

# Cloud Native XDR and SOC Analytics

AN IDC CONTINUOUS INTELLIGENCE SERVICE

IDC's *Cloud Native XDR and SOC Analytics* covers the evolution of extended detection and response (XDR) and the tools and processes required to uplevel the role of tier 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 Intelligence and Threat Analytics
- Cloud-Native XDR (non-endpoint based)
- Threat Intelligence Platforms and Security Services (pending)
- SOAR
- Firewall Automation

## Core Research

- SOC 2 Analyst Survey
- Tier 2 Analytics Market Glance
- 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. To learn more about the analysts and published research, please visit: [Cloud Native XDR and SOC Analytics](#).

## Key Questions Answered

1. What is the size and market opportunity for tier 2 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 NITA solutions?
5. How has the competitive landscape changed through digital transformation and adoption of cloud and enabling technologies?

## Companies Analyzed

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

Alert Logic, AlgoSec, AT&T, Beyond Security, BeyondTrust, BitSight, Broadcom, Checkmarx, DarkTrace, Dell Technologies, Exostar, ExtraHop Networks, FireEye, Fujitsu, HCL Technologies, Help Systems, IBM, Ivanti, Kaseya, Kenna Security, LogRhythm, LookingGlass, McAfee, MetricStream, Micro Focus, Microsoft, NortonLifeLock, NSFOCUS, NTT Application Security, OpenText, Palo Alto Networks, Qualys, Rapid7, ServiceNow, Skybox, Splunk, Sumo Logic, Synopsys, Tanium, Tenable, Tripwire, Tufin, Vectra, Venustech Group, Veracode, and WhiteSource