Cloud Native XDR and Artificial Intelligence Security Analytics

IDC's *Cloud Native XDR and Artificial Intelligence Security Analytics* covers the evolution of extended detection and response (XDR), the role of artificial intelligence (AI) in cybersecurity platforms, and the tools and processes required to uplevel the role of Level 1 security operation center (SOC) analysts into more proactive roles in threat hunting and mitigation in software. A representative mix of technologies that comprise SOC analytics includes SOAR, network intelligence and threat analytics (NITA), deception, threat intelligence platforms and security services (TIP/TISS) adversary tools, process dump tools, sandboxing/reversing tools, and Windows/OSX/Linux evidence collection. This research is the advanced analytics companion to IDC's cybersecurity security information and event management (SIEM) and security and vulnerability management (SVM) market, which focuses on SIEM, SVM, and attack surface management tools.

MARKETS AND SUBJECTS ANALYZED

- Network detection and response
- Cloud-native XDR (non-endpoint based)
- Threat intelligence platforms and security services
- SOAR
- Firewall automation
- Generative AI in SOC processes

CORE RESEARCH

- Level 2 Analyst Survey
- Effects of GenAI in Detection and Response
- IDC Market Analysis Perspective
- Cloud-Native XDR, NITA, SOAR, and Threat Intelligence Market Share and Forecast

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. Planned research in 2025 includes a global survey about XDR end user usage and use cases. To learn more about the analysts and published research, please visit: Cloud Native XDR and Artificial Intelligence Security Analytics.

KEY QUESTIONS ANSWERED

1. What is the size and market opportunity security analytics solutions?
2. Which is the architecture of XDR?
3. What is the size and market opportunity for advanced security orchestration solutions?
4. What is the size and market opportunity for NDR solutions?
5. How has the competitive landscape changed through digital transformation and adoption of cloud and enabling technologies?
6. What role will generative AI play in creating advantages for SOC analysts, and what roles may be replaced or subsumed?

COMPANIES ANALYZED

This service reviews the strategies, market positioning, and future direction of several providers in the tier 2 SOC analytics market, including:

Accenture, Alert Logic, AlgoSec, Amazon Web Services, Anomali, Arista Networks, AT&T, Bitdefender, Booz Allen, Broadcom, Bugcrowd, Checkmarx, Checkpoint, Cisco, CrowdStrike, Cybersixgill, Darktrace, Dazz, Dell Technologies, Elastic, ESET, Exabeam, ExtraHop Networks, Flashpoint, Forcepoint, Fortinet, Fortra, Gigamon, Google, Gurucul, HCL Technologies, Help Systems, Hunters.ai, IBM, InfoBlox, Intel, Intel471, Kaspersky, Kaseya, LevelBlue, LogRhythm, LookingGlass, Lumen, Mandiant, McAfee, MetricStream, Micro Focus, Microsoft, MixMode, Netenrich, NetScout, NetWitness, NIKSUN, NortonLifeLock, NSFOCUS, Nudge Security, OpenText, Oracle, Palo Alto Networks, Plixer, PwC, Qualys, Rapid7, Recorded Future, Red Hat, ReversingLabs, Riverbed Technology, Secureworks, SecurityScorecard, Semperis, SentinelOne, ServiceNow, Skybox Security, Sophos, Splunk, StellarCyber, StrikeReady, Sumo Logic, Swimlane, Tanium, Tenable, Tencent, ThreatConnect, Tines, Torq, Trellix, TrendMicro, Tufin, Trustwave, Vectra, Venustech Group, VMware, Zero Fox, and Zoho..