BLACKNOISE

OPTIMIZED PENTEST STRATEGIES: MORE EFFICIENCY WITH AUTOMATED ATTACK SIMULATION

November 2024

Businesses are facing a constant increase in cyber threats, making it crucial to regularly test the security of their systems. Penetration testing (pentest) has long been the preferred method for assessing security vulnerabilities. Today, automation through Breach & Attack Simulation (BAS) and Attack Surface Management (ASM) platforms is emerging as an essential and effective complement to traditional pentesting approaches.

LIMITATION OF TRADITIONAL PENTESTING

Pentesting involves replicating hacker attacks on a system to identify exploitable vulnerabilities. While effective, it's a focused and isolated approach with limitations that are increasingly seen as obstacles:

- **High Cost and Duration:** Pentesting requires experts to perform technical actions, analyze results, draft reports, and present findings over several days.
- **Variable Expertise:** With the rapid evolution of IT environments (cloud, virtualization, PaaS, IaaS, APIs), the skill level required for pentesters is constantly rising.
- **Limited Unitary Testing:** Pentests are usually conducted system by system or application by application, which doesn't allow for effective coverage of the entire infrastructure.
- **Inscreased Regulatory Compliance:** Regulations require more frequent and extensive testing, increasing the workload for companies and placing added strain on the availability of experts.

BREACH & ATTACK SIMULATION: AUTOMATION FOR CYBER OPTIMIZATION

Breach & Attack Simulation (BAS) solutions are transforming how security is controlled. They enables comprehensive assessments of vulnerabilities and risks, providing substantial benefits for users:

- **Real-Time Results:** Attack simulations offer an instant view of an organization's exposure to threats, allowing for quick responses and adjustments to security strategies based on new attack tactics and techniques.
- **Broad, Repetitive Coverage:** BAS solutions automate testing across the entire infrastructure, identifying vulnerabilities across a wider attack surface.
- **Resource Optimization:** BAS results allow human audits to focus where they are truly needed.
- **Enhanced SOC Monitoring:** BAS platforms help identify blind spots in monitoring systems, ensuring the effectiveness of detection scenarios and improving defenses against increasingly sophisticated attack techniques.

WHY COMBINE THE TWO APPROACHES ?

While BAS automates and optimizes testing, pentesting remains essential for compliance audits and specific security evaluations. By combining these two approaches, companies can maximize test coverage, strengthen the relevance of technical audits, and optimize budget usage.

Conclusion

The choice between pentesting and Breach & Attack Simulation depends on each organization's specific needs. While pentesting remains crucial for regulatory audits, integrating a BAS platform provides a modern and efficient approach for proactive security. By leveraging automation, businesses can enhance resilience to cyber threats, confidently meet compliance requirements, and optimize budget commitments.

BLACKNOISE

More info


contact@blacknoise.co


www.blacknoise.co