satius

Managed Breach and Attack Simulation

Shift to Cyber Resilience with proactive testing of your defenses through attacks simulation.

Gain Confidence in Your Security Controls

Only 22% of organizations are highly confident that their security controls work as they are supposed to. [1]

With a multi-layered security strategy, the defense-in-depth approach is a pillar in cybersecurity. But as cyberattacks continue infiltrating these layered defenses, this strategy is proving insufficient for protection. The core fallacy of this approach is the assumption that the defensive mechanisms will function consistently and effectively. To address this challenge, forward-thinking organizations are using Breach and Attack Simulation (BAS) to test, validate, and improve the effectiveness of their security controls. Beyond theoretical security, BAS provides organizations with real-world attack scenarios that accurately simulate known and emerging adversarial tactics, techniques, and procedures (TTPs).

Why Satius

Satius Security specializes in delivering cutting-edge Breach and Attack Simulation (BAS) services tailored to meet the unique cybersecurity needs of organizations. With a team of highly certified cybersecurity experts, Satius leverages its deep expertise to conduct controlled simulations of real-world cyber attacks. Their BAS services enable clients to proactively identify and mitigate weaknesses within their security defenses, incident response processes, and overall cyber resilience. Satius's knowledgeable professionals meticulously craft BAS campaigns, replicating the tactics, techniques, and procedures employed by sophisticated threat actors. Through these simulations, organizations can assess the effectiveness of their security controls, validate incident response capabilities, and foster a culture of continuous improvement in cybersecurity practices.

Benefits of BAS

By conducting continuous and simulations via BAS, organizations can proactively identify and address gaps in their security infrastructure before attackers can exploit them. Unlike traditional security assessments, BAS provides actionable, in-depth insights for an enhanced security posture, empowering security teams to fine-tune their security controls.

- Prove controls are working up to expectations
- Measure readiness to prevent and detect threats.
- Quickly respond to changes in the threat landscape.
- Get the best ROI from your investments.

Contact Us

✉ Info@satius.io

🌐 www.satius.io

What We Can Cover

Network Infiltration

To evaluate the effectiveness of network security measures, the simulation agent will attempt to download a malicious payload from the internet to see if the Firewall / IPS/ Sandbox can stop the harmful payload.

Email Infiltration

To assess the efficiency of mail security devices or mail providers, the agent will send malicious payloads to the customer's dedicated email address and verify that the payload was received.

Data Exfiltration

measure the efficacy of your data loss prevention system. The simulation agent will attempt to exfiltrate fictitious sensitive data (PCI, HIBAA templates), and it will determine whether the controls in place are sufficient to halt the exfiltration of data.

Endpoint attack simulation

evaluates the effectiveness of endpoint security protections by simulating the whole attack lifecycle as mapped to the MITRE architecture. The simulation agent simulates assaults to see if the endpoint can block them.

Web Application

Simulate web application attacks from an external agent to a dedicated agent functioning as a hosted web application, usually in the DMZ, this module evaluates the efficacy of web application firewalls. It determines if these attacks can be stopped by the set WAF.

Cloud Security Auditing

Perform a cloud provider service scan to find important cloud misconfigurations that hackers might exploit. Excessive rights, unprotected S3 buckets, and cryptographic failures are just a few examples.

Cloud Attack Simulation

In the event attackers are able to access your cloud environment, they will likely attempt to access critical systems by escalating privileges. The simulation agent will gather resources from cloud environment and simulates attacks in a Local Policy Simulator to identify overly permissive IAM policies,

	Ransomware	Essential	Cloud	Premium	Premium +
EndPoint Attack Simulation	✓ Only For Ransomware Attacks	✓	-	✓	✓
Network Infiltration	✓ Only For Ransomware Attacks	✓	-	✓	✓
Email Infiltration	✓ Only For Ransomware Attacks	✓	-	✓	✓
Data Exfiltration	-	-	-	✓	✓
Web Application	-	-	-	✓	✓
Cloud Attack Simulation	-	-	✓	-	✓
Cloud Security Auditing	-	-	✓	-	✓
Detection Analytics SIEM/EDR	-	-	-	-	✓

Contact Us

Info@satius.io

www.satius.io