Tier 2 SOC Analytics

AN IDC CONTINUOUS INTELLIGENCE SERVICE

IDC's *Tier 2 SOC Analytics* covers advanced cybersecurity analytics platforms targeting Level 2 and Level 3 SOC analyst roles including adversary emulation, disk image creation tools, evidence collection, incident management, log analysis tools, memory analysis tools, memory imaging tools, process dump tools, sandboxing/reversing tools, and Windows/OSX/Linux evidence collection. This research is the advanced analytics companion to IDC's Cybersecurity Analytics, Intelligence, Response and Orchestration service, which focuses on analytic security platforms, security and vulnerability management (SVM), and security orchestration platforms targeting Level 1 SOC analyst roles.

Markets and Subjects Analyzed

- Network Intelligence and Threat Analytics (NTIA)
- XDR
- Forensics and Incident Investigation
- Policy and Compliance Appliances
- Orchestration and Automation Tools

Core Research

- SOC 2 Analyst Survey
- Tier 2 Analytics Market Glance
- IDC TechScape
- Threat Analytics Market 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: Tier 2 SOC Analytics.

Key Questions Answered

1. What is the size and market opportunity for tier 2 security analytics solutions?
2. Which are the major players in XDR?
3. What is the size and market opportunity for advanced security orchestration solutions?
4. What is the size and market opportunity for advanced threat analytics 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