BLACKNOISE

Ensure ongoing PCI DSS compliance with 5 key measures

June 2025

ERIUM

5 major controls to validate through attack simulation

1 Strict control of network connections to and from the CDE

Simulation solutions can continuously test for the absence of unauthorized connections between different network segments, particularly to the card data environment (CDE) or exfiltration from it to the Internet. They simulate access attempts from various subnets to validate the effectiveness of firewalls, ACLs, and segmentation. This type of dynamic testing is more reliable than a simple static audit of the configuration. It helps to detect unintended or misconfigured access routes.

2 Proactive detection through behavioral analysis

PCI DSS requirements expect advanced security solutions to continuously monitor system behavior. Simulations allow testing whether these tools detect typical technical actions of an attacker, such as privilege escalation, lateral movements, establishing persistence, or abnormal behaviors in processes. This helps validate the actual capability of EDR/XDR solutions to identify threats from the early stages of the attack as well as at different stages of the Kill Chain.

3 Incident Monitoring and Rapid Response to Anomalies

Attack simulations can generate suspicious activities (exfiltration, command execution, user creation) to test detection and alert escalation. This allows for the evaluation of logging and SIEM systems: are they properly configured to spot these events? Are alerts transmitted in a timely manner? Is a failure of critical security control systems subject to an alert?

4 Resilience of Critical Security Controls

PCI DSS requires that malfunctions or failures of critical controls (such as IDS, antivirus, firewalls) be detected and corrected quickly. Simulations can intentionally trigger behaviors or scenarios revealing a failure (e.g., non-blocking firewall, inactive IDS) to check if alerts are generated. This allows for assessing the robustness of the monitoring of the defense systems themselves, particularly their complementarity through multi-level detection mechanisms.

5 Team Training for Incident Response

The effectiveness of an incident response plan relies on the preparation of the teams. Simulation solutions allow for the creation of controlled compromise scenarios to observe how teams react. This way, one can evaluate training, reaction times, and alignment with documented procedures. It is an excellent tool for operational validation of processes and strengthening internal skills.

20+ PCI DSS detailed requirements covered

4 BlackNoise attack scenarios

55+ technical events

PCI DSS Requirements	BlackNoise events type	Priority
1.2) Network security controls (NSCs) are configured and maintained.	Scan events	Intermediate
1.3) Network access to and from the cardholder data environment is restricted.	Scan & exfiltration events	Intermediate
1.4) Network connections between trusted and untrusted networks are controlled	Scan events	Intermediate
2.2) System components are configured and managed securely	System events	Intermediate
5.2) Malicious software (malware) is prevented, or detected and addressed	System events	High
5.3) Anti-malware mechanisms and processes are active, maintained, and monitored	System events	High
10.2) Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events	Bruteforce & log events	High
10.3) Audit logs are protected from destruction and unauthorized modifications	Log events	High
10.4) Audit logs are reviewed to identify anomalies or suspicious activity	Scan, exfiltration, system and bruteforce events	Intermediate
10.7) Failures of critical security control systems are detected, reported, and responded to promptly	Scan, exfiltration, system and bruteforce events	High
11.5) Network intrusions and unexpected file changes are detected and responded to	Scan & system events	High
11.6) Unauthorized changes on payment pages are detected and responded to	System events	Intermediate
12.10) Suspected and confirmed security incidents that could impact the CDE are responded to immediately	Scan, exfiltration, system and bruteforce events	High

BLACKNOISE

www.blacknoise.co

contact@blacknoise.co