SIEM, Exposure Management and Related Artificial Intelligence Technologies

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), exposure management platforms, and artificial intelligence (AI)–related technologies. Specific functions covered include device vulnerability management, SIEM, attack surface management, breach and attack simulation/security validation, and automated red teaming. This service is designed to create in-depth coverage of analytics tools used in the security operation centers and vulnerability management teams.

MARKETS AND SUBJECTS ANALYZED

- AI security and AI security assistants
- Device vulnerability management/exposure management
- SIEM
- Attack surface management
- Breach and attack simulation/security validation

CORE RESEARCH

- Artificial Intelligence Security Use Cases
- Device Vulnerability Management Market Share and Forecast
- IDC MarketScape: SIEM
- SIEM Market Share and Forecast
- Attack Surface Management and Breach and Attack Simulation Market Forecast
- SIEM and Device Vulnerability Management User Surveys
- 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/exposure 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 improving exposure management and security operations?
6. What do end users feel is important in SIEM and exposure management today?
7. 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, AWS, Axonius, Balbix, Blumira, Brinqa, Censys, Cisco, Claroty, CrowdStrike, Cyber Hunters, CyCognito, Cymulate, Das Security, Darktrace, Datadog, Devo, Dragos, Elastic, Exabeam, Fortinet, Fortra, Google, Graylog, Gurucul, IBM, Ivanti, JupiterOne, Logpoint, LogRhythm, Microsoft, NetWitness, NopSec, Nozomi, NSFOCUS, Nucleus Security, OpenText, Outpost24, Palo Alto Networks, Panther, Pentera, Picus Security, QiAnXin Group, Qualys, Radiflow, Rapid7, SafeBreach, Securonix, SentinelOne, ServiceNow, Skybox Security, Snowflake, Splunk, Sumo Logic, Tanium, Tenable, Trellix, Trend Micro, Venustech Group, Vulcan Cyber, XM Cyber, Zoho, and Zscaler.