Market Share

Worldwide Cybersecurity AIRO and Tier 2 SOC Analytics Market Shares, 2020: The Seeds That Become Cloud-Native XDR

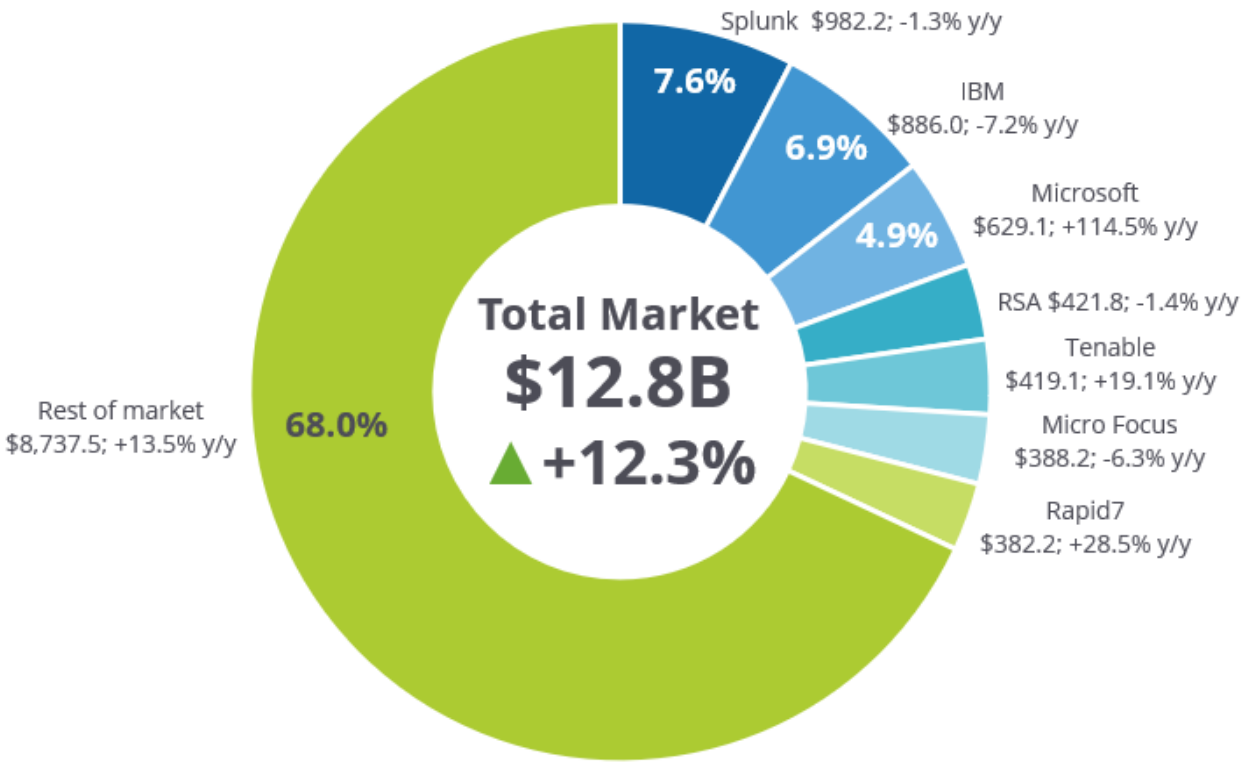
Christopher Kissel Michelle Abraham Michael Suby Frank Dickson
Christopher Rodriguez

THIS IDC MARKET SHARE EXCERPT FEATURES IRONNET CYBERSECURITY

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Cybersecurity Analytics, Intelligence, Response, and Orchestration and Tier 2 SOC Analytics 2020 Share Snapshot



Note: 2020 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2021

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC Market Share: Worldwide Cybersecurity AIRO and Tier 2 SOC Analytics Market Shares, 2020: The Seeds that Become Cloud-Native XDR (Doc # US47081421). All or parts of the following sections are included in this excerpt: Executive Summary, Who Shaped the Year, Market Context, Appendix and Learn More. Also included are Figure 1 and Table 1.

EXECUTIVE SUMMARY

As of early June 2021, COVID-19 still rages as a global pandemic — it is still too early to write the historical tomes about the pandemic's social, political, and business effects. However, there was a very specific instance that occurred in late March 2020 through to the early summer of 2020 wholly germane to the vendors and buyers of analytics, response, intelligence, and orchestration (AIRO) tools. The observable global societal and business effects included:

- **Aside from essential workers, the human populace was encouraged to quarantine as much as possible.** Out of necessity, the global workforce was driven to work from home (WFH). By some estimates, in the United States, the WFH workforce approached 40% of all workers. Many of these jobs are not going back to on-premises and, at the very least, will be a mix of remote and on premises.
- **Certain businesses were driven to their knees, and several businesses folded up shop never to return.** The most at-risk businesses were hospitality businesses such as hotels, cruise ships, and restaurants. The travel industry was waylaid. Self-evidently, large multinational corporations such as Boeing, JW Marriott, Hertz, and American Airlines had to lay off employees in droves. The loss of revenues put companies in the precarious position of allocating reduced moneys for salary, goods and services, and cybersecurity budgets.
- **The traditional buying cycles of many AIRO products was abruptly disrupted.** The proof-of-concept (POC) cycle for security information and event management (SIEM) was on premises, and contacts commonly were three years and into seven figures in U.S. dollars. The POC included on-hands training, and both the seller and the buyer required boardroom executive decision maker sign-offs to win the contract. Other on-premises POC (then, and sometimes still) large contracts included network intelligence and threat analytics (NITA) tools and security orchestration and automation response (SOAR) tools.
- **The slowly evolving adaptation being made by businesses toward digital transformation (DX) rapidly accelerated.** Businesses may have been cool to DX (a double entendre intended as companies may have been taking their time toward DX or were disbelieving), but the WFH "branch offices of one" changed both networking and security architectures relative to businesses on the fly. One of the underlying themes of this study is that the forced transition to DX was largely a boom for AIRO technologies and less a bust.

The pandemic changed the philosophies of both cybersecurity vendors and cybersecurity product buyers. Vendors that relied on enterprise licenses quickly learned how to adapt their products for software-as-a-service (SaaS) delivery. Buyers that may have preferred to have longer POC sales cycles or favored on premises and public cloud as a secondary option started to migrate to cloud delivered — one nice aspect of SaaS is that the vast majority of contracts are for one year but are often billed monthly).

In addition, businesses became more reliant on applications. An application that may have emanated centrally from a private datacenter with controls increasingly went straight to the end user. As this occurred though, the security operation center (SOC) loses visibility. To offer protection, the SOC would have to look for anomalies either in network performance monitoring or in batch data. Both of these conditions created opportunities for NITA product providers, which is a dynamic that is discussed throughout the document.

Ultimately, the revenue from the sale of cybersecurity AIRO products hit a temporary pause from mid-March to mid-May. Sadly, it is also becoming evident that increased activity from cybergangs and nation-states is taking places (perhaps as much a diplomatic problem as it is a cybersecurity problem). In any event, cybersecurity became a more salient need than ever to protect a remote workforce and to ensure the safety of the remote shopper as well.

This IDC study provides worldwide market share data for cybersecurity analytics, intelligence, response, and orchestration (AIRO) and tier 2 SOC analytics for calendar year 2020.

"The idea of 'adapt and overcome' was never more evident to businesses as well as to the cybersecurity tool providers that protected them," said Chris Kissel, research director, Cybersecurity and Trust Products. "Often, the extensibility of cybersecurity AIRO products is controlled, but when the sudden migration to a remote workforce occurred, we learned that detection and response and security orchestration tools were equal to the task."

ADVICE FOR TECHNOLOGY SUPPLIERS

A word that is often misunderstood is "articulate." The general impression is that an articulate person uses the fanciest word or phrase to explain a situation. This is not right. Articulation is the ability of one person to convey the greatest amount of information and intention to another party so that the information is well understood and usable.

Right now, cybersecurity vendors have to articulate their goods and services as meaningfully as possible. Marketing is complicated, but outcomes derived from security products should not be. Taglines should read:

- Gain visibility of your VPN.
- Protect against ransomware.
- Reduce the attack surface.

In longer POC cycles, sales engineers can show other professionals how to optimize or tweak software for specific environments, but "out of the box" means more than ever now. Here are other dynamics that software vendors should be aware of:

- **From the customer's perspective, it is all about articulating and then proving a responsible cybersecurity posture**. IT is tough stuff. Network crashes and exposures can occur from possibilities of the most benign and accidental but fateful employee activity through to a highly intelligent and orchestrated nation-state attack. In companies with 2,500+ employees, roughly 72% will experience a ransomware attack that affects at least one endpoint in a calendar year. Businesses must be able to articulate and engender a culture where every reasonable precaution is taken to protect the most critical data and machines, provide digital resiliency including perimeter protection, and have quick isolation techniques, a disaster recovery plan in place, and a response plan including notifying customers and law enforcement when there is a

breach. When a company can prove that these procedures are in place, it cuts down its indemnity, but more importantly, the right procedures ensure that the businesses correctly and consciously act on the behalf of the best interests of its stakeholders.

- **Businesses need to understand their risk; therefore, vendors start by articulating risk and then branch out.** It is absolutely true that businesses would like to know when there are significant vulnerabilities on their network and would like to know the second that there is adversarial behavior on its network. Reality is different. In device vulnerability management, for example, on a given list of possible vulnerabilities, somewhere between 5% and 10% of all vulnerabilities have an active exploit kit. Ideally, even an academic or dormant vulnerability would be patched, but a business has limited time and human manpower constraints. And linking to the first point about cybersecurity posture, "risk" is the ability to link metrics to issues pertaining to the value of assets, mean time to detect (MTTD), and mean time to respond (MTTR); conforming to regulatory standards; and applying trust in handling customer and contractor sensitive data.
- **In so many businesses, IT/DevSecOps personnel are the same person.** Worth reinstating from last year, often, cybersecurity analysts start with the assumption that businesses have a dedicated SOC. IDC does not have a vetted number, but it is safe to say that more than 90% of all businesses do not have a dedicated SOC. Unfortunately, any business that has an association with the internet has information or assets potentially under siege by an adversary. Many companies have an "IT guy," and that person does everything from hooking up Ethernet cabling to setting up passwords to writing firewall rules. The industry can't keep throwing bodies at problems; it will have to make up the employment gaps in software.

  Currently, no cybersecurity vendor can be all things to everyone, but they must connect to the fiber that provides the best overall outcomes. The adversary can attack at the time of BIOS when a machine is booted on through to man-in-the-middle cookies used when an online retail transaction is occurring. Increasingly, more attention is given to containers and DevOps — first, it starts to the left of the conventional cybersecurity stack, and second, many companies had to develop applications to account for the realities of a mobile workforce. This means that companies should have either connectors or app store options to make their platforms extensible to other aspects within the IT/security stack.
- **Cybersecurity product vendors must invest in what were thought to be soft values.** The customer expects more from you, cybersecurity vendor. For all of the wizardry available on a cybersecurity dashboard, often, an analyst will need to know how to use a feature; there has to be a human being on the other end. IDC also believes that a product should be issued with a certain number of credits or tokens as a term of service. For instance, if a company wants to use threat hunting, it might receive 10 tokens as a part of software contract. A token could be an hour of labor or a specific insight or action. The token idea could be used to help with script development to connect toolsets via an OpenAPI, to configure servers, or to attach tools to Active Directory (AD) (see Table 1).

TABLE 1

Worldwide Cybersecurity Analytics, Intelligence, Response, and Orchestration and Tier 2 SOC Analytics Revenue by Technology, 2019 and 2020 ($M)

	2019	2020	2019–2020 Growth (%)	2020 Share (%)
Legacy cybersecurity SIEM, VM, and AIRO enabling	8,729.2	9,590.1	9.9	74.7
Network intelligence and threat analytics (formerly threat analytics)	1,575.0	1,861.4	18.2	14.5
Network intelligence	938.9	1,166.6	24.2	
PCAP/NPM	417.5	443.5	6.2	
Emulation and deep packet insights	137.5	150.6	9.5	
Deception	81.1	100.6	24.0	
Automation and orchestration	1,103.3	1,300.4	17.9	10.1
Cloud-native XDR	26.8	94.4	251.7	0.7
Total	11,434.3	12,846.3	12.3	100.0

Source: IDC, June 2021

WHO SHAPED THE YEAR

This Excerpt was prepared for IronNet Cybersecurity but also included the following vendors: ExtraHop, Palo Alto Networks, and Vectra

The following companies excelled in 2020 and into early 2021. IDC believes that good technology creates revenue opportunities and this becomes a virtuous cycle. However, IDC is recognizing larger hopes. IronNet is noted for building cybersecurity practices for vertical markets but also for initiating a private organization and U.S. government threat defense collective.

IronNet Cybersecurity

The IronNet differentiator is its Collective Defense platform that consists of its IronDefense network detection and response and its unique IronDome threat sharing solution that facilitates a crowdsource-like environment, in which IronDefense threat detections from individual companies are shared anonymously and in real time among members of a secured Collective Defense community. The benefits of the IronNet solution are to speed up sharing of information to help enterprises combat attackers together instead of alone and to enable immediate sharing rather than weeks or months after the incident. There is also an option to send anonymized insights to the U.S. government to allow it to act, if necessary, especially against nation-state actors.

The IronNet Collective Defense platform can be made specific to industries, supply chains, or geographies to crowdsource data about attacks. IronNet believes it has an opportunity to expand existing communities as well as add new cornerstone customers to develop Collective Defense communities. Global expansion is part of its strategy, and the company has worked with international customers to build regional Collective Defense communities in Asia/Pacific (including Japan) and EMEA.

IronNet addresses the scarcity of security professionals, closing the talent gap with AI-based behavioral analytics that automatically detect and rate alerts. The IronDefense analytics engine uses supervised and unsupervised ML to identify harmful network perimeter traffic as well as east-west traffic within the enterprise. An integrated expert system automatically acquires contextual data and applies investigative playbooks to prioritize risk. A hunt module is included and enables security analysts to hunt across all collected network metadata or to drill into network flows down to individual PCAP data. IronDome automatically correlates IronDefense detections across an enterprise's Collective Defense community, and enterprises can share insights with others who already may be working on similar detections in real time. This capability allows peer enterprises within a community to benefit from its combined efforts in detection, remediation, and mitigation to enable faster detection and response to cyberattacks at earlier stages of the intrusion.

Enterprises can choose to deploy the IronNet Collective Defense platform in the cloud or on premises with hardware or virtual appliances. Pricing is subscription based and starts at a few thousand dollars per month and increases with the number of employees, traffic volume, and/or tiers of services. In May 2021, a new private cloud option was released that allows customers to deploy the platform on hyperconverged infrastructure (HCI). IronNet brings in log data from cloud environments as well as the many point solutions of its ecosystem partners and can bring in data from public cloud deployments for analysis. Its most recent release added integrations with AWS, CrowdStrike, Microsoft Azure, Microsoft Office 365, Palo Alto Networks, and Zscaler. IronNet has also joined with a number of services partners such as Jacobs Engineering, Raytheon Technologies, and Accenture to deliver end-to-end solutions.

IronNet announced on March 2021 that it is going public via a combination with special purpose acquisition company LGL Systems Acquisition. The proceeds of the transaction will be used to accelerate IronNet's revenue growth, to expand its product portfolio, and for working capital to fund increasing demand. Its estimated revenue for fiscal year ending January 31, 2022, is $54 million with a gross profit margin of 74%, up from revenue of $28.9 million in the previous fiscal year. Ninety percent of revenue is from software, with 81% from the private sector, primarily from the financial services and energy and utilities verticals.

MARKET CONTEXT

Significant Market Developments

We have peppered this document with observations about each individual technology in cybersecurity AIRO. Here we summarize the biggest market developments:

- Businesses were forced into digital transformation, and cybersecurity AIRO technologies filled in the gaps.
- Cybersecurity AIRO vendors that had SaaS offerings did very well, especially in SIEM.

- Vendors need for businesses to understand and articulate risk. In cybersecurity, risk is the summary of implied trust, exploitability, asset criticality and the fiduciary responsibility that companies demonstrate toward their employees, stakeholders, contractors, and customers.
- While not covered in AIRO, data has its own gravity. Equipoise will be required to maximize the power of data while protecting the identities and anonymity of source data.
- User behavioral analytics are ubiquitous across AIRO technologies.
- DevOps is increasingly becoming a part of the cybersecurity stack.
- Incident detection and response remains wildly important (naturally) but must be considered in the overall context of prevention, network performance, and digital resilience.
- Making external threat intelligence about malware and adversaries requires more than feeds through an OpenAPI.
- The first expressions of XDR are proprietary.

Ultimately, cybersecurity vendors have to see themselves as strategic partners for the business that they serve. Soft values such as script development, customer service, limited threat hunting, and even advising adjacent IT purchases to help with an overall posture are not just amenities; they are expectations businesses had of cybersecurity vendors during a global pandemic.

METHODOLOGY

This IDC cybersecurity market share document represents the summation of all 2020 reports as well as market trends known into early May 2021. Importantly, the revenue estimates were derived in the same cycle as the Worldwide Security Tracker.

In this study, IDC is tracking several primary markets. This means that the revenue generated for one SKU can only be realized once (the revenue cannot be double counted in network intelligence and threat analytics and SIEM, for instance). The second note is that there are revenues from physical appliances that are not represented in IDC's Software Tracker that are captured in these market revenue estimates, although these revenues are a very nominal part of the industry whole.

The IDC software market sizing and forecasts are presented in terms of commercial software revenue. IDC uses the term commercial software to distinguish commercially available software from custom software. Commercial software is programs or codesets of any type commercially available through sale, lease, rental, or as a service. Commercial software revenue typically includes fees for initial and continued right-to-use commercial software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. Commercial software must be available for competitive bidding. These use cases are counted by IDC as commercial software revenue.

Commercial software revenue excludes service revenue derived from training, consulting, and systems integration that is separate (or unbundled) from the right-to-use license but does include the implicit value of software included in a service that offers software functionality by a different pricing scheme. It is the total commercial software revenue that is further allocated to markets, geographic areas and, sometimes, operating environments. For further details, see *IDC's Worldwide Software Taxonomy, 2021* (IDC #US47588620, April 2021).

As part of the cadence with this document and intimated previously, IDC sent revenue estimates to companies in this study for review and a chance to comment. Under no circumstance will IDC disclose the degree of transparency a vendor provided for a specific revenue estimate. Many companies may offer a precise revenue estimate or guide an analyst to 10-K/10-Q or related statements. Other companies are privately held or do not comment; others still provide ballpark estimates. In addition, the security team works with the larger Tracker Group, and we reconcile revenues to add to a larger whole. Other tools at the disposal of the analyst are contracts won, press releases, and number of employees. Otherwise, it is unfair and unethical to compromise the confidentiality of the participating vendors.

The data presented in this study is IDC estimates only.

Note: All numbers in this document may not be exact due to rounding.

MARKET DEFINITION

The acronym AIRO is derived from analytics, intelligence, response, and orchestration (AIRO). Software products in this market include those that create, monitor, assess, and report security policy; determine the configuration, structure, and attributes for a given device; perform security assessments and vulnerability scanning; aggregate and correlate security logs; and provide management of various security technologies from a single point of control.

The cybersecurity AIRO taxonomy is made up of three submarkets and nine discrete technologies that roll up into the three submarkets. The three submarkets are analytics and intelligence, response, and orchestration. The nine technologies are SIEM; network intelligence and threat analytics (NITA); third-party risk and benchmarking; forensics and incident investigation; policy and compliance products/appliances; security governance, risk, and compliance (GRC); device vulnerability management; application vulnerability management; and orchestration and automation tools.

The general classifications of the technologies still fit and are explained in the sections that follow. However, in many cases, the technologies often blend together. One example would be in application vulnerability management where IDC is estimating the revenues for dynamic application security testing (DAST). The same platform may include static application security testing (SAST) or runtime application self-protection (RASP) on the platform. Splunk's Enterprise platform is both IT service management and SIEM. With few exceptions though, IDC makes a concerted effort to only count one SKU in one revenue bucket.

Analytics and Intelligence (Input and Analysis)

The analytics and intelligence cycle in cybersecurity AIRO is the beginning of a formal investigation cycle but does need further erudition. (Note: The description of analytics and intelligence is not meant to be set in stone.) Analytics and intelligence, response, and orchestration are becoming increasingly intertwined. The following are general fabrics that describe the functionality of tools:

- Analytics is such a ubiquitous term in security and, indeed, in all software that it is almost without meaning. In cybersecurity AIRO, analytics is an abstraction layer that complements intelligence and finds anomalies. Analytics would also refer to commonly correlated data sets, such as user behavioral analytics (UBA) or user and entity behavioral analytics (UEBA), alerts aggregation, and configuration drift. Additional analytics layers refine anomalies to a single version of truth (hopefully) and queue analysts into the next steps in their investigations.

- Intelligence would be the further refinement of analytics. In cybersecurity AIRO, the first meaning of intelligence is the telemetry that can be gathered from the network. Telemetry sources include batch data from applications, various network flow data, curated data from sources such as threat intelligence sources, and metadata, which is the collection of packet headers and the indexing of full packets. Intelligence works hand in hand with analytics to work data collection into meaningful insights and a workflow for IT/SecOps.

Now to discuss the discrete technologies:

- Network intelligence and threat analytics (NIST) is a technology sector within the cybersecurity AIRO product group within the IDC Security and Trust set of services. The acronym for NITA establishes the foundation for the types of technologies and platforms that are mapped within the service. Network intelligence roughly maps to the common industry acronym NDR. The reason for the expanded definition is IDC wanted to include all the ways that the network itself is used for detection. In this study, there are four discrete technologies that become the totality of NITA:
  - **Network intelligence.** Network intelligence extracts metadata from packets and applies insights about the packet based on user behaviors (UBA) and network events and often cross-correlates with threat intelligence or attack simulation to find possible adversaries. These are often L3 tools but can also be L4–7. Network intelligence platforms can also combine external threat intelligence, known bad domains, malware families, and advanced persistent threat actors to metadata occurring (or occurred) on the network. The objective for the types of analytics used in network intelligence is to reduce the number of threats and/or string alerts to create one version of truth. Last, because network intelligence enriches data, these platforms (in theory) facilitate search better than SIEM or IaaS.
  - **Deception.** Deception has a legacy technology perception of setting decoys, lures, and honeypots, but these vendors also now focus on distributed or endpoint deception, where deceptions trip attackers attempting to move off the attack beachhead — credential harvesting, lateral and cloud movement, attack path reduction, and so forth. Worth noting about deception, the working assumption is that the alerts coming from a deception platform are high fidelity — if the recreated files, registries, or IP/MAC devices are approached, there is no reason for the authenticated user to be attempting access.
  - **Full packet capture (PCAP) and network performance monitoring tools (NPM).** The first set of these tools would be platforms that perform full PCAP for analytics and forensic investigations. The con about using PCAP tools is that storage is expensive and full fidelity event replay is hard to perform over time. However, the adversary cannot hide in the packets; even with all of the evidence finding IOC much less, the actual adversary in PCAP tools is difficult. In many instances, only PCAP is admissible in criminal court. NPM has high bandwidth capabilities and was designed to monitor high media events such as video and IP telephony events. Statistical analyses of jitter and potential bottlenecks help telecom operators with media. Ultimately, many of the NPM tool providers converted their platforms for network security.
  - **Emulation and deep packet insights.** Test emulation is a tool that runs threat simulations with payloads on a network, which is slightly different from attack simulation (attack simulation is not included in this category and, as a product group, not currently included in the cybersecurity AIRO taxonomy). Emulation occurs when a live agent is placed on machines that measure how a device is performing when real malware is introduced on a network emulation layer. The deep packet inspection tools come from vendors that

perform file analysis and derivatives of sandboxes to identify IOC. The advantage of this technology is that a sandbox creates latencies while a file is being convicted, which is important not only in north-south traffic but in moving traffic laterally within internal servers.

Orchestration (Automation)

- **Security orchestration** is a method of connecting security tools and integrating disparate security systems. Orchestration is the connected layer that streamlines security processes and powers security automation. In addition, orchestration enables an organization to maximize the productivity of its scarcest security resource, people, by reducing frequent and repetitive tasks generated within a given workload.
- **Automation and orchestration** are becoming increasingly important concepts in cybersecurity AIRO. Orchestration helps a SOC move with the agility that the adversary does by updating SIEM filters, updating AV engines and firewalls with information about malware signatures, blacklisting bad websites, and so forth. Automated functions dynamically institute playbooks, trigger the download of proper patches, and then initiate a vulnerability assessment scan. Parts of both automation and orchestration can be replicated within RESTful and OpenAPI. In addition, automation and orchestration are found in SIEM, EDR, threat analytics, and NAC platforms. However, this category is only about standalone companies that offer automation and orchestration, not the subsegment function included in various platforms.

Security orchestration includes ServiceNow, Splunk (Phantom), Cortex SOAR (from Demisto), and Swimlane. The automation revenues IDC is tracking belong to firewall automation vendors such as FireMon and Tufin.

- **Cloud native XDR** is being defined dynamically and in real time. Currently, IDC is considering cloud-native XDR to be a unified dashboard and set of processes with a baseline expectation of log management, data from an endpoint agent, external threat intelligence, and user and entity behavioral analytics (UEBA). The revenue estimates presented in tier 2 SOC analytics though included XDR revenues from companies that are converting discrete technologies form NITA, productizing threat intelligence security services (TISS), and even offer XDR as a natural extension to device vulnerability management, SIEM or, conceivably, SOAR platforms.

RELATED RESEARCH

- *Worldwide Network Intelligence and Threat Analytics Forecast, 2020-2024: Tempering Multiple Data Sources for Meaningful Cybersecurity Insights* (IDC #US46350920, December 2020)
- *Worldwide Network Intelligence and Threat Analytics Market Shares, 2019: How the Network Is Used to Unmask the Adversary* (IDC #US46351020, December 2020)
- *Market Analysis Perspective: Worldwide Cybersecurity Analytics, Intelligence, Response, and Orchestration, 2020* (IDC #US46837720, September 2020)
- *Worldwide Device Vulnerability Management Forecast, 2020-2024: What Lies Beneath the Attack Surface* (IDC #US46286620, May 2020)
- *Worldwide Device Vulnerability Management Market Shares, 2019: Finding the Transitional Elements Between Device Assessment Scanning and Risk-Based Remediation* (IDC #US46284720, May 2020)
- *Analytics: The Foundation of the Future of Trust* (IDC #DR2020_T7_CK, March 2020)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com