

SIEM, Exposure Management and Related Artificial Intelligence Technologies

AN IDC CONTINUOUS INTELLIGENCE SERVICE

IDC's *SIEM, Exposure Management and Related Artificial Intelligence Technologies* service covers security software and hardware products related to security information and event management (SIEM) and exposure management platforms. Specific functions covered include device and application vulnerability management, SIEM, attack surface management, breach and attack simulation/security validation, and automated red teaming. The service is designed to create in-depth coverage of analytics tools used in the security operation centers.

Markets and Subjects Analyzed

- Application vulnerability management
- Device vulnerability management
- SIEM
- Attack surface management
- Breach and attack simulation/security validation

Core Research

- Application Vulnerability Management Market Share
- Device Vulnerability Management Market Share and Forecast
- IDC MarketScape: Device Vulnerability Management
- SIEM Market Share and Forecast
- Attack Surface Management and Breach and Attack Simulation Market Forecast
- SIEM and Device Vulnerability Management User Survey
- Market Analysis Perspective

In addition to the insight provided in this service, IDC may conduct research on specific topics or emerging market segments via research offerings that require additional IDC funding and client investment. To learn more about the analysts and published research, please visit: [SIEM, Exposure Management and Related Artificial Intelligence Technologies](#).

Key Questions Answered

1. Who are the major players in the SIEM market?
2. Who are the major players in the vulnerability management space?
3. What is the size and market opportunity for SIEM solutions?
4. What is the size and market opportunity for exposure management solutions?
5. How is artificial intelligence (AI) improving exposure management?
6. How are these technologies using AI today, and what is coming in the future?
7. How is generative AI being leveraged to improve the usability of security analytics tools?
8. How are today's separate products becoming features in new combined offerings?

Companies Analyzed

This service reviews the strategies, market positioning, and future direction of several providers in the security market, including:

Armis, AttackIQ, Axonius, Balbix, Brinqa, Censys, Checkmarx, Cisco, Contrast Security, CrowdStrike, CyCognito, Cymulate, DAS Security, Devo, Exabeam, Elastic, Fortinet, Fortra, Google, HCL Technologies, IBM, Invicti, Ivanti, JupiterOne, Logpoint, LogRhythm, Mandiant, Mend, Microsoft, NetWitness, NopSec, NSFOCUS, Open Text, Outpost24, Palo Alto Networks, Pentera, Picus Security, Positive Technologies, Qi An Xin Group, Qualys, Rapid7, SafeBreach, Securonix, ServiceNow, Skybox Security, Snyk, Sonatype, Splunk, Sumo Logic, Synopsys, Tanium, Tenable, Trellix, Venustech Group, Veracode, Vulcan Cyber, XM Cyber, and Zoho.