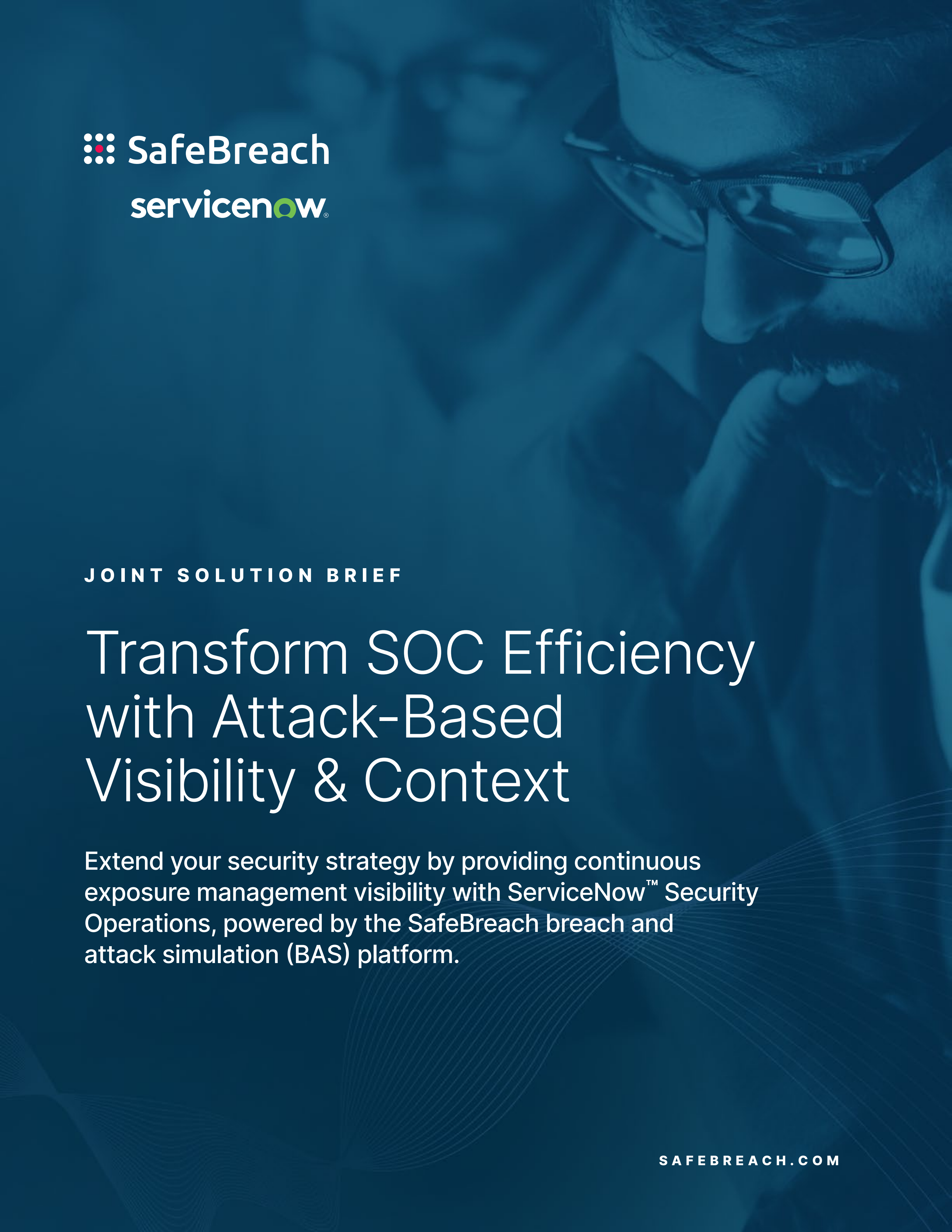


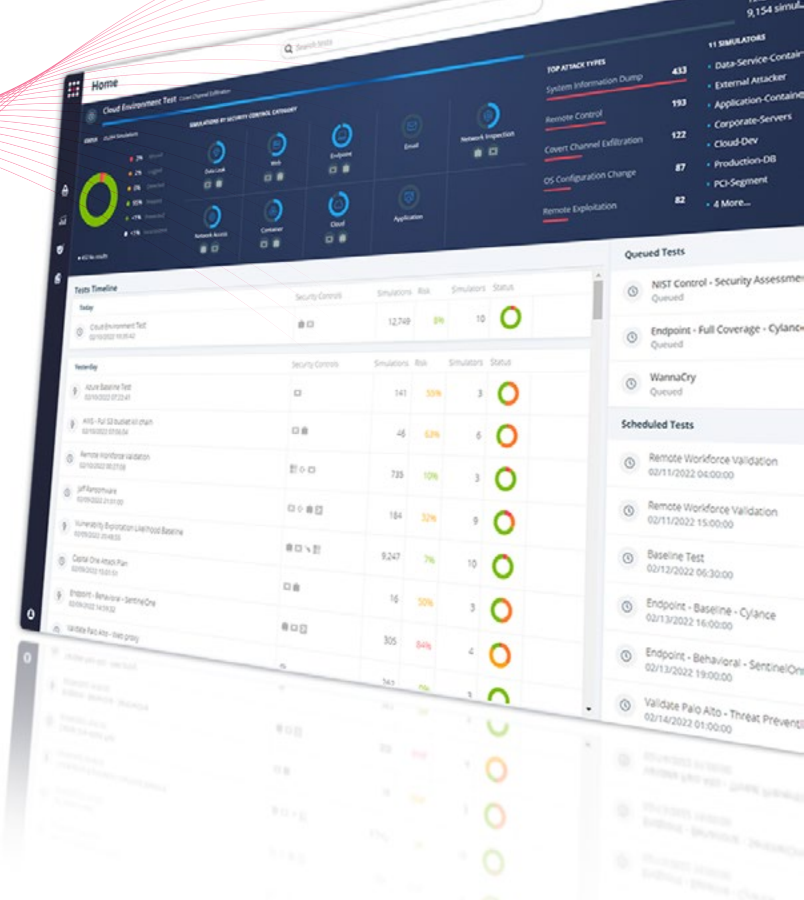
SafeBreach

servicenow

JOINT SOLUTION BRIEF

Transform SOC Efficiency with Attack-Based Visibility & Context

Extend your security strategy by providing continuous exposure management visibility with ServiceNow™ Security Operations, powered by the SafeBreach breach and attack simulation (BAS) platform.



TOP ATTACK TYPES

System Information Dump	433
Remote Control	193
Covert Channel Exfiltration	122
OS Configuration Change	87
Remote Exploitation	82

11 SIMULATORS

- Data-Service-Contain
- External Attacker
- Application-Containe
- Corporate-Servers
- Cloud-Dev
- Production-DB
- PCI-Segment
- 4 More...

Tests Timeline

Today	Security Controls	Simulations	Risk	Simulators	Status
Cloud Environment Test		12,749	8%	10	

Yesterday	Security Controls	Simulations	Risk	Simulators	Status
Azure Baseline Test		141	55%	3	
AWS - Full S3 bucket kill chain		46	63%	6	
Remote Workforce Validation		735	10%	3	
Jeff Ransomware		184	32%	9	
Vulnerability Exploitation Likelihood Baseline		9,247	7%	10	
Capital One Attack Plan		16	50%	3	
Endpoint - Behavioral - SentinelOne		305	84%	4	
Validate Palo Alto - [illegible]					

Queued Tests

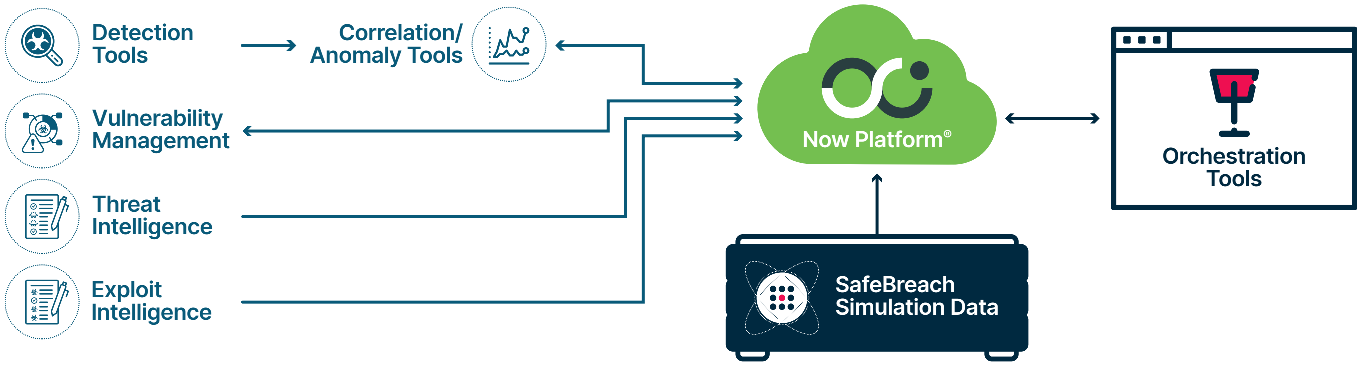
- NIST Control - Security Assessme
  Queued
- Endpoint - Full Coverage - Cylanc
  Queued
- WannaCry
  Queued

Scheduled Tests

- Remote Workforce Validation
  02/11/2022 04:00:00
- Remote Workforce Validation
  02/11/2022 15:00:00
- Baseline Test
  02/12/2022 06:30:00
- Endpoint - Baseline - Cylance
  02/13/2022 16:00:00
- Endpoint - Behavioral - SentinelOn
  02/13/2022 19:00:00
- Validate Palo Alto - Threat Prevent
  02/14/2022 01:00:00

Organizations spend millions of dollars on building their security stack in an ongoing effort to fully protect their enterprise. Yet, research has shown that even with a more sophisticated security stack and dynamic IT infrastructure, an organization's ability to contain an active threat has declined. Rather than helping, the increase in security tools has led understaffed teams to feel overwhelmed with alerts. One small control misconfiguration in any of the security tools can create a security gap that attackers can easily exploit, and a delay in threat response by potentially overwhelmed teams can have disastrous consequences for the enterprise.

The SafeBreach and ServiceNow joint solution helps enterprises transform their security posture by simplifying the identification of critical security gaps and risks before they can be exploited. SafeBreach's market-leading library of over 30,000 attacks enables ServiceNow customers to validate their security control infrastructure and processes with real-world attacks. The holistic view provided by this integration enhances security operations at all levels by adding continuous exposure management visibility, helping security practitioners identify, prioritize, and rapidly remediate high-impact security gaps, and providing executives with a continuous view of their risk, trends, and security posture.



How the Integration Works

SafeBreach simulates attacks to see whether they are blocked by an organization's existing security controls. With SafeBreach's automated analysis, relevant logs are correlated with simulation results. The ServiceNow integration allows SafeBreach to send the results of these simulations to the ServiceNow Now Platform® and create IT Service Management (ITSM) incidents and Security Incident Response (SIR) incidents based on the details of the simulation results or insights provided. Through the incident creation functionality, details from simulation results or insights will be populated directly into the incident, providing incident response teams with valuable context that can be leveraged to prioritize the remediation of critical security threats.

Benefits of the Integration – Together SafeBreach and ServiceNow Security Operations:

Gain unparalleled visibility into the organizational threat landscape to improve detection, response, and remediation speed and efficacy

Progressively transform security operations by developing a security baseline and continuously moving that baseline forward

Help identify gaps in threat detection and response by mapping exposures to business risk

Understand your risk against the latest threats and remediate any coverage gaps before they are exploited

USE CASE 1

Operationalize MITRE ATT&CK® to Protect Against Latest Threats

Challenge

Enterprise security operations center (SOC) teams often own and operate dozens of security tools that help analysts address the detection, prioritization, and remediation of critical events and threats within their environment. Misconfigured or drifted security controls may cause security gaps that can reduce SOC efficacy, causing challenges in maintaining a hardened security posture. Leveraging the MITRE ATT&CK framework can improve the consistency of security operations and enable faster detection of advanced threats. However, the MITRE ATT&CK framework can be notoriously difficult to operationalize in an enterprise environment with multiple security controls.

Solution

SafeBreach's real-world attack simulation results and insights are mapped to TTPs, threat groups, and tools based on the MITRE ATT&CK framework to bring visibility into the performance of security controls against advanced threats. By mapping these simulation findings to the MITRE ATT&CK framework, SafeBreach allows security analysts to quickly and continuously identify gaps in threat coverage. Security analysts can use the MITRE ATT&CK capability in Threat Intelligence, part of ServiceNow Security Incident Response (SIR), to automatically get a high-level overview of detected threats against the MITRE ATT&CK framework, as well as a thorough understanding of the effectiveness of their controls based on SafeBreach detection and mitigation scores. Combining SafeBreach's broad MITRE coverage with ServiceNow's ability to rapidly orchestrate remediation, security teams can optimize the breach detection, investigation, and remediation process, improving the overall defensive ability of the organization.

USE CASE 2

Optimize Performance of Deployed Security Controls

Challenge

To combat the threats posed by cyber attackers, security teams continually implement and tune a wide variety of security controls. However, given the dynamic threat landscape, security control configurations and policies can quickly become obsolete and need constant tweaking to ensure they are able to accurately detect, prevent, and mitigate advanced threats. Failure to do so can lead to attackers bypassing organizational defenses to inflict massive business losses. Security teams need a way to continuously discover security gaps, remediate, and validate fixes against rapidly changing threats.

Solution

SafeBreach validates organizational security controls by executing attacks from known threat groups, safely and continuously, to bring visibility into which network, endpoint, and cloud controls prevented an attack and which attacks sailed past them. The dedicated SafeBreach Labs team monitors the threat landscape 24/7 to ensure the SafeBreach Hacker's Playbook includes coverage for the latest indications of compromise (IOCs) and tactics, techniques, and procedures (TTPs). The ServiceNow integration allows SafeBreach to manually send the results of SafeBreach simulations (including metadata, attack parameters, classifications, and correlated security events) to ServiceNow. Once sent, ServiceNow automatically opens incidents according to the results received. The integration also fetches detailed SafeBreach insights (including risk impact, severity, affected targets, security control category, IOCs, and remediation data) for any attack that was missed by the security control. This level of detail allows analysts to gain valuable context needed to fix any misconfigurations before an attacker can exploit them.

About SafeBreach

Combining the mindset of a CISO and the toolset of a hacker, SafeBreach is the pioneer in breach and attack simulation (BAS) and is the most widely used continuous security validation platform. SafeBreach continuously executes attacks, correlates results to help visualize security gaps, and leverages contextual insights to highlight remediation efforts. With its Hacker's Playbook™, the industry's most extensive collection of attack data enabled by state-of-the-art threat intelligence research, SafeBreach empowers organizations to get proactive about security with a simple approach that replaces hope with data.

About ServiceNow

ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud-based platform and solutions help digitize and unify organizations so that they can find smarter, faster, better ways to make work flow. So employees and customers can be more connected, more innovative, and more agile. And we can all create the future we imagine. The world works with ServiceNow™. For more information, visit **www.servicenow.com**.