KuppingerCole Report

LEADERSHIP COMPASS

By John Tolbert

October 22, 2020

Security Orchestration Automation and Response (SOAR)

This report provides an overview of the SOAR market and provides you with a compass to help you to find the solution that best meets your needs. We examine the SOAR market segment, product/service functionality, relative market share, and innovative approaches to providing SOAR solutions.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

As the number and sophistication of cyberattacks have continued to increase over the years, some vendors realized that the traditional approaches and tools of cybersecurity likewise have failed to keep up. Twenty-five years ago, a single firewall may have been enough to protect sensitive resources within the corporate network, but this is no longer the case. Many security conscious organizations can find themselves administering over 50 different and disjointed security tools.

Just a decade ago, Security Information and Event Management (SIEM) products were hailed as the ultimate solution for managing security operations. In many organizations, they still form the foundation of modern Security Operations Centers. However, visibility of potential security events alone does not help analysts to assess each discovered threat, nor does it reduce the amount of time spent on repetitive manual tasks that constitute an incident response process.

First generation SIEMs did provide value, but many early SIEM users report that the volume of false positives caused problems in trying to sift out what was worthy of attention and follow-up and what was not. Second generation SIEMs usually incorporate Machine Learning (ML) detection models as a means to reduce false positives and provide more actionable intelligence to analysts and admins.

Parallel to these newer SIEM solutions, a class of incident response platforms has emerged focusing on creating more streamlined and automated workflows for dealing with security incidents.
Security Orchestration, Automation and Response (SOAR) products are the latest iteration of this evolution. Driven by the growing demand to implement centralized, automated control over incident analysis and response workflows across disparate security solutions, vendors are expanding their existing security intelligence, security orchestration or incident response platforms to combine the key capabilities across all three of these market segments. Complementing or directly integrating with SIEMs, SOAR platforms aim to become the foundation of contemporary Security Operations Centers (SOCs).

Modern cybersecurity architectures must include tools and services that cover everything from the network layer to the application layer and all the devices in between. Network layer security tools include firewalls, VPNs, routers/switches, Software Defined Networking (SDN) control planes, Intrusion Detection and Prevention Systems (IDS/IPS), email gateways, web gateways, Network Detection & Response (NDR) solutions, and Distributed Deception Platforms (DDPs). Associated cloud resources should have Cloud Access Security Brokers (CASBs) for both network and application layer controls, and Cloud Workload Protection Platforms (CWPPs) to secure loads in IaaS and PaaS.

Endpoints need Endpoint Protection (EPP) suites and Endpoint Detection & Response (EDR). EPP should contain a multiplicity of security functions: advanced anti-malware agents that can proactively discover and prevent malware from executing, utilizing ML-enhanced behavioral and memory analysis, exploit prevention, and other measures. EPP should also perform application control, integrate with or provide endpoint firewall protection, URL filtering, critical system file monitoring, asset inventory and patch management, and

vulnerability management. EDR solutions have deeper monitoring and analysis functions that look for signs of attacks on endpoints that may have gone unnoticed by EPP. EDR should have automatic analysis and remediation capabilities. All kinds of endpoints should be considered, not just desktops and laptops, but also servers, virtual servers, containers, mobile phones, and IoT devices.

Application security starts with secure coding practices. Nevertheless, additional security mechanisms are needed and when deployed can help protect apps from attacks. Defenses at the application layer may include protocol gateways, reverse proxies, API gateways, and Web Application Firewalls (WAFs). CASB and CWPP solutions are useful for cloud hosted applications.
Databases, Big Data systems, data lakes, and data analytics tools must also be considered. Databases have built-in security constructs that must be employed to control access and protect against sabotage. SQL database security is well established but can be harmonized with enterprise security policies using SQL proxies and API security gateways. Big Data tools and related storage units require a mix of application, network, and cloud security tools for proper coverage.

Last but certainly not least is identity. We have heard for years that “Identity is the new perimeter”. This means that Identity and Access Management (IAM) systems play a critical role in the overall security architecture. Traditional security perimeters have become more porous over the years to allow higher level traffic to communicate directly with business or mission-critical applications. Digital identity is what allows for better protection of all resources along the path from “outside” to “inside”, by enforcing strong authentication and granular authorization. Thus, IAM concepts, systems, and controls must pervade all digital environments.

SOAR systems can be fed by all these kinds of security solutions, although mostly indirectly through the aforementioned SIEMs. Most SOARs can take in telemetry via APIs or in CEF and syslog format for those that also function as SIEMs. SOAR systems generally have OOTB connectors (software configurations and code in the form of packaged API calls) to facilitate data collection from upstream sources. In some cases, analysts need access to full packet captures, so NetFlow and PCAP are supported by a few vendors. In those cases, vendors have appliances that can connect on SPAN/TAP ports on network devices to achieve full packet capture.

The orchestration aspect of SOAR involves not only the collection of telemetry from these different sources, but also initiating a workflow, opening cases and tickets where appropriate, and correlation and enrichment of event information. Many large organizations, especially the type looking for SOAR systems, have IT Service Management (ITSM) Suites that dispatch and track activities in the form of tickets. SOAR solutions have case management capabilities by design, but they must also interoperate with existing ITSM solutions. For example, a ransomware attack will generate alerts from one or more endpoints and possibly network monitoring and data storage monitoring systems. SOAR’s job is to distinguish between related and unrelated events across all connected systems, assemble it coherently, enrich the event information by acquiring additional intelligence about observed entities (files, URLs, IP addresses, user accounts, etc.), create and/or coordinate tickets with ITSMs, with the goal of assisting human analysts and/or taking pre-programmed responses in playbooks.

Enrichment of event data can be facilitated by SOAR systems by the automatic collection of additional

forensic evidence on-site, such as outputs of EPP scans, obtaining non-standard log files, memory dumps, etc. Some vendor solutions can kick off somewhat automated threat hunts (looking for IOCs across multiple nodes in an environment) and add the results to preliminary investigation. SOAR solutions should also be able to generate queries to threat intelligence sources based on suspicious items and patterns observed from upstream telemetry. Some vendors have extensive threat intelligence capabilities which are utilized by their SOAR solutions. External threat intelligence sources may and ideally should be used to supplement internal threat intel sources. Examples of threat intelligence content include IOCs (files, hashes, IPs, URLs, and so forth), compromised credential intelligence, device intelligence (often from Mobile Network Operators [MNOs]), and domain/file/IP/URL reputation information. Ideally SOAR solutions will accomplish all the foregoing actions automatically prior to or while alerting a human analyst.

When an analyst is alerted and assigned a case, all pertinent information related to the event should be constructed and presented by the SOAR platform to the analysts for their investigation. The SOAR platform should package information coherently, with descriptions and recommendations for actions.

Most SOAR vendors adhere to the paradigm of a playbook. Playbooks typically address common security scenarios and can be triggered either by manual analyst action or automatically if allowed by policy and supported by the vendor. Examples of security events that may trigger playbooks are phishing, malware, ransomware, failed login attempts, excessive or abnormal use of privileged credentials, prohibited communication attempts, attempts to access unauthorized resources, file copying or moving, attempts to transfer data using unauthorized webmail providers, attempts to transfer data to blocked IPs or URLs, unusual process launches, unusual application to network port activities, unusual network communication patterns, and so on.

The end goal of SOAR is being able to automate incident responses among the various security systems. To this end, SOAR platforms often support dozens to hundreds of playbook scenarios and offer hundreds to thousands of possible incident response actions.

Cybersecurity and IAM vendors have increasingly been exposing functions of their products and services via APIs, such as reporting, querying, workflow integration, and critical commands. The following are examples of functions by system type that many SOAR products allow the invocation of programmatically:

Email gateways

- Quarantine/delete email identified as having malicious content or content in violation of policy

EPP/EDR

- Terminate processes
- Delete files
- Get device info
- Isolate nodes

- Pull forensic data
- Hunt for Indicators of Compromise (IOCs)
- Lookup domain, file, or IP address reputation
- Start EPP scans on remote nodes
- Reboot a device
- Rollback a device configuration to last known good state

Firewalls, IDS/IPS, routers, switches, NDR, and VPNs

- Block traffic by port
- Block traffic by IP address / range
- Isolate nodes

IAM

- Get user info
- Suspend/delete user
- Force step-up authentication event

IaaS

- Enable/disable users
- Add/remove tags (such as in EC2)
- Start/stop instances

ITSM

- Get ticket info
- Create/update tickets
- Reassign tickets
- Close tickets

SIEM

- Execute queries

Web gateways and proxies

- Block traffic by IP address or URL

The preceding is a list of abstracted high-level actions. The actual syntax and parameters passed over APIs differs between products, which is one of the many challenges SOAR platform vendors face in building their solutions. SOAR solutions that have connectors for large numbers of security products have invested significant effort in developing them. Consequently, the more security connectors a SOAR platform can offer, the more likely that product can fit in a customer's environment and deliver real value for security analysts. However, having a large number of connectors is not a primary determinant in tools choice; what matters most is finding the SOAR solution that has the specific connectors your organization needs.

1.1 Market Segment

The SOAR market, while still far from reaching full maturity, already has a reasonably well-established terminology and core set of capabilities. The term "SOAR" itself is already embraced by many vendors.

Some vendors in the market started out with a mission to address what they saw as missing functionality in the broader cybersecurity market. These startups may have gone through several rounds of funding and grown a sizable customer base. Furthermore, some of the bigger specialty startups in the SOAR market have been acquired by large cybersecurity stack vendors who were desirous to add these types of capabilities to their already extensive suites of products and services. In other cases, SOAR has been an outgrowth to complementary product offerings (most commonly SIEM) at some of the mid-tier vendors in the market.

Customers in the SOAR market tend to be somewhat larger SMBs, enterprises, and government agencies. Organizations that have established IT security departments, especially those with SOCs, are the most likely to see a need for SOAR. SMBs and some enterprises that are either outsourcing IT functions or adding security capabilities but not adding staff are turning to MSSP options that have SOAR.

The SOAR market is valid globally, but the greatest uptake has been in North America, followed by Europe. We expect to see more organizations across the world adding SOAR to their cybersecurity portfolios in the years ahead. SOAR as an outsourced function provided by MSSPs is also likely to grow in popularity.

One of the reasons that SOAR may be slower to be adopted outside of North America is the paucity of support for cybersecurity vendors outside the US. Most of the connectors built for SOAR products are for prominent American vendors. The vast majority of SOAR vendors do not have support for products of the large cybersecurity vendors that are headquartered in EU and APAC.

1.2 Delivery models

SOAR solutions often require complex deployment models. In most cases, on-premise components must be implemented, including software agents for upstream security systems from which telemetry will be gathered, and appliances and/or virtual appliances that serve as collection, analysis, operational, and management nodes for the SOAR solution.

SOAR systems also generally provide support for various cloud hosted environments such as IaaS and PaaS, which requires agents or images to be installed or the use of customized APIs. Some support specific SaaS applications as well.

In addition to APIs and connectors for security tools, SOAR platforms have user interfaces for administrators and analysts. Some vendors offer this as a capability on the components installed on-premises and others offer it as a cloud-hosted service.

Few SOAR vendors offer managed services whereby they collect and examine telemetry from customers, and then either automatically or, on the customer's behalf, execute incident response actions from playbooks. However, Managed Security Service Providers (MSSPs) license SOAR platforms from the major vendors and operate them for clients.

1.3 Required capabilities

Broadly speaking, there are three major concentrations of technical capabilities within SOAR solutions.

Security data collection, correlation and enrichment: a SOAR platform can collect historical and real-time security telemetry either on its own or ingest security events from a SIEM solution. If necessary, the data should be enriched with additional business context and forensic information, external threat intelligence, or other data sources according to established workflows.

Security Orchestration and Automation: a SOAR platform should implement comprehensive workflow management capabilities to ensure that tasks across multiple environments and security tools can be efficiently coordinated. Whenever possible, repetitive parts of these workflows should be automated to free the analyst's time for more creative tasks. For manual steps, intelligent guidance and decision support capabilities are a major plus.

Incident Response and mitigation: for identified security incidents, a SOAR platform should be able to offer a range of predefined resolutions: ranging from simple actions like creating a ticket for manual processing or quarantining compromised nodes to more sophisticated playbooks that coordinate response processes across multiple systems and departments: from IT to GRC to legal and public relations. For IR operations, the availability of connectors and configurable APIs and specific collections of actions per system type are paramount concerns for those implementing SOAR.

Evaluation Criteria Key Features

- Telemetry collection: the ability to collect potential security event information from a broad range of systems. Pre-configured connectors are ideal in most circumstances. The ability to accept feeds and formats and perform queries using CEF, CSV, OpenDXL, osquery, REST APIs, and syslog is optional and mainly seen in SOAR products which have arisen from SIEMs.
- Correlation: once ingested, effective SOAR solutions must parse large volumes of data from different sources and assemble related bits of information into a package that can be evaluated by and acted upon by human and AI/ML processes. ML enhanced detection and selection algorithms are preferred and, in most cases, necessary to adequately handle the volumes of telemetry in large organizations. Some vendors package User Behavioral Analysis (UBA) with their SOAR platforms so they can add historical insights to current event data. This type of analysis generally relies upon different subsets of ML detection algorithms specific for UBA. The correlation process must often be supplemented with enrichment of acquired data.
- Enrichment: Both known IOCs and suspicious items such as files, process launches, registry entries, IPs, URLs, etc. may percolate up from underlying security systems or be identified as IOCs or at least suspicious by an upstream SIEM or by the SOAR system itself. SOAR solutions can automate the collection of threat intelligence and querying of 3rd-party sources regarding these suspicious items associated with a case. The SOAR solution then packages the collected intelligence for analyst review.
- Workflow orchestration, automation, and case management: SOARs are designed to facilitate rapid investigations and responses to possible security incidents. While telemetry collection, preliminary analysis, and information enrichment can happen prior to analyst involvement, SOARs must provide ergonomic interfaces for human analysts at the point where their input is needed. Generally speaking, SOARs should by design seek to eliminate repetitive and menial tasks that analysts have to do to increase the speed of processing and successful resolution of security incidents. Thus, SOARs must offer logical and flexible workflow automation capabilities in the context of case management. SOARs are expected to perform evidence collection and triage; and then be able to create and manage cases. SOARs must be able to interoperate with all the relevant tools within the customer's security portfolio, allowing real-time forensic analysis, querying of remote systems, and execution of investigative actions. For this reason, SOARs generally must work with ITSM and ticketing applications and direct (often asynchronously) the interactions between the other components of the customer's infrastructure. While SOARs ship with pre-defined workflows, they should be customizable to meet individual customer needs and extensible to enable customers to add new security tools to their environments as needed. Extensibility is the key to future-proofing

SOAR implementations.

- Incident response: the ability of a SOAR system to respond to incidents depends on the variety of connectors and quality of implementation of those connectors. The types of systems with which SOAR must interoperate include email/web gateways, EPP/EDR, firewalls/network security devices and services, IAM, IaaS instances, ITSM, and SIEM. Incident response capabilities should also extend to non-IT processes where possible. For example, SOAR playbooks can often provide guidance and the ability to automate communications about ongoing incidents if defined. Most vendor platforms come with some pre-defined playbooks for common situations. Playbooks should be customizable and support conditional logic for automated incident responses.

We are not covering solutions that only focus on a specific type of IT environment or a subset of security information (for example, firewall orchestration or network traffic monitoring). We expect full-featured SOAR products to be able to serve as comprehensive and extensible security analytics platforms for SOCs.

We understand that most existing SOAR offerings have evolved from previous-generation, more specialized SIEM, incident response or security automation solutions, and their core capabilities may vary substantially depending on their origin. In other cases, threat intelligence platforms have begun to metamorphose into SOARs. Regardless of their genesis, we expect reasonably mature solutions to have balanced capabilities across all core functional areas.

The criteria evaluated in this Leadership Compass reflect the varieties of use cases, experiences, business rules, and technical capabilities required by KuppingerCole clients today, and what we anticipate clients will need in the future. The products examined meet many of the requirements described above, although they sometimes take different approaches in solving the business problems.

When evaluating the products and services, besides looking at our standard criteria of

- overall functionality and usability
- internal product/service security
- size of the company
- number of tenants/customers and end-user consumers
- number of developers
- partner ecosystem
- licensing mod

We have also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other offerings available in the market. Features that are considered innovative are listed below.

- Support for standards such as STIX, TAXII, and CyBox.
- Contributions to the Open Cybersecurity Alliance (OCA), an industry association sponsored by OASIS for the promotion of interoperability between products in the SOAR space.
- SOAR functionality across multi-cloud environments.
- Well-documented APIs that allow customers to extend SOAR connectivity to other solutions.
- Multi-Factor Authentication (MFA) and identity federation for customer admins and analysts.
- Workflows and playbooks that address communications and PR aspects of major security incidents.
- Large numbers of built-in connectors to facilitate deployment alongside a variety of other security tools.

Please note that we only listed a sample of features, and we consider other capabilities per solution as well when evaluating and rating the various SOAR solutions.

2 Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Figure 1: The Overall Leadership rating for the SOAR market segment

Palo Alto Networks, IBM, D3 Security, Exabeam, and ServiceNow are the overall leaders in this edition of the Leadership Compass on SOAR. Each of their products in this market show a high degree of product completeness, innovation, and market share in this evolving and growing field. Both IBM and Palo Alto have made strategic technological acquisitions which fit well with their strong cybersecurity portfolios. D3 Security and Exabeam have focused on security operations management since they began, and their SOAR products reflect expertise in this area. ServiceNow is a large IT service management vendor with a strong

security operations platform. The close alignment between ITSM and security as demonstrated by ServiceNow's excellence is possibly a sign of future trends in these areas.

Rather tightly grouped at the top of the Challenger section are DF Labs and Siemplify. Both are specialists in the field.

In the central section of the Challenger block we find ThreatConnect, followed by ManageEngine, Micro Focus, and SIRP. ThreatConnect has entered the SOAR market by way of their high-quality curations of threat intelligence business. SIRP is a SOAR specialist with a focus on risk-based security operations. Micro Focus recently added SOAR to their product portfolio through the acquisition of ATAR. ManageEngine is growing SOAR functionality organically and adding it to their stack of IT and security solutions.

Overall Leaders are (in alphabetical order):

- D3 Security
- Exabeam
- IBM
- Palo Alto
- ServiceNow

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of service features and the overall capabilities of the various services.

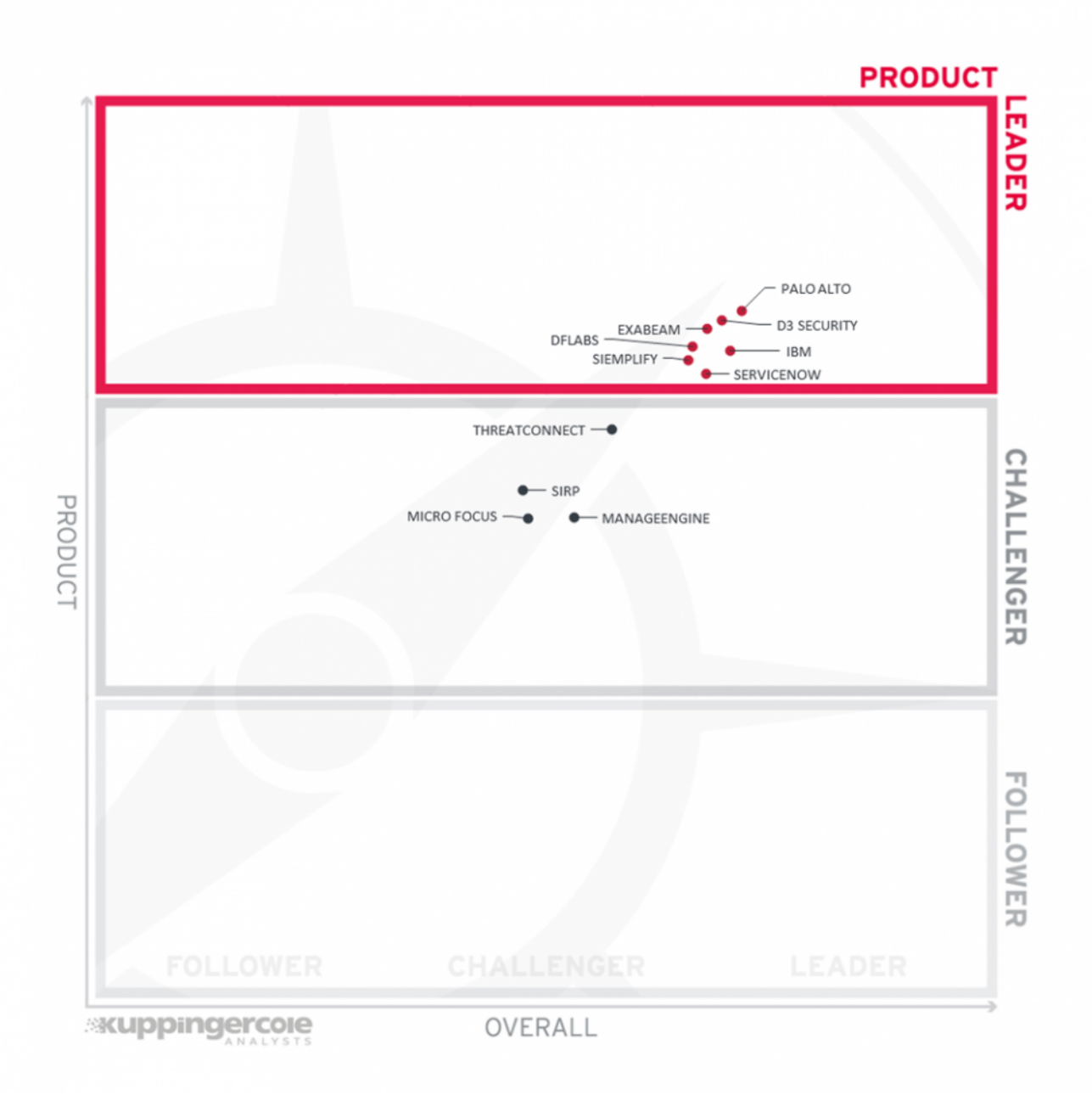


Figure 2: Product Leaders in the SOAR market segment

Product Leadership is where we examine the functional strength and completeness of services.

Palo Alto is at the top of the Product Leadership chart as a result of the Demisto acquisition plus their threat intelligence capabilities. Many of the standalone SOAR products are also leaders here: D3 Security, DF Labs, and Siemplify. IBM with their full-service suite of security solutions, Exabeam with their full security management platform, and ServiceNow with their well-integrated security ops platform round out the Product Leaders.

ThreatConnect appears at the top of the Challenger section, followed by SIRP, ManageEngine, and Micro

Focus. ThreatConnect is leveraging their strengths in threat intel management and have concentrated on the orchestration part of SOAR.

SIRP is a startup specialized in SOAR. ManageEngine is adding SOAR functions to their suite. Micro Focus recently picked up ATAR, which itself was a relatively new SOAR product, and will integrate it into their ArcSight product.

Product Leaders (in alphabetical order):

- D3 Security
- DF Labs
- Exabeam
- IBM
- Palo Alto
- ServiceNow
- Siemplify

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new ¬-releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

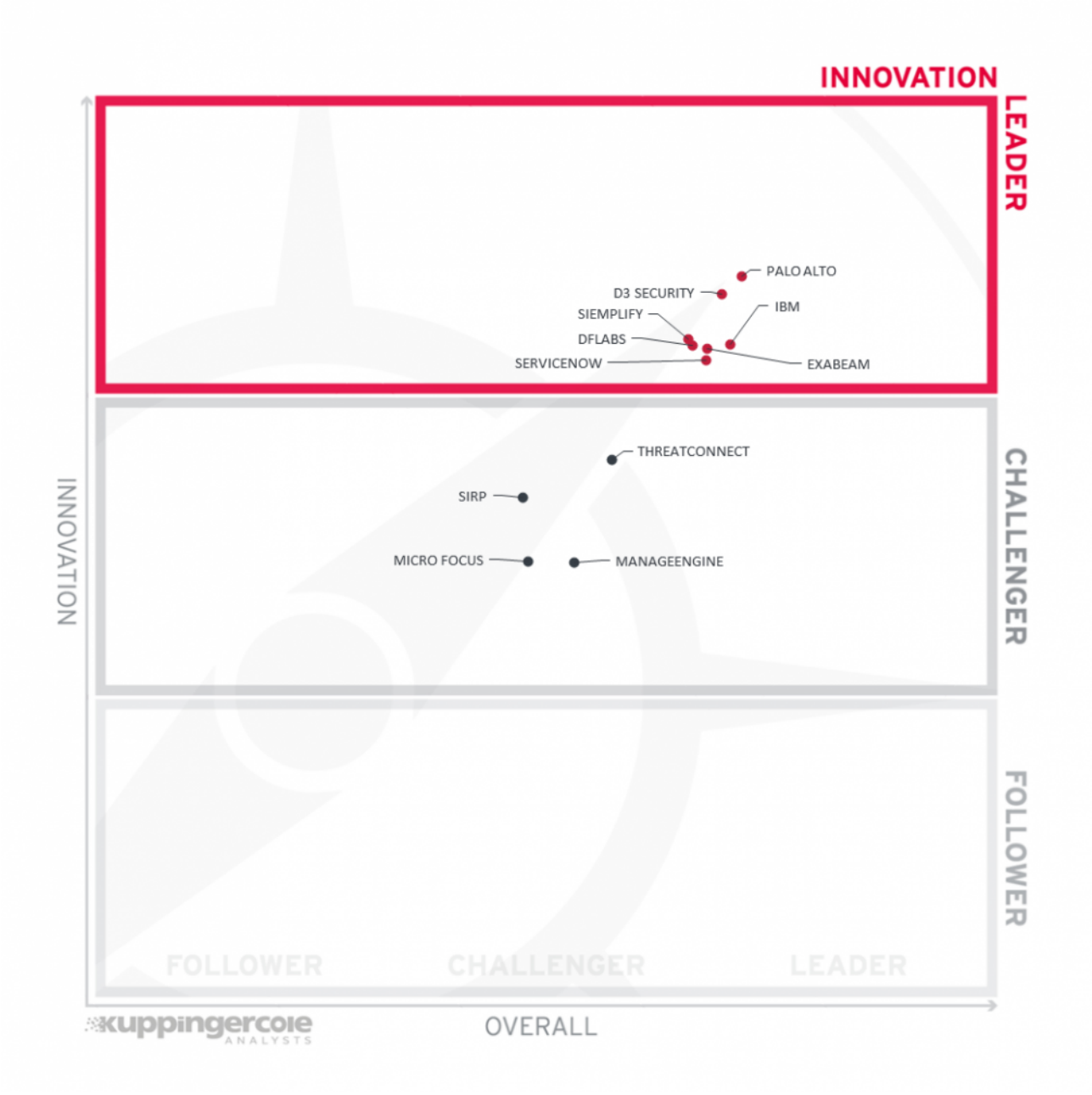


Figure 3: Innovation Leaders in the SOAR market segment

The Innovation Leaders are Palo Alto, D3 Security, Siemplify, IBM, DF Labs, Exabeam, and ServiceNow. All are SOAR specialists (or were if you consider Demisto prior to the Palo Alto acquisition). Innovators in the SOAR market are those with the most cutting-edge features and use of the latest technology.

ThreatConnect is the top challenger in innovation. SIRP is above the midpoint in the Challenger space. ManageEngine and Micro Focus are near the center of the Challenger area. Each have strengths and areas of innovation. This is a rapidly evolving discipline, and we expect that each of these will continue to add ground-breaking features in the months ahead.

Innovation Leaders (in alphabetical order):

- D3 Security
- DF Labs
- Exabeam
- IBM
- Palo Alto
- ServiceNow
- Siemplify

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

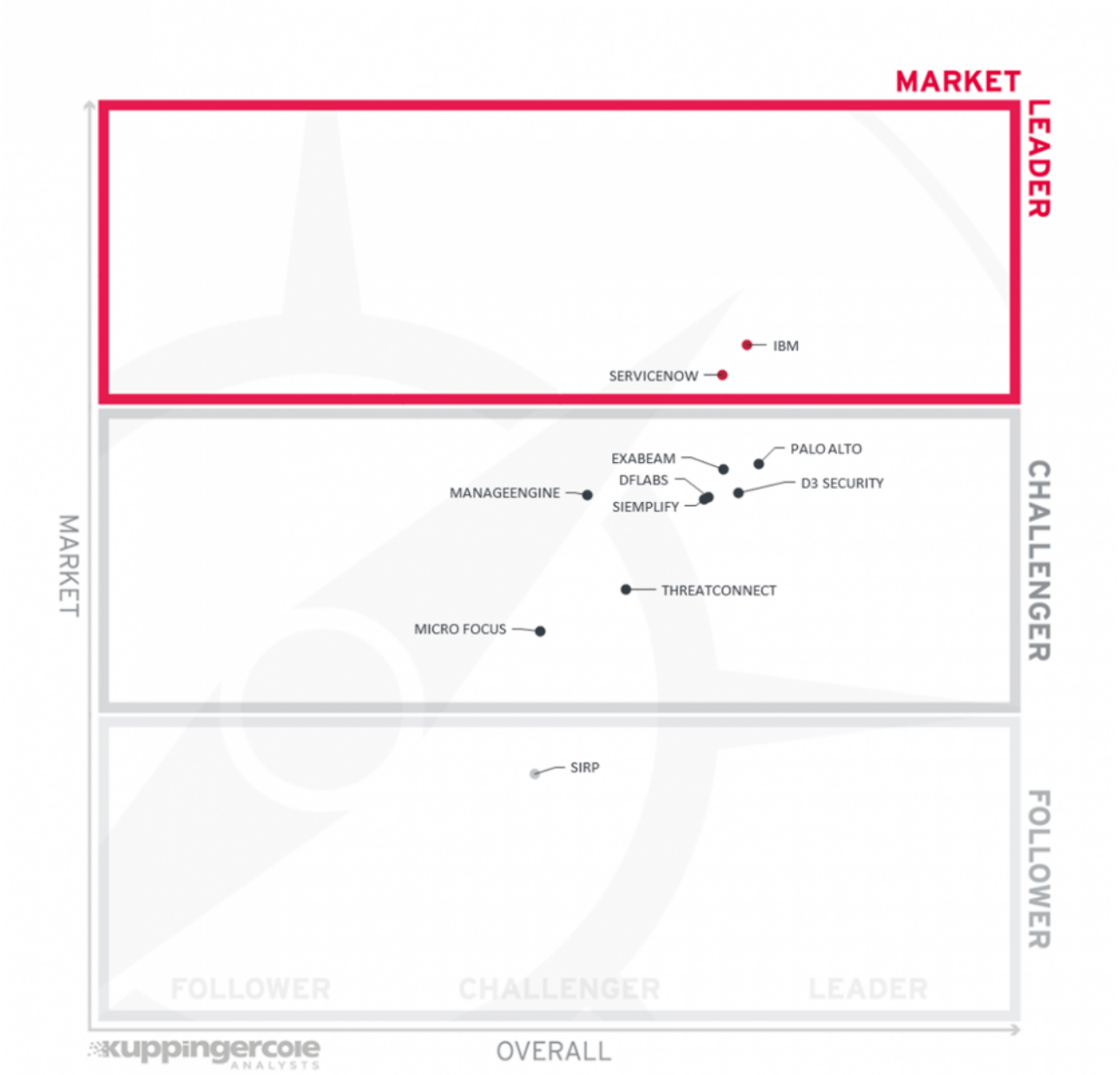


Figure 4: Market Leaders in the SOAR market segment

IBM and ServiceNow are the Market Leaders. Both have not only good SOAR products that many customers are using, but they also have financial strength, geographic distribution of customers and partner, and extensive ecosystems of system integrators.

The top Challengers in the Market are Palo Alto, Exabeam, ManageEngine, D3 Security, DF Labs, and Siemplify. As the SOAR market itself grows, we imagine that these could become Market Leaders too. The lower half of the Challenger block has ThreatConnect and Micro Focus.

SIRP is at the top of the Follower section, which is not unexpected given the recency of their market entry.

Market Leaders (in alphabetical order):

- IBM
- ServiceNow

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

3.1 The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership

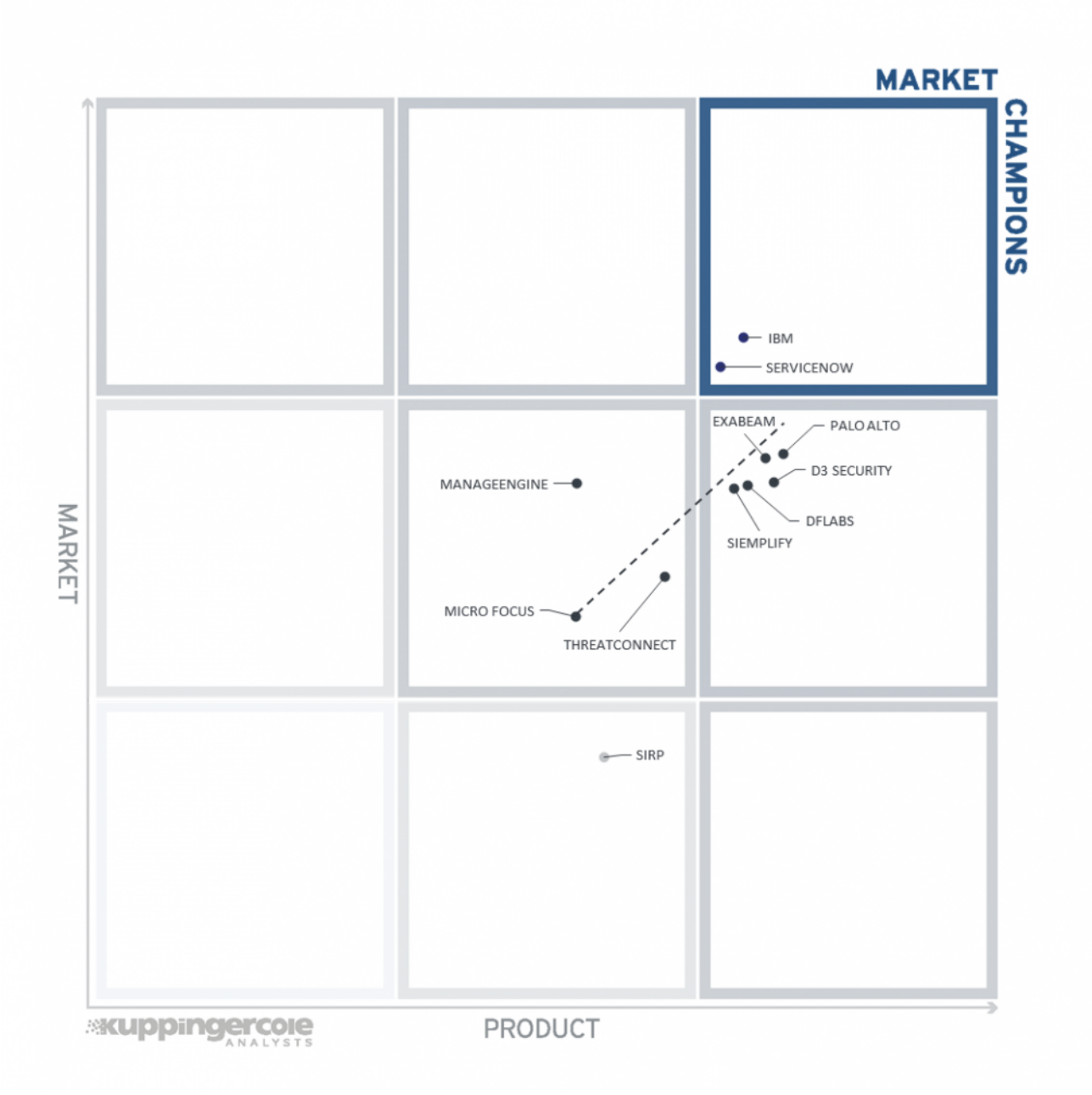


Figure 5: The Market/Product Matrix.

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership.

In this view we find IBM and ServiceNow in the top right box as Market Champions. Both companies have strong SOAR products in their suites and corresponding market position.

D3 Security, DF Labs, Exabeam, Palo Alto, and Siemplify are in the right center but below the line. These are strong products. All the vendors below the line are underperforming in terms of market share. However,

we believe that this means each has a chance for significant growth.

ManageEngine, Micro Focus, and ThreatConnect are in the center box. They are performing nearly as expected in the market for their relative product strength.

As a newcomer with a good product, SIRP is in the lower center below the line. They have room to grow.?

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

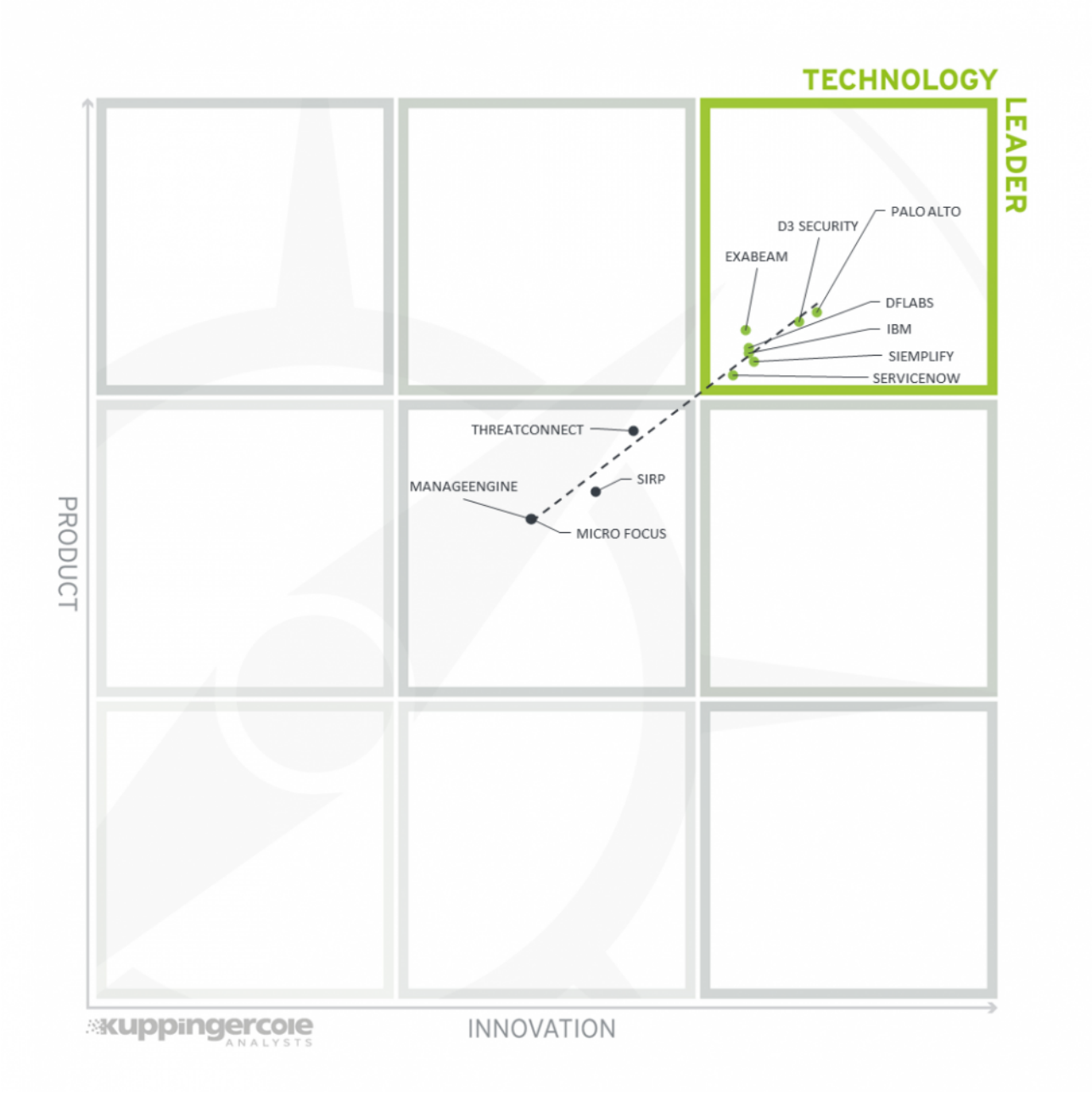


Figure 6: The Product/Innovation Matrix.

Vendors below the line are more innovative; vendors above the line are, compared to the current Product Leadership positioning, less innovative.

The Technology Leaders in this first iteration of the Leadership Compass on SOAR are Palo Alto, D3 Security, Exabeam, DF Labs, IBM, Siemplify, and ServiceNow. All their positions show close adherence to the line, meaning that Product Leaders also happen to be Innovation Leaders. Innovation is necessary to stay ahead in SOAR.

In the center, we find ThreatConnect, SIRP, ManageEngine, and Micro Focus. Again, the placement here

reveals that product completeness and innovation are directly correlative.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

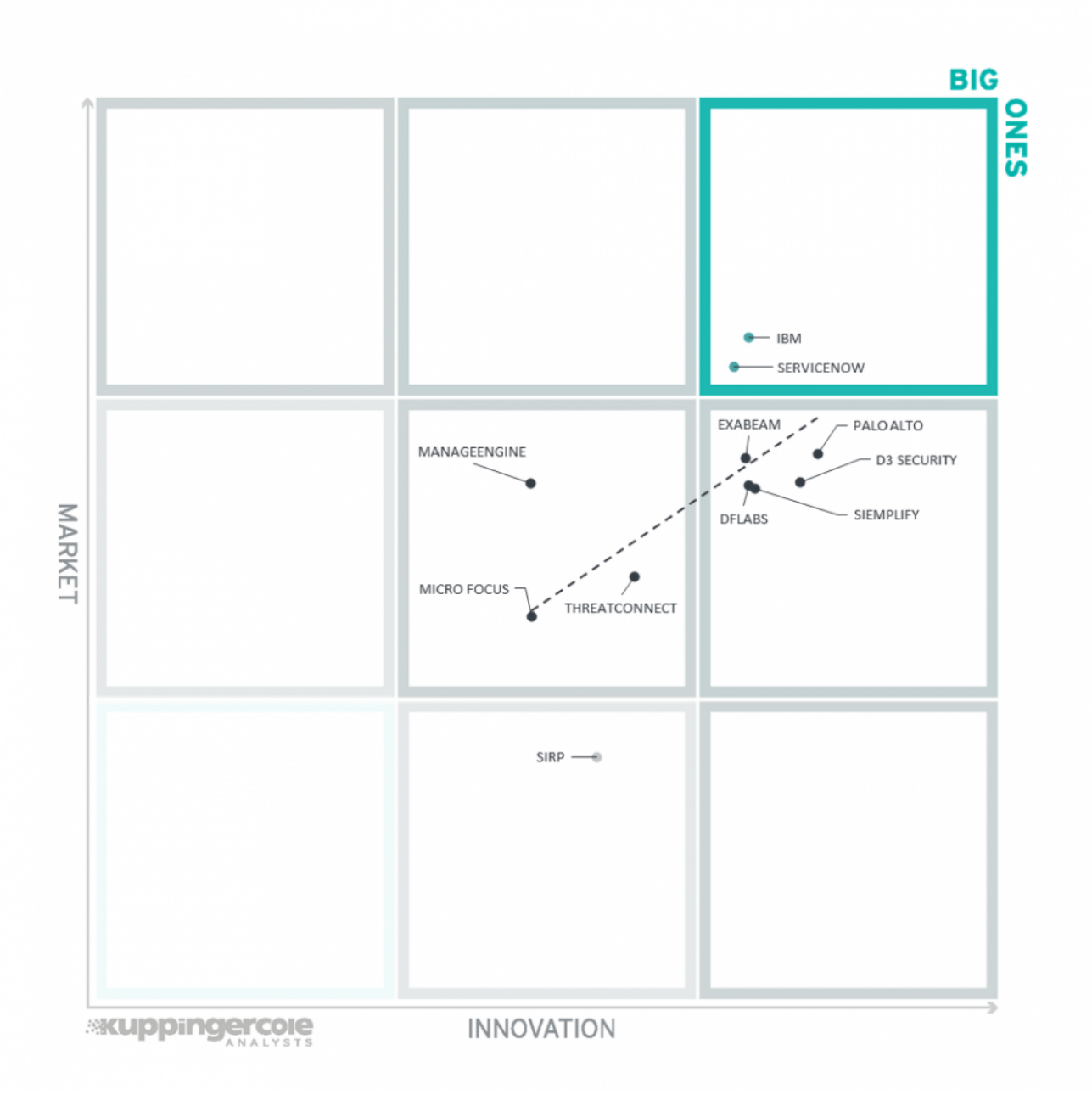


Figure 7: The Innovation/Market Matrix.

This chart shows how innovation is received in the marketplace.

IBM and ServiceNow are the Big Ones in SOAR. They have the intersection of sizable market presence as well as sufficient innovation in their offering.

In the center right, we find Palo Alto, Exabeam, D3 Security, DF Labs, and Siemplify. They have innovative products that could see an increase market share in the months ahead. In the center box, ManageEngine, ThreatConnect, and Micro Focus show an even mix of innovation and position in the market.

SIRP is in the bottom center. They have room to pick up new customers as they evolve their SOAR product.

4 Products and Vendors at a glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on SOAR. This overview goes into detail on the various aspects we include in our ratings, such as security, overall functionality, etc. It provides a more granular perspective, beyond the Leadership ratings such as Product Leadership, and allows identifying in which areas vendors and their offerings score stronger or weaker. Details on the rating categories and scale are listed in chapter 7.2 to 7.4.

4.1 Ratings at a glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Product	Security	Functionality	Interoperability	Usability	Deployment
D3 NextGen SOAR	●	●	●	●	●
DFLabs	●	●	●	●	●
Exabeam Security Management Platform	●	●	●	●	●
IBM Security QRadar, Advisor with Watson, Resilient SOAR Platform	●	●	●	●	●
ManageEngine Log360	●	●	●	●	●
Micro Focus ATAR	●	●	●	●	●
Palo Alto Networks Cortex XSOAR	●	●	●	●	●
ServiceNow Security Incident Response	●	●	●	●	●
Siemplify Security Operations Platforms	●	●	●	●	●
SIRP	●	●	●	●	●
ThreatConnect	●	●	●	●	●
Legend		● critical	● weak	● neutral	● positive ● strong positive

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
D3 Security	strong positive	positive	neutral	positive
DFLabs	strong positive	positive	neutral	neutral
Exabeam	strong positive	positive	positive	neutral
IBM	strong positive	strong positive	strong positive	strong positive
ManageEngine	weak	positive	positive	positive
Micro Focus	neutral	weak	positive	strong positive
Palo Alto Networks	strong positive	positive	strong positive	strong positive
ServiceNow	strong positive	strong positive	strong positive	strong positive
Siemplify	strong positive	positive	neutral	neutral
SIRP	neutral	weak	weak	weak
ThreatConnect	positive	neutral	weak	neutral
Legend	critical	weak	neutral	positive	strong positive

In Innovativeness, this rating would be applied if vendors provide none or very few of the more advanced features we look for, such as support for MFA for admins and analysts, support for threat information exchange standards, inclusion of communications in playbooks, etc.

This rating would be applied for Market Position in the case where vendors only have regional visibility. Usually the number of existing customers and size of deployments are also comparatively small in these cases.

In Financial Strength, critical ratings may be given in the case of a lack of information about financial strength, for startups with low seed funding and/or little evidence of revenue, or for vendors with a very limited customer base. This rating itself doesn't necessarily imply that the vendor is in a critical financial situation; however, the potential for massive investments for quick growth appears to be limited. On the other hand, it's also possible that vendors with better ratings might fail and disappear from the market.

5 Product/service evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the LC SOAR, we look at the following 8 categories:

- Telemetry Collection
  SOARs primarily draw input from SIEMs; thus, having connectors for a range of SIEM platforms is needed. Moreover, SOARs may support standards such as CEF, OpenDXL, osquery, SNMP, and syslog; and direct collection of telemetry from upstream sources via pre-configured connectors. Some solutions in this space support full packet capture (NetFlow, PCAP, etc.) This category measures the availability of SIEM connectors and support for direct collection of security event data.
- Enrichment
  Enrichment is the process of adding intelligence and context to security events and incidents. SOAR platforms may pull threat intelligence from within their own network but should also support subscriptions to and queries to 3rd-party threat intelligence sources. This measures the quantity and quality of threat intelligence sources available to each vendor's SOAR solution.
- Case Management
  This metric evaluates how well the SOAR solution automatically processes enriched event information and presents it to analysts for action. Case management also includes automation of preliminary analysis, background triage, and interoperability with ticketing systems.
- IAM
  This metric shows the quantity of connectors available for and depth of interoperability with IAM systems including IDaaS. For more information on IAM interoperability requirements for SOAR, see chapter 1.
- Cloud
  This metric shows the quantity of connectors available for and depth of interoperability with IaaS, PaaS, and SaaS solutions. This also includes SOAR vendor management support. For more

information on cloud services interoperability requirements for SOAR, see chapter 1.

- Email/Web
  This metric shows the quantity of connectors available for and depth of interoperability with email and web gateways/proxies. For more information on email and web gateway interoperability requirements for SOAR, see chapter 1.
- EPP/EDR
  This metric shows the quantity of connectors available for and depth of interoperability with EPP and EDR solutions. For more information on EPP/EDR interoperability requirements for SOAR, see chapter 1.
- Network
  This metric shows the quantity of connectors available for and depth of interoperability with network security solutions, encompassing firewalls, IDS/IPS, NDR, and VPNs. For more information on network security interoperability requirements for SOAR, see chapter 1.

The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some vendor services may have gaps in certain areas, while are strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities in all categories of SOAR technologies.

5.1 D3 Security

D3 Security was founded in 2003 in Vancouver. The company is privately held. D3's focus is on "intent-based SOAR", which uses attacker techniques to validate threats and disrupt the kill chain. Their NextGen SOAR can be deployed on-premise, and on both private and public cloud. D3 does not host a managed service, but 3rd-party MSSPs use their products. Licensing is per seat.

For telemetry collection, D3 has certified connectors for ArcSight, AWS Security Hub, Chronicle, Datadog Security Monitoring, Elasticsearch, FortiSIEM, Huntsman, IBM QRadar, LogRhythm, Microsoft Azure Sentinel, McAfee ESM, Proofpoint TAP, ProtectWise, Rapid7, RSA Netwitness, SentinelOne, Splunk ES, and SumoLogic. D3 can also ingest CSV, Syslog, and XML; and can query and communicate using OpenDXL, osquery, and REST APIs. D3 does not capture packets and does not provide agents.

For case management, D3 interoperates with BMC Remedy, Jira Service Desk, ServiceNow, and ZenDesk. D3 receives threat intel from and can query Cisco Umbrella, DomainTools, MaxMind, McAfee Threat Intelligence Exchange, Micro Focus Threat Central, MISP, ReversingLabs, ThreatQuotient, Palo Alto AutoFocus, Pulsedive, RiskIQ PassiveTotal, Symantec Global Intelligence Network, The Hive-Project, ThreatConnect, TruStar, VirusTotal, and Webroot. D3 supports STIX and TAXII.

D3 has a good assortment of connectors. For cloud management, they have integrations with AWS, Azure, BMC TrueSight, and DataDog; IAM connectors for Microsoft Active Directory and Okta; Cisco, Crowdstrike, Cylance, FireEye, Fortinet, Imperva, McAfee, Microsoft, MobileIron, Sophos, Symantec, Tanium, TrendMicro, and VMWare Carbon Black EPP/EDR solutions; and many network security connectors including Cisco, Checkpoint, F5, Forcepoint, Fortinet, Juniper, McAfee, Palo Alto, Symantec, Tufin, and ZScaler.

Events are mapped to MITRE ATT&CK. D3 offers pre-built and customizable playbooks. Automated response actions can be triggered by policies. The admin/analyst GUI is also customizable. D3 supports Yubikeys for 2FA and SAML for federated authentication.

D3 NextGen SOAR has good administrative security including 2FA and federation. Choosing the right SOAR product involves matching the tools you have deployed with what a SOAR vendor supports. D3 has connectors for a comparatively large number of other tools, and also supports all the right standards thereby enabling their customers to extend their solution as needed. Organizations looking for pure-play SOARs should put D3 Security on their RFP list.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

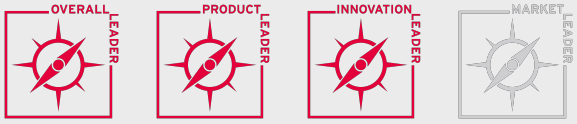
Strengths

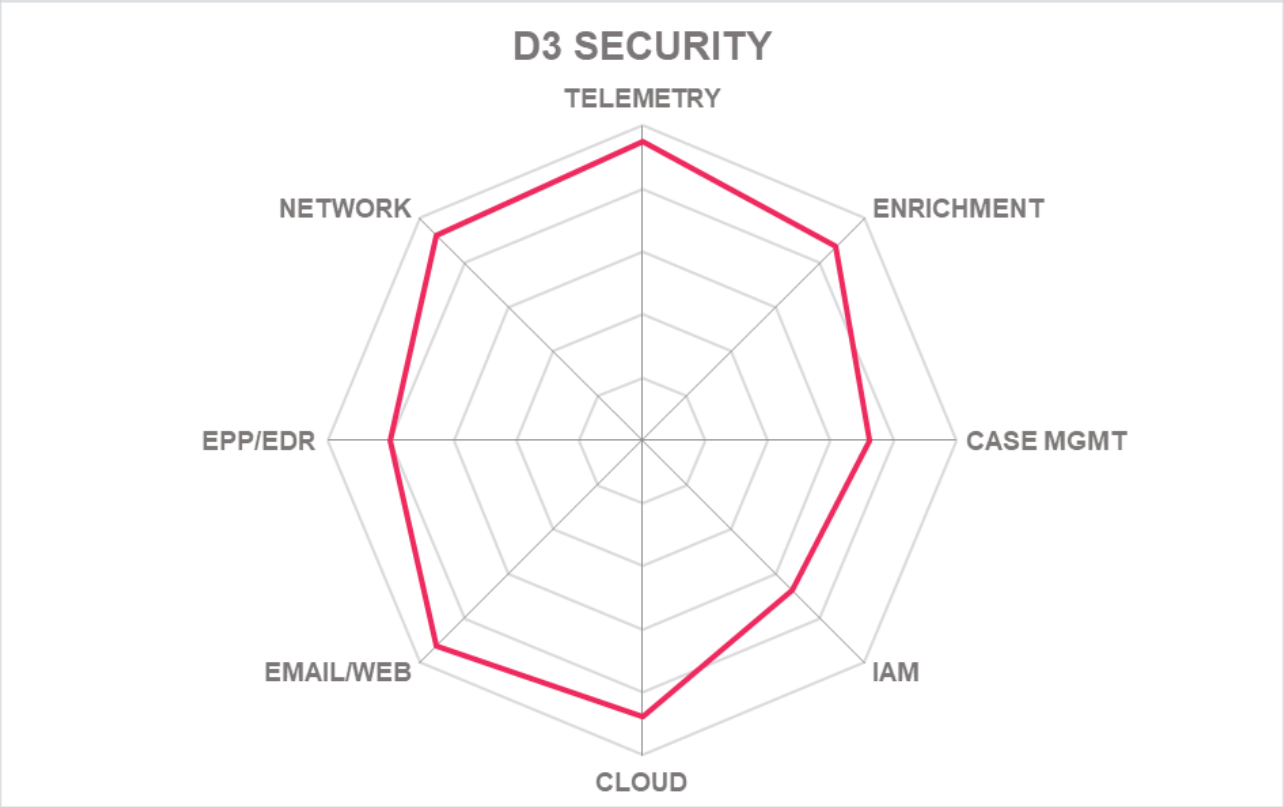
- 2FA & SAML for admin/analyst authentication
- Playbooks offer “no-code” and nested action capabilities
- Playbooks can be used for SecOps, IR, IT Dev/Ops, ICS/OT, physical security, and HR functions.
- MITRE ATT&CK and custom TTP mapping for inbound telemetry and analyst interfaces
- OpenDXL support

Challenges

- Missing support for popular EU based security vendor products
- Container and Kubernetes support is on the near-term roadmap

Leader in




D3 SECURITY
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.2 DFLabs

DFLabs was founded in Milan in 2004. They are a privately funded SOAR specialist now. They do not operate their software as a service, but they license it to MSSPs who run it for customers. IncMan SOAR is licensed by the number of admin/analyst users and number of deployed components.

IncMan has connectors for pulling event data from AlienVault, Elastic Stack, FireEye Helix, Fortinet, IBM QRadar, LogPoint, McAfee, MicroFocus ArcSight, Rapid7, RSA, Securonix, Solarwinds, Splunk, SumoLogic, and Syslog-NG. DFLabs supports APIs, CEF, and syslog. IncMan does not capture packets.

IncMan collects and prioritizes event information for analysts. For case management, it can integrate with BMC Remedy, CA Service Desk, Cherwell, ConnectWise, FreshDesk, Jira, McAfee, PagerDuty, and ServiceNow. Supported data enrichment sources include Cisco Umbrella, HackerTarget, Hexillion Domain Dossier, MaxMind, and Whois. Threat intel sources available are AbuseIPDB, AlienVault, Any.Run, Blueliv, Censys, Cisco, Cofense, DarkOwl, Digital Shadows, DomainTools, FireEye, HackerTarget, Hybrid Analysis, IBM X-Force, Kaspersky, KnowBe4, Lastline, McAfee, MISP, Palo Alto, PhishTank, Recorded Future, RiskIQ, Shodan, Sophos, Symantec, TheHive-Project, ThreatCrowd, ThreatConnect, ThreatMiner, TrendMicro, URLHaus, and Virus Total. DFLabs supports STIX and TAXII.

DFLabs has a good **assortment of connectors** offering deep API integration with many products. IncMan can execute granular actions in cloud environments including AWS, Microsoft AD, Azure, and Exchange/OneDrive/SharePoint, VMware vSphere, and Zoom. For endpoint platforms, IncMan can integrate with Carbon Black, Cisco, Crowdstrike, Cybereason, Cylance, FireEye, McAfee, and Symantec. DFLabs supports IAM integration via LDAP and Microsoft AD only. Supported network and email security solution integrations include Checkpoint, Cisco, Corelight, F5, Fidelis, FireEye, Fortinet, Gmail, Imperva, McAfee, Palo Alto, RSA, Symantec, Trend Micro, Tufin, and VMware.

IncMan SOAR ships with more than 100 runbooks (playbooks) covering basic scenarios including automated investigation and correlation steps. Customers can extend them or build new ones using their scripting language and conditional logic. Fully automated responses can be triggered which IncMan then uses to execute actions via APIs in the connected products. MFA for admins and analysts can be configured via the LDAP and/or AD connectors.

DFLabs' focus is on SOAR. They are a smaller vendor, headquartered in Europe but with a geographically well-distributed customer and partner base. IncMan ships with a good amount of connectors and runbooks compared to the market. DFLabs provides their Open Integration Framework to allow customers to extend their platform as needed. MFA can be configured but should be built in. Organizations looking for SOAR functionality, particularly those in Europe who are mindful about GDPR, should consider DFLabs for RFPs.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

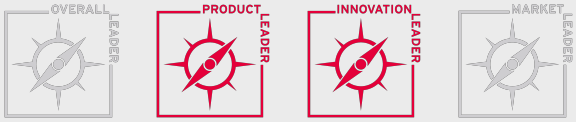
Strengths

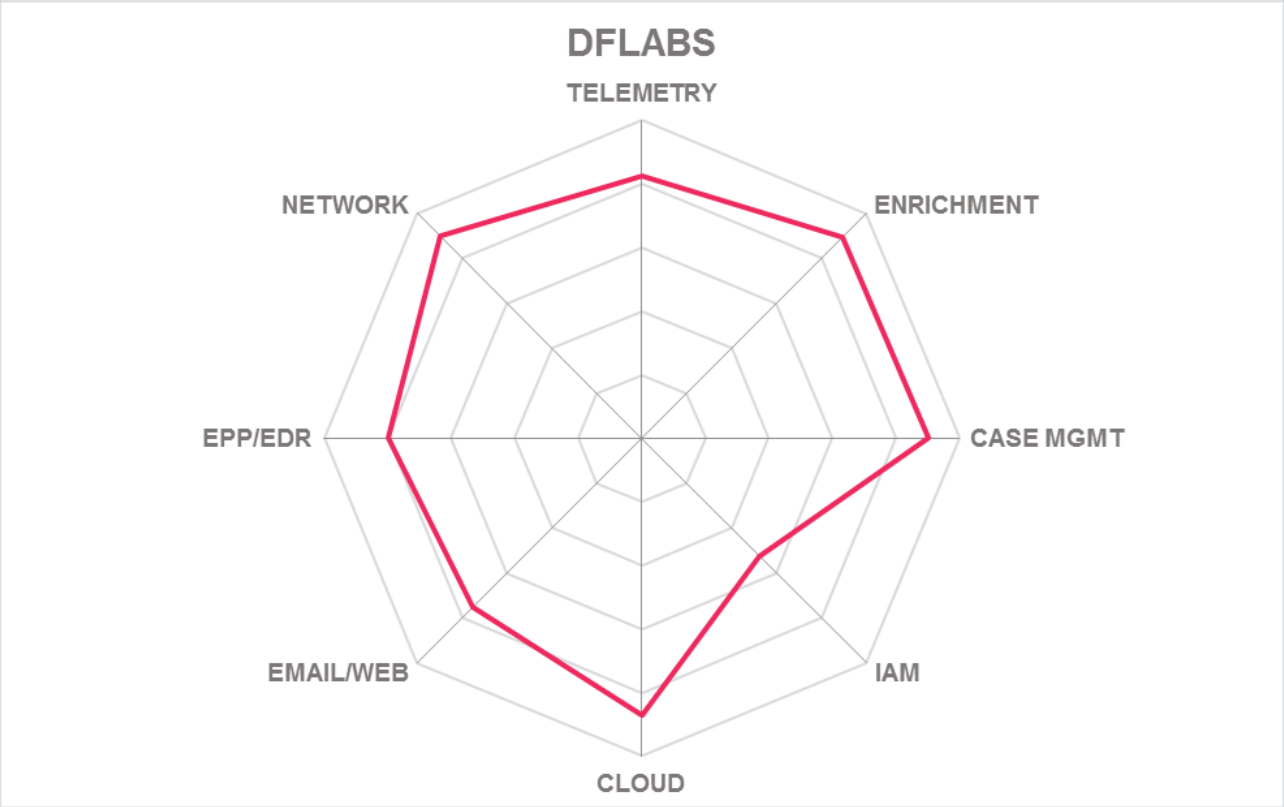
- SOAR specialist
- Extensive list of SIEMs supported
- Variety of different threat intel sources available
- Granular controls for cloud
- Support for IoT in platform
- OCA contributor and founding member

Challenges

- Covers some major endpoint security platforms, but misses a few significant EU headquartered vendors
- More IAM connectivity needed
- Built-in MFA options would be useful

Leader in




DFLABS
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.3 Exabeam

Exabeam was founded in 2013 in Silicon Valley. They are a late-stage, well-funded but still private security analytics company. Exabeam offers a fully integrated security analytics management platform, which encompasses UBA, next-gen SIEM, threat intelligence, as well as SOAR. Exabeam has a cloud-first strategy for management, hosting their solution as SaaS and allowing customers to run in AWS or GCP; but also offers hardware appliances for on-site deployments for customers who want them. Hybrid architectures are also supported. The solution is licensed by the number of users, not traffic or log volumes. Hardware installations incur additional licensing fees.

Exabeam itself is a SIEM, but can also augment ElasticSearch, IBM QRadar, LogRhythm, McAfee, MicroFocus ArcSight, Nitro, RSA, and Splunk SIEMs. Exabeam supports CEF and syslog formats. Exabeam does not natively capture packets, but can analyze NetFlow/PCAPs via integrations with Cisco, Corelight, FireEye, Snort, etc.

For ITSM, Exabeam has connectors for BMC Remedy, Jira, and ServiceNow. Exabeam can pull in threat intel from AlienVault, Anomali, Cisco Umbrella, DomainTools, Forcepoint, haveibeenpwned, IBM X-Force, IntSights, MaxMind, Palo Alto, Proofpoint, Recorded Future, ReversingLabs, RiskIQ, Shodan, ThreatConnect, ThreatQuotient, URLVoid, and Virus Total.

Exabeam has **many connectors**. For automated responses, Exabeam has deep integration with AWS, allowing granular control over instances. For IAM systems, Exabeam can disable/enable users in Microsoft Active Directory, CyberArk, Duo, and Okta. Exabeam can also delete malicious emails in Google Gmail, Microsoft Exchange, and SMTP servers. For endpoint security tools, Exabeam supports ops such as node isolation and executing scans (available functions vary by endpoint product, depending on what is exposed in their APIs) in Carbon Black, Cisco, Crowdstrike, Cylance, FireEye, McAfee, Microsoft Defender ATP, SentinelOne, and Symantec. At the network layer, Exabeam can block IPs on Checkpoint, Fortinet, and Palo Alto firewalls; detonate files/URLs in Cisco, Cuckoo, FireEye, and Palo Alto sandboxes; and query Rapid7 and Tenable for vulnerability management data.

Exabeam is aligned with MITRE ATT&CK, and analysts can even threat hunt based on TTPs and elements in the framework. A natural language query interface enables junior SOC analysts to become productive quickly. Exabeam provides built-in reports that cover regulatory compliance over areas such as GDPR, NERC CIP, PCI-DSS, SOx, etc. Exabeam supports federated authentication via Duo, Google, and Ping, allowing LDAP authentication to support additional methods such as SmartCards and CAC where required.

Exabeam positions their Security Management Platform as a replacement for SIEM systems and as an augmentation for legacy SIEMs, which includes SOAR capabilities. Exabeam attests/certifies with US FedRAMP, HIPAA/HITRUST, PCI-DSS, and SSAE 18 SOC 2 Type 2. Exabeam has a wide range of connectors for various data sources and security tools, enabling deep integration and automated responses. Their Security Management Platform exceeds expectations in terms of SOAR features and should be near the top of any organization’s SOAR RFP list.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

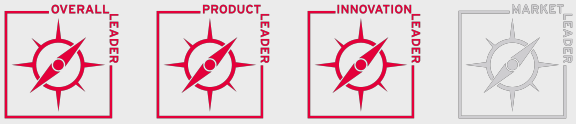
Strengths

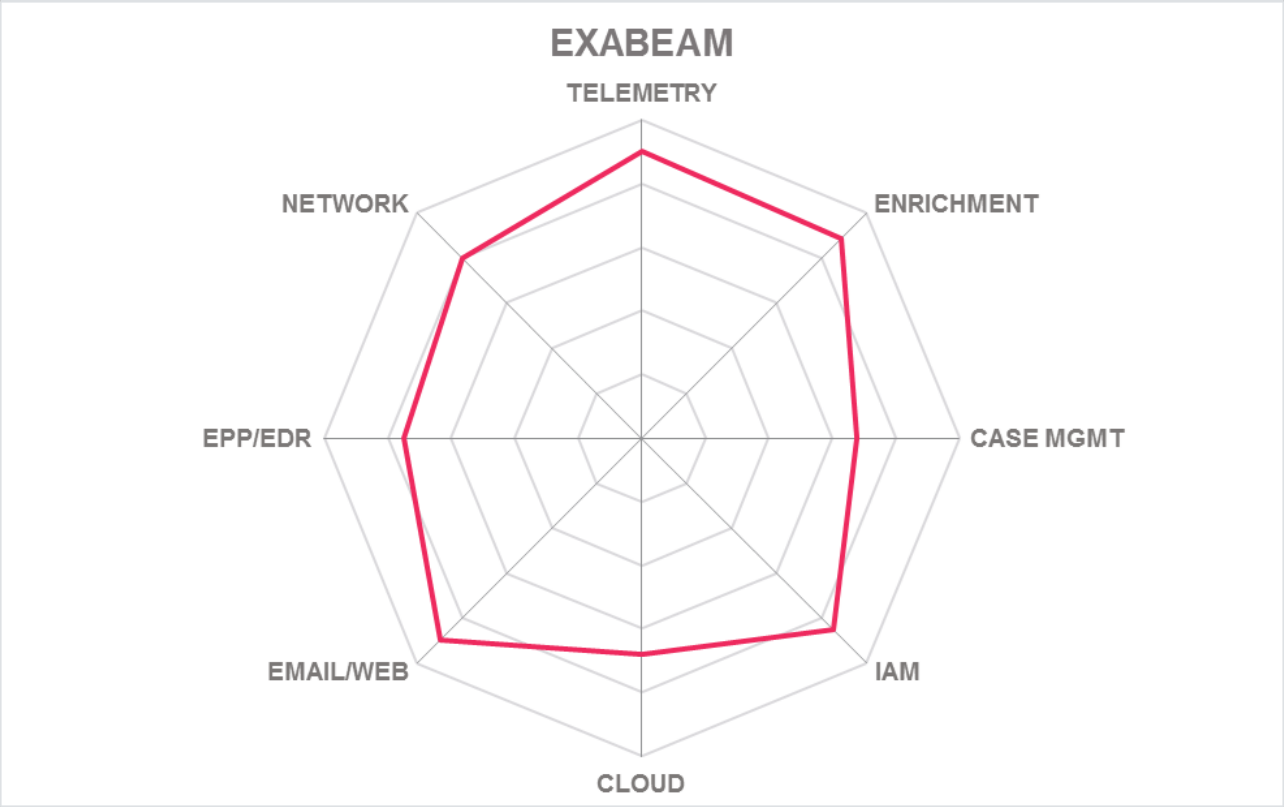
- Large variety of OOTB threat intel sources
- Above average number of connectors for security tools allows robust automatic responses
- Canned compliance reports
- Natural language query interface
- Search by MITRE ATT&CK TTP type

Challenges

- Missing integrations with some leading EU-based cybersecurity products
- More direct MFA options would be useful

Leader in




EXABEAM
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.4 IBM

IBM covers the SOAR technology area with the conjunction of three products listed above. IBM has a full security and identity management solutions, of which these are parts. QRadar, for instance, is a leading SIEM solution. The IBM solution can be deployed on-premises as appliances/virtual appliances and in AWS/Azure/GCP. IBM and MSSPs host this SOAR solution. For on-premise implementation, these three IBM products are licensed individually per server or by number of actions and users; for cloud delivery, virtual servers are licensed per instance over fixed terms and by user subscriptions.

IBM's SOAR solution integrates tightly with IBM QRadar, but also interoperates with Splunk. However, IBM supports **a wide array of data formats and protocols** for receiving telemetry including CEF, JDBC, HTTP, SCP, SFTP, and syslog, as well as many proprietary APIs. On-premise components can be deployed in-line and/or tap into span ports for full packet capture and analysis.

IBM Resilient has its own rich case management functions, and IBM App Exchange has connectors for Jira and ServiceNow. IBM X-Force threat intel is built-in, and customers can select additional sources in the **X-Force App Exchange** such as AbuseIPDB, Anomali, Carbon Black, EclecticIQ, haveibeenpwned, Intezer, McAfee, MISP, Recorded Future, Reversing Labs, RiskIQ, and TruStar. IBM supports STIX/TAXII.

IBM can disable/enable users and control instances in AWS/Azure/GCP. IBM can automate responses such as scan initiation and node isolation in **EPP/EDR systems such as** Carbon Black, Cisco, Crowdstrike, Cybereason, Cylance, Digital Guardian, McAfee, Microsoft Defender ATP, Palo Alto, SentinelOne, and Symantec. IBM supports disabling/enabling users and requiring step-up authentication **in IAM solutions** including IBM's SecurityVerify, Microsoft Active Directory and Azure AD, and Wallix Bastion. At the network layer, IBM Resilient can view events but has limited abilities to trigger automated responses on firewalls, IDS/IPS, and NDR types of tools. Other actions can be customized in scripts on IBM QRadar if deployed, as well as using Ansible. Exact capabilities for each integration are determined by functions available in partner APIs. IBM Resilient has dedicated workflows for handling data privacy breaches.

IBM's suite of SOAR products workflows can be aligned to MITRE ATT&CK. IBM's SOAR can utilize admin and analyst MFA methods, including SAML for federation. Resilient ships with customizable playbooks which can use complex conditional logic. App Exchange has many modules available to facilitate various types of **compliance and reporting.**

IBM's SOAR suite attests/certifies with ISO 15408 and 27001. IBM's SOAR offering has many connectors for bringing in disparate sources of information for analysis. IBM QRadar is a prominent SIEM solution and combined with Watson and Resilient bring strong orchestration features for SOC analysts' investigations. More automated response capabilities to 3rd-party tools would strengthen the solution.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●●

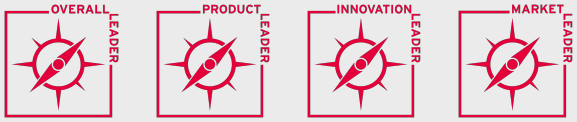
Strengths

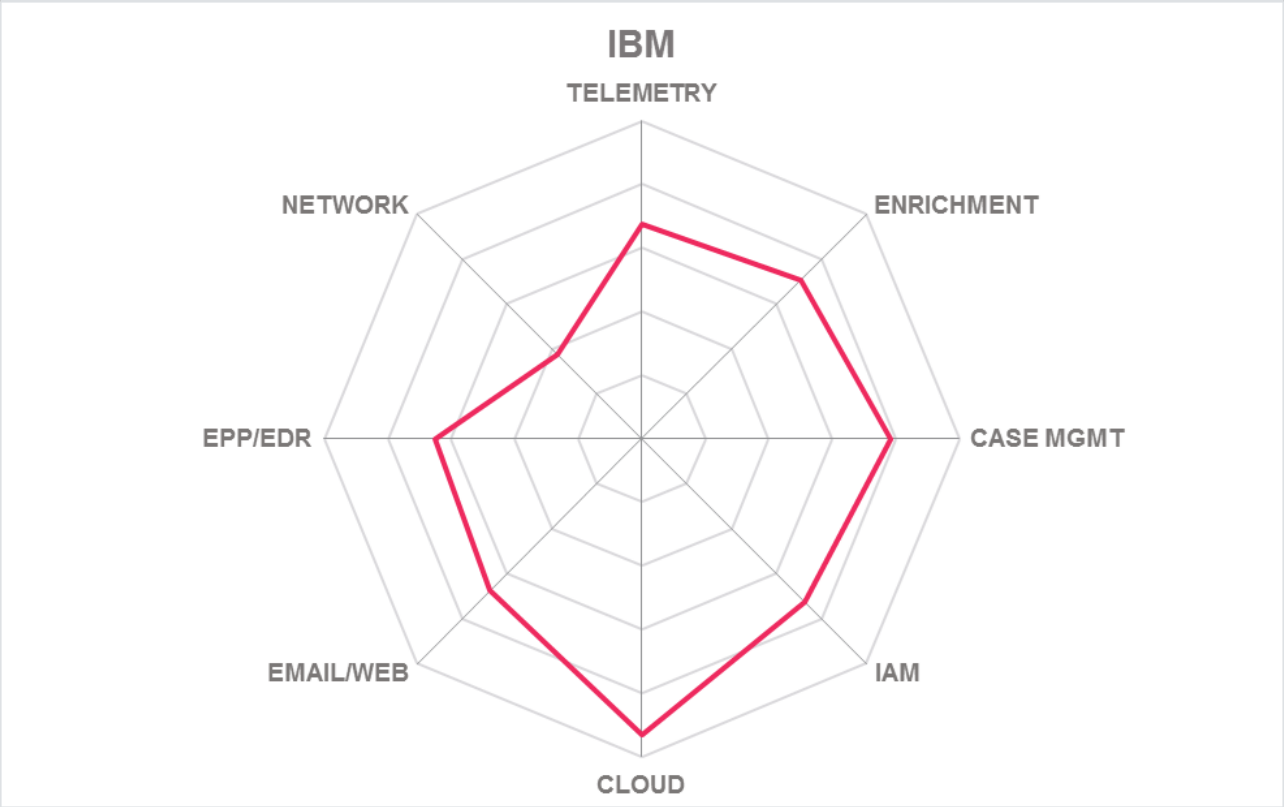
- Broadest selection of input formats and protocols
- Optional packet capture and analysis
- Enhanced by Watson AI
- IBM X-Force included, and large variety of 3rd-party threat intel sources can be added
- OCA founding member

Challenges

- Complex licensing model
- Limited ITSM integration
- Missing integrations with leading EU-based cybersecurity tools
- Somewhat limited in automated responses to 3rd-party tools

Leader in




IBM
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.5 ManageEngine

ManageEngine is a division of privately held ZOHO and was founded in 1996. ManageEngine also has products for IT Help Desk management, patch and vulnerability management, MDM, SIEM, PAM, and other areas of IT management and security. UEBA can be added-on to Log360 deployments for an upcharge. ManageEngine has some MSSPs running Log360. The solution can be deployed on-premises or in AWS/Azure. Licensing is per server.

Log360 is a SIEM, so it does not have connectors for other SIEMs. It does support RPC, SFTP, syslog, and WMI for log imports. It does not perform packet capture itself. As an outgrowth of SIEM, it has not yet attained some SOAR like capabilities such as collaborative investigations and attack visualizations.

Log360 integrates with ManageEngine's own ServiceDesk Plus as well as BMC Remedy, Jira, Kayako, ServiceNow, and ZenDesk. Case management operations rely on their ServiceDesk Plus. Grouping information into events and perform automated investigations is not currently available but on their roadmap. ManageEngine uses AlienVault and Webroot for threat intelligence. More STIX/TAXII conformant threat intel sources can be configured by customers.

ManageEngine has monitoring agents for AWS/Azure/GCP IaaS and O365/Salesforce SaaS but does not allow responses such as disabling users and stopping instances. Integrations allowing complex responses in downstream tools such as endpoint and network security have not been implemented, but customers can create their own by invoking other products' APIs.

An effort is underway to align Log360 with MITRE ATT&CK framework for easier threat hunting. Workflows and analysis use Elastic Search interface. The solution has dashboards and more than 1,000 built-in reports covering compliance for FISMA, GLBA, GDPR, HIPAA, and PCI-DSS, but its visualization capabilities are limited. MFA can be configured, including options for Active Directory, Google Authenticator, Smart Cards, and RADIUS.

ManageEngine Log360 has both SIEM and SOAR in a single package. The SOAR functionality is limited but growing. ManageEngine is a large global IT company with good geographic distribution of support and integration partners. Organizations that are already ManageEngine and Zoho customers may find it easy to add SIEM and some SOAR functionality to their security portfolios.

Security	●●●●●
Functionality	●●○○○
Interoperability	●●●○○
Usability	●●●○○
Deployment	●●●○○

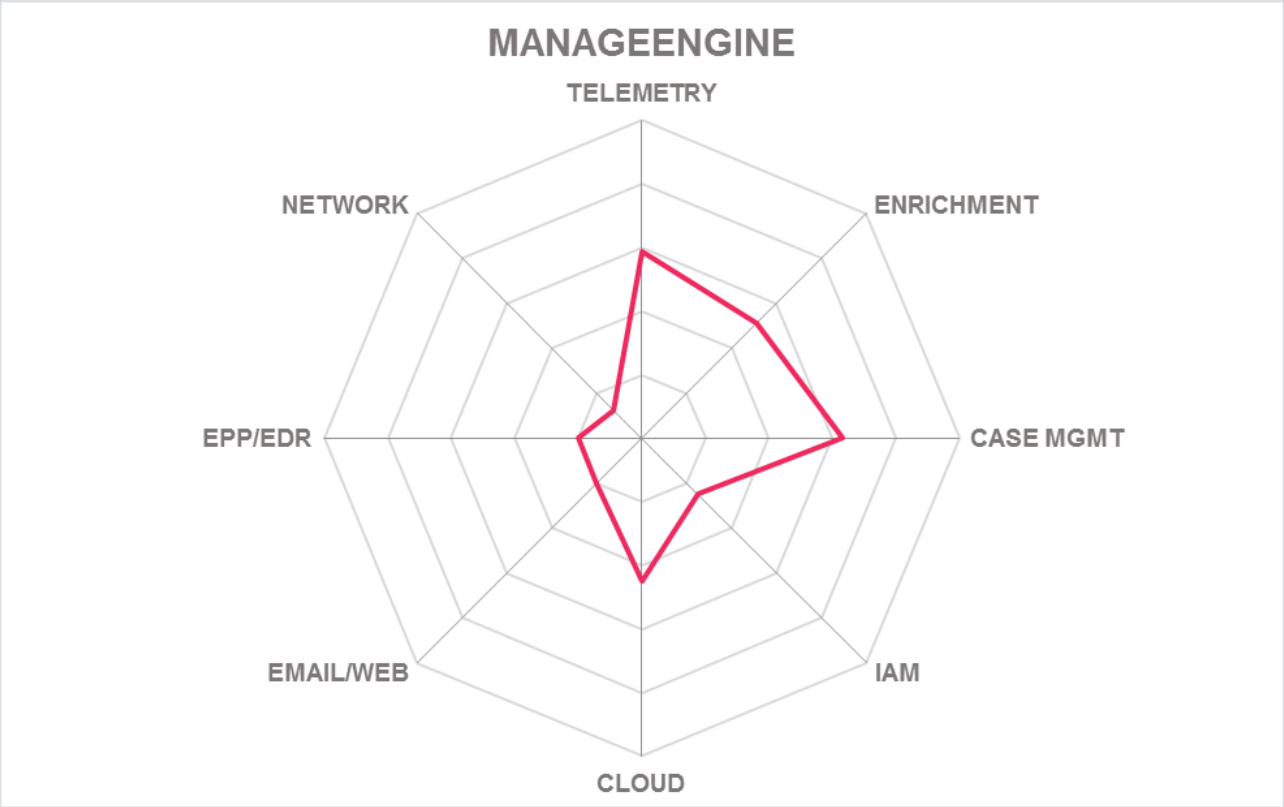
ManageEngine

Strengths

- SIEM with integrated SOAR features
- Straightforward licensing
- MFA options available

Challenges

- Integrations that allow response actions in the cloud and on-premise security tools needed
- Log360 Cloud does not yet have feature parity with on-prem version, though on roadmap
- Narrow range of default threat intel feeds, but extensible
- Missing connectors for endpoint and network security products
- No connectors for other SIEMs


MANAGEENGINE
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.6 Micro Focus

Micro Focus is an IT software vendor with products covering many aspects of security, including a leading SIEM product that it acquired in 2010, ArcSight. Micro Focus picked up ATAR Labs, a SOAR specialist in July 2020. ATAR has on-premise and cloud components and requires a SIEM. ATAR is run by some MSSPs. ATAR is licensed according to numbers of users and deployed components. The ATAR product is deeply integrated with Micro Focus ArcSight, Interset, and Logger currently, and will eventually merge with ArcSight.

As a pure SOAR product, ATAR does not currently collect logs or capture packets. Through integration with RSA NetWitness, analysts can review packet captures. It does have integrations with other SIEMs such as Alien Vault, IBM QRadar, LogRhythm, McAfee, RSA, and Splunk.

ATAR provides an incident management interface for analysts, and also interoperates with HP Service Management, Jira, and ServiceNow ITSMs. ATAR can take in threat intel from Alien Vault, Anomali, Checkpoint, FireEye, IBM X-Force, Invictus Europe, Kaspersky, Palo Alto, Passive Total, Recorded Future, STM CyThreat, Symantec, Team Cymru, Turkcell Bozok, TR-CERT Feed, and Virus Total. STIX/TAXII format and protocol are not yet supported, however.

ATAR correlates events from SIEMs and enables cross-platform analysis. Manual responses can be directed from the console. Automation of responses can be configured by customers. There are no connectors for IaaS at present, but ATAR can snapshot/suspend/reboot VMWare ESXi instances. User info can be queried from IAM systems but disabling/suspending users is not supported. ATAR can initiate email purges and notifications in Microsoft Exchange and O365. ATAR has integrations with Carbon Black, FireEye, Kaspersky, McAfee, Symantec, and Trend Micro EPP products which, depending on the APIs of the downstream products, allow for starting scans, deleting files, isolating nodes, etc. At the network layer, ATAR can instruct Arbor Networks, Checkpoint, Cisco, F5, FireEye, Forcepoint, Fortinet, Juniper, McAfee, Palo Alto, Sophos XG, and Symantec devices to block IPs and/or URLs. Suspicious files can be dispatched to FortiSandbox, IBM X-Force, Symantec, and Virus Total for detonation.

For admin and analyst authentication, ATAR integrates with Microsoft Active Directory and CyberArk. Granular permissions can be assigned per role. ATAR does not map to MITRE ATT&CK currently.

ATAR was an early stage startup specializing in SOAR that was quite recently acquired by Micro Focus. It has most of the basic features needed for SOAR, but likely needs time to mature and expand functionality. As the SOAR product matures, Micro Focus ArcSight customers will benefit from having ATAR's SOAR capabilities.

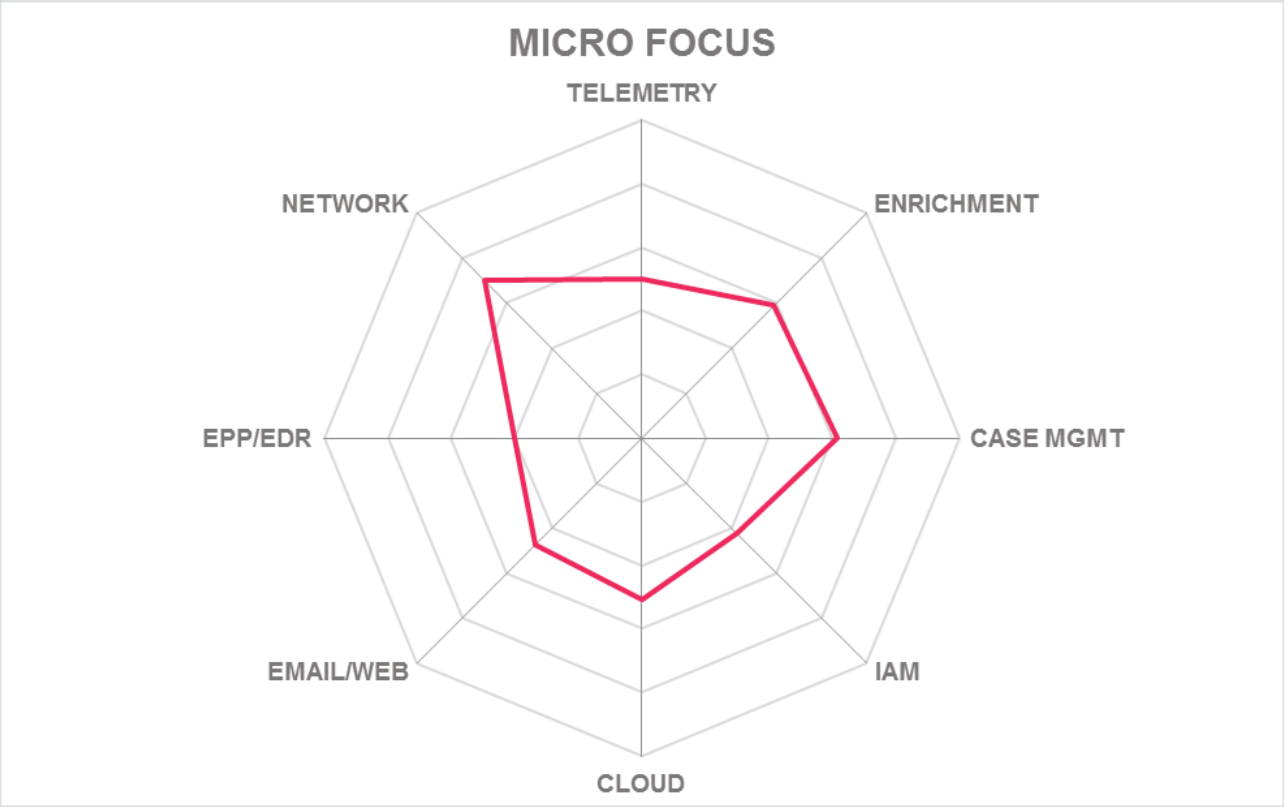
Security	● ● ● ● ○
Functionality	● ● ● ○ ○
Interoperability	● ● ○ ○ ○
Usability	● ● ● ○ ○
Deployment	● ● ● ● ○

Strengths

- ATAR was SOAR pure-play but moving to unification with Micro Focus SIEM
- For on-premise deployments, strong authentication is possible via Microsoft AD integration
- Intuitive analyst interface

Challenges

- Existing ITSM integration capabilities should be extended
- STIX/TAXII not supported
- No support for cloud SIEM sources; no integration with IaaS/PaaS for responses
- No integrations with leading European endpoint security tools


MICRO FOCUS
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.7 Palo Alto Networks

Palo Alto Networks, founded in 2005 in Santa Clara, CA, was the pioneer in Next Generation Firewall (NGFW) technology, and is also a major player in the SOAR market after the acquisition of Demisto. Palo Alto also offers endpoint security, XDR, threat intelligence feeds, and other security products. XSOAR is packaged for on-premise and cloud-to-cloud deployment, with a management console that can run on-premises or in the cloud. Palo Alto hosts a managed service, and some MSSPs use their software for SOAR functions as well. XSOAR is licensed per admin/analyst user.

XSOAR takes input from all major SIEMs including Cortex Data Lake, Devo, Exabeam, Fireeye Helix, FortiSIEM, IBM QRadar, LogRhythm, McAfee ESM, Microsoft Graph Security, MicroFocus Arcsight, Microsoft Azure Security Center and Sentinel, RSA NetWitness, Securonix, Splunk, and SumoLogic. Containers are supported by Prisma Compute. XSOAR supports CEF and syslog for other sources. XSOAR does not capture packets but through integration with supported products can receive and analyze captures.

XSOAR features real-time collaboration and case management. It can integrate with ITSM solutions including BMC Remedy, Cherwell, EasyVista, Freshdesk, Jira, ServiceNow, and Zendesk. XSOAR manages threat intelligence, including Palo Alto's extensive in-network sources, plus AlienVault, Anomali, Cofense, Cymon, Domain Tools, Farsight Security, Open Phish, Recorded Future, and Virus Total. XSOAR can also receive any STIX/TAXII feed.

XSOAR ships with >3,000 playbook actions that cover triage, evidence collection, and complex actions via a long list of connectors. XSOAR can disable/enable users and stop/start instances in AWS/Azure/GCP. XSOAR has easy to install connectors for endpoint security solutions including Carbon Black, Crowdstrike, Cybereason, Cylance, SentinelOne, Symantec, Tanium, etc. IAM integrations include CyberArk, Duo, Microsoft Active Directory, and Okta. XSOAR playbooks can manipulate Palo Alto products and other network security solutions by CheckPoint, F5, Fortinet, ProtectWise, Signal Sciences, Tufin, Vectra, and ZScaler. It can also execute deletion of malicious emails in Gmail and Microsoft Exchange. Permissible actions available in the large number of playbooks depend on API implementations of these products.

Event correlation can be mapped to MITRE ATT&CK. XSOAR supports SAML federation and integration with LDAP and Microsoft AD for other forms of MFA.

Palo Alto offers advanced security features, including attestations/certifications for FIPS 140-2, ISO 27001, HIPAA/HITRUST, and SSAE 18 SOC 2 Type 2. Their solution is highly scalable and configurable. The strength of a SOAR system is based not only on the ability to orchestrate but also to provide automatable responses. The large number of connectors available plus the ability to extend the platform make Palo Alto's XSOAR one of the dominant products on the market today.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

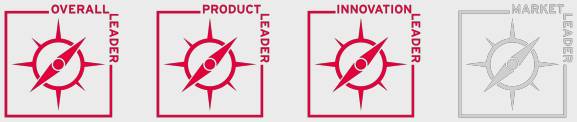
Strengths

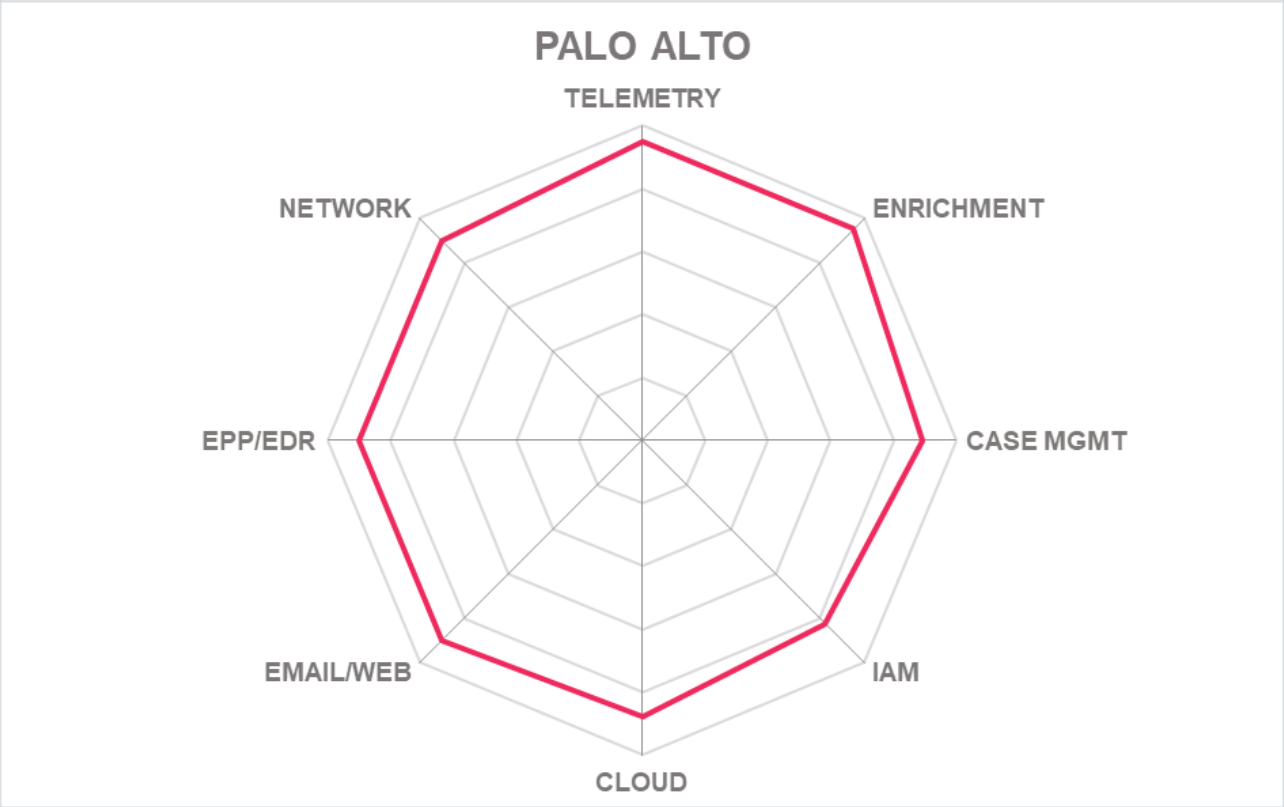
- Large number of connectors for most kinds of security tools
- High quality threat intel built-in, other feeds are easy to add
- Ships with many configurable playbooks covering a wide variety of use cases
- Collaborative investigations facilitated by visual playbook editor

Challenges

- Missing integrations for leading EU-based security tools
- More native MFA options would be helpful

Leader in




PALO ALTO
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.8 ServiceNow

ServiceNow, founded in 2004 in San Diego, is a large IT management, operations, and business management software vendor. They also have products in the IT security, asset management, GRC, and DevOps areas, providing solutions for both employee and customer facing enterprises. Their SOAR offering has on-premise components, but the interface can be hosted in the cloud. Licensing is based on the number of upstream monitored or queried devices.

For telemetry sources, ServiceNow can integrate with IBM QRadar, LogRhythm, McAfee, Micro Focus ArcSight, Microsoft, Securonix, Splunk, and ingest email and syslog. ServiceNow can also use REST APIs, SSH, and SOAP to pull security event information from upstream systems. ServiceNow does not capture packets or perform security event analysis at that level.

ServiceNow offers a leading ITSM solution, therefore it has good case management in its platform, but also integrates with other ITSMs such as BMC Remedy and Jira. ServiceNow has connectors for many threat intel sources, including AlienVault, Anomali, Cisco, Cofense, Crowdstrike, Digital Shadows, Flashpoint, haveibeenpwned, Hybrid Analysis, OPSWAT, Palo Alto Networks, PhishTank, Recorded Future, Reverse WHOIS, RiskIQ, Shodan, Secureworks, Synack, Threat Crowd, and Virus Total. Moreover, ServiceNow understands STIX/TAXII so additional feeds can be consumed.

ServiceNow customers can extend AWS/Azure/GCP connectors to allow remote disabling of users and stop/start of cloud instances. For IAM systems, ServiceNow integrates with Avatier, AWS, BeyondTrust, Centrify, ClearSkye, FortiCode, Google Directory, IBM, Microsoft AD, Okta, Ping Identity, RSA, and Signicat IAM solutions. ServiceNow integrates with endpoint security tools: Carbon Black, Crowdstrike, Cybereason, Cytomic/Panda, Digital Defense, Forescout, Malwarebytes, McAfee, Symantec, and Tanium. ServiceNow off-the-shelf integrations can trigger actions on Algosec, Checkpoint, Cisco, Darktrace, Extrahop, Forescout, Infoblox, McAfee, Palo Alto, and Tripwire network infrastructure, and interact with email systems including Agari, Microsoft Exchange/O365, Mimecast, and PhishBait. It also offers its own vulnerability prioritization and management product called Vulnerability Response and integrates with vulnerability assessment and management components in Crowdstrike, Digital Defense, Outpost 24, Qualys, Rapid7, Tenable, Tripwire, and Outpost 24. Playbooks are available via The Action Library, custom actions enabled by FlowDesigner, but like all SOAR products are constrained by downstream product APIs.

The Security Incident Response Platform is aligned with MITRE ATT&CK currently. ServiceNow supports SAML federation and Google, LDAP, and OAuth authentication.

Security Incident Response Platform uses FIPS 140-2 encryption where needed, and attests/certifies with ISO 27001 and SSAE 18 SOC2 Type 2. ServiceNow is quite scalable and has excellent case management features. It has built out integrations with many and diverse sets of threat intelligence for enrichments. As with most SOAR solutions, customers can extend integrations with some effort. ServiceNow should add to their list of pre-built connectors, especially in the areas of endpoint/network security and IAM vendors. Organizations who use ServiceNow for ITSM or other functions may find it easy to gain SOAR functionality by adding Security Incident Responder.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●●

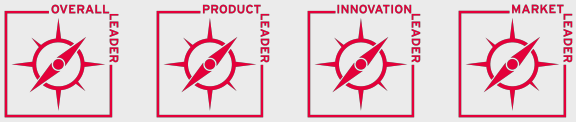
Strengths

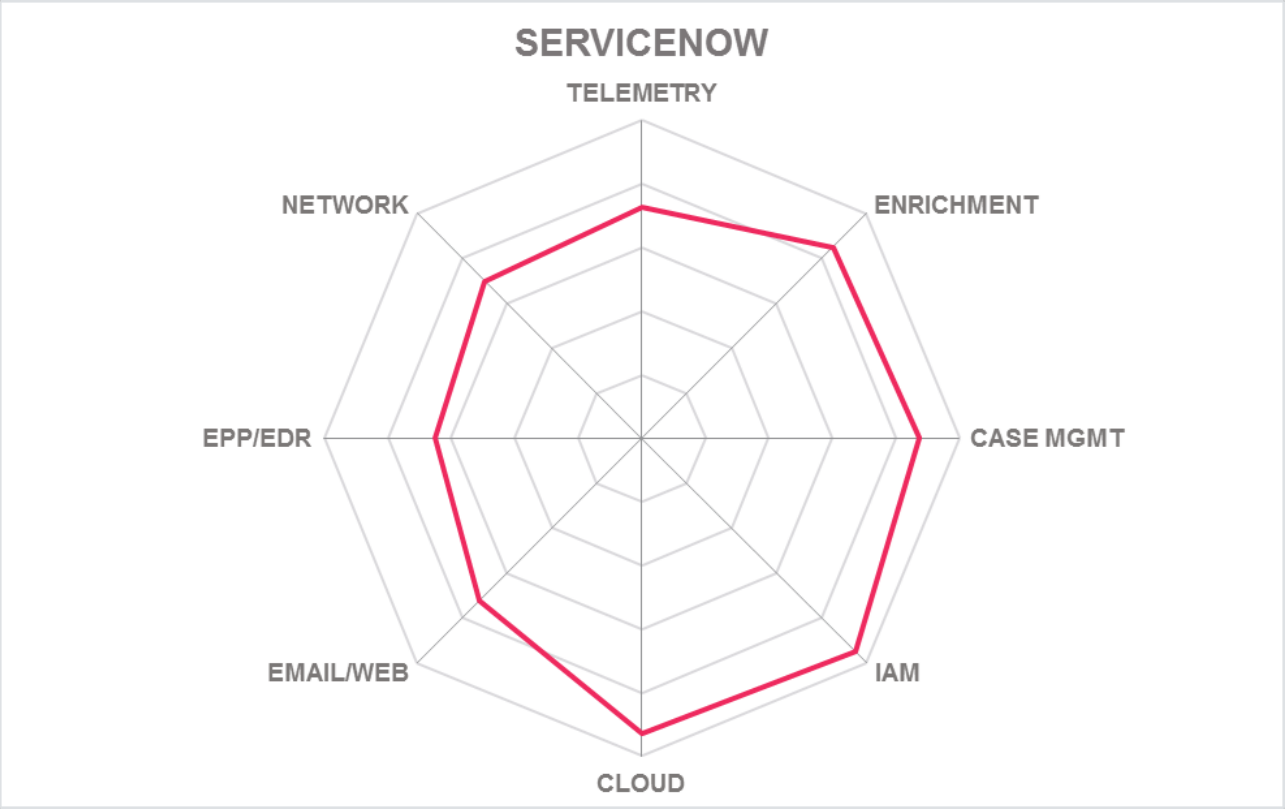
- MFA for admins and analysts
- Large selection of threat intel sources for enrichment
- Good integration with other ServiceNow products for case and asset management
- Good support for IaaS

Challenges

- Additional telemetry connectors would be useful
- Lacks support for some common endpoint and network security tools

Leader in




SERVICENOW
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.9 Siemplify

Siemplify is a mid-stage startup concentrating on SOAR. They were founded in 2015 and are headquartered in New York. Deployments have on-premise components but can be managed from the cloud or by MSSPs. Licensing is per user/year.

As a pure SOAR solution, Siemplify requires integration with an underlying SIEM, therefore it does not use CEF or syslog for log collection or provide agents for endpoints. Moreover, it does not capture packets but can pull information from some NTA/NDR solutions for analysis. Siemplify receives telemetry from AlienVault, IBM QRadar, LogRhythm, McAfee, MicroFocus ArcSight, Microsoft Azure Sentinel, Splunk, and SumoLogic.

Siemplify automatically organizes event data into threat-centric cases and enriches the cases with a vast array of threat intelligence sources: Anomali, APIVoid, Certly, Cisco Talos and Threat Grid, Cymon, Domain Tools, haveibeenpwned, IBM X-Force, IntSights, MalShare, MDL, McAfee, Microsoft Security Graph, MISP, Palo Alto AutoFocus, Phishing Initiative, Recorded Future, RiskIQ, Shodan, Symantec, Threat Crowd, ThreatExchange, ThreatQuotient, ThreatConnect, URLScan, and Virus Total. However, it does not assign risk scores to events. Siemplify also supports STIX/TAXII. Siemplify integrates with many ITSM platforms including CA Service Desk, ConnectWise, Jira, Manage Engine Service Desk Plus, MicroFocus Service Automation, ServiceNow, SysAid, and ZenDesk.

Siemplify's playbooks can trigger actions in downstream systems. Siemplify integrates with Azure, Checkpoint Cloud Guard, and Netskope cloud security products; Carbon Black, Crowdstrike, Cybereason, Cylance, Endgame, FireEye, McAfee, Microsoft Windows Defender ATP, Palo Alto, SentinelOne, Sophos, Symantec, Tanium, and TrendMicro endpoint security; Proofpoint for email security; CyberArk and Okta IAM; Checkpoint, Cisco, F5, Fortinet, Juniper, McAfee, Palo Alto, ProtectWise, and ZScaler for firewalls and network security devices. Exact capabilities depend on which functions are exposed by these products' APIs. Playbooks can be customized and extended in their Python-based IDE.

Siemplify's analyst interface is aligned with MITRE ATT&CK. SAML federation is supported, so MFA can be implemented via SAML.

Siemplify attest/certifies with ISO 9001, 15408, and 27001, and SSAE 18 SOC 2 Type 2. Their vendor agnostic approach makes it easier for organizations to insert SOAR in complex security portfolios. Support for cloud environments is likely to grow. Accepting SAML federation is good but building in more MFA options would be better. Any organization looking for pure SOAR solutions with lots of connectors for existing security tools should take a look at Siemplify.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●●

Siemplify

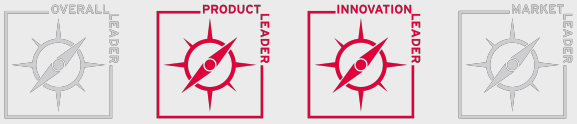
Strengths

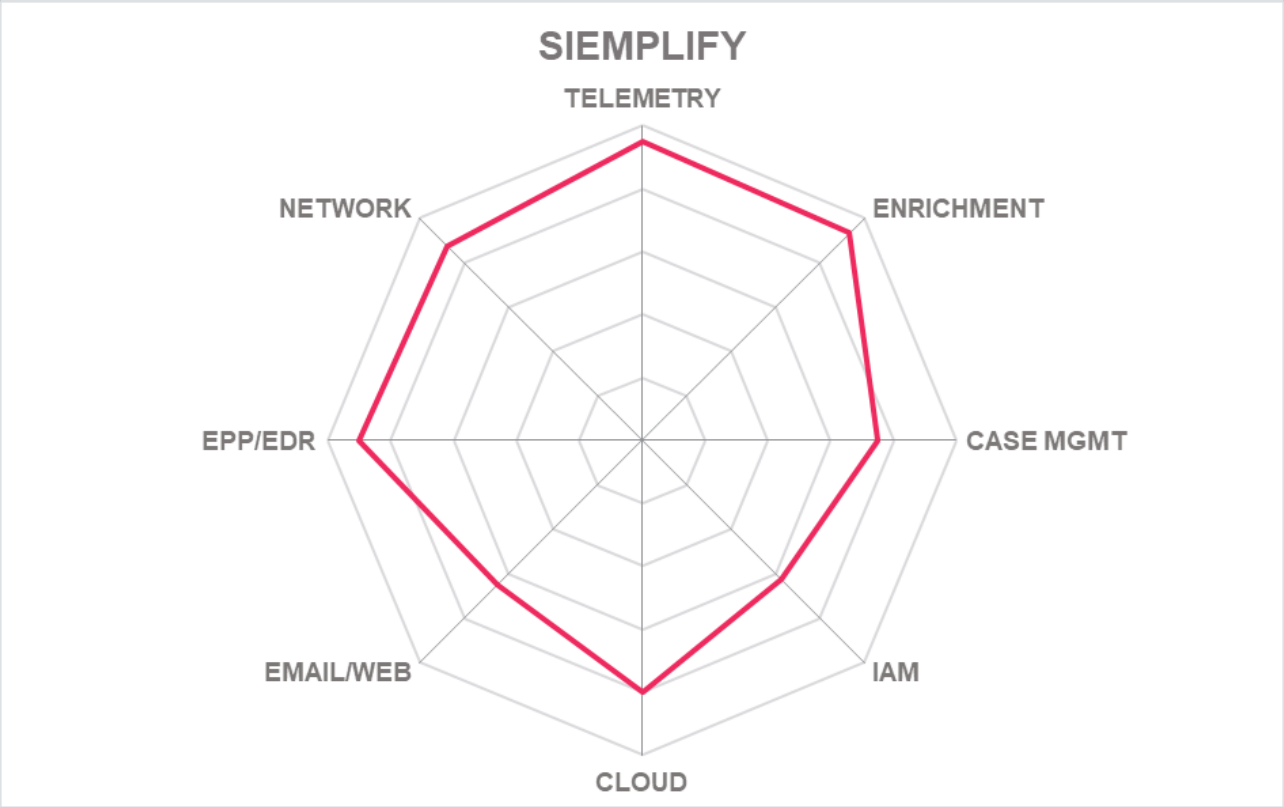
- Many connectors for ITSM
- Diverse assortment of threat intel sources
- Threat-centric case management
- Good selection of connectors for downstream security tools
- Standalone SOAR platform

Challenges

- Late to cloud hosting
- Missing support for major EU cybersecurity tool vendors
- Built-in MFA beyond SAML would be beneficial

Leader in




SIEMPLIFY
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.10 SIRP

SIRP is an early stage startup founded in 2017 and based in London. Their sole product is SOAR which is focused on risk-based security operations. The solution comprises both on-premise and cloud components. SIRP also offers SOAR as a managed service that enterprises and MSSPs can use. The solution is licensed per user per year.

SIRP is a pure-play SOAR product relies on SIEMs such as AlienVault, IBM QRadar, LogRhythm, MicroFocus ArcSight, and Splunk SIEMs. The product does not support direct collection of logs or packet captures.

SIRP works with BMC Remedy, Jira, ManageEngine, and ServiceNow ITSMs. SIRP evaluates events and their threat intel context and assigns risk values to each. SIRP processes threat intel from AbuseIPDB, Anomali, APIVoid, Cymon, DataDog, Devo, Domain Tools, Farsight Security, haveibeenpwned, ipInfo, MaxMind, MISP, PhishLabs, PhishMe, PhishTank, Security Trails, ThreatGrid, ThreatConnect, and Virus Total. STIX/TAXII are supported. This product does not perform UBA, outlier analysis, or event correlation. Reports for regulatory compliance are not available.

Playbooks in SIRP can be customized and can execute actions in remote systems. It ships with 300 pre-defined integrations. SIRP has extensive controls for AWS/EC2 and VMware vSphere. SIRP can direct endpoint systems, depending on API functions, to initiate scans, kill processes, isolate nodes, etc. Endpoint security systems for which there are integrations include Carbon Black, Cisco, Crowdstrike, Cylance, FireEye, Fortinet, Microsoft Defender ATP, Palo Alto, Symantec, and Trend Micro. SIRP playbooks can trigger deletions of malicious email in Gmail and Microsoft O365. Integrations with network layer security solutions include F5, FireEye, Imperva, Juniper, Lastline, Palo Alto, and ZScaler.

SIRP does not perform MITRE ATT&CK mapping in the console. SAML is supported for admin/analyst authentication, and additional methods are being considered.

SIRP has not yet achieved cloud or security certifications. SIRP is a newer entrant in the market and has more work in front of them to add functionality and grow their client and partner base. However, it does have basic SOAR functionality, strengths as listed above, and integrations with some uncommon threat intel sources, so this will appeal to some organizations.

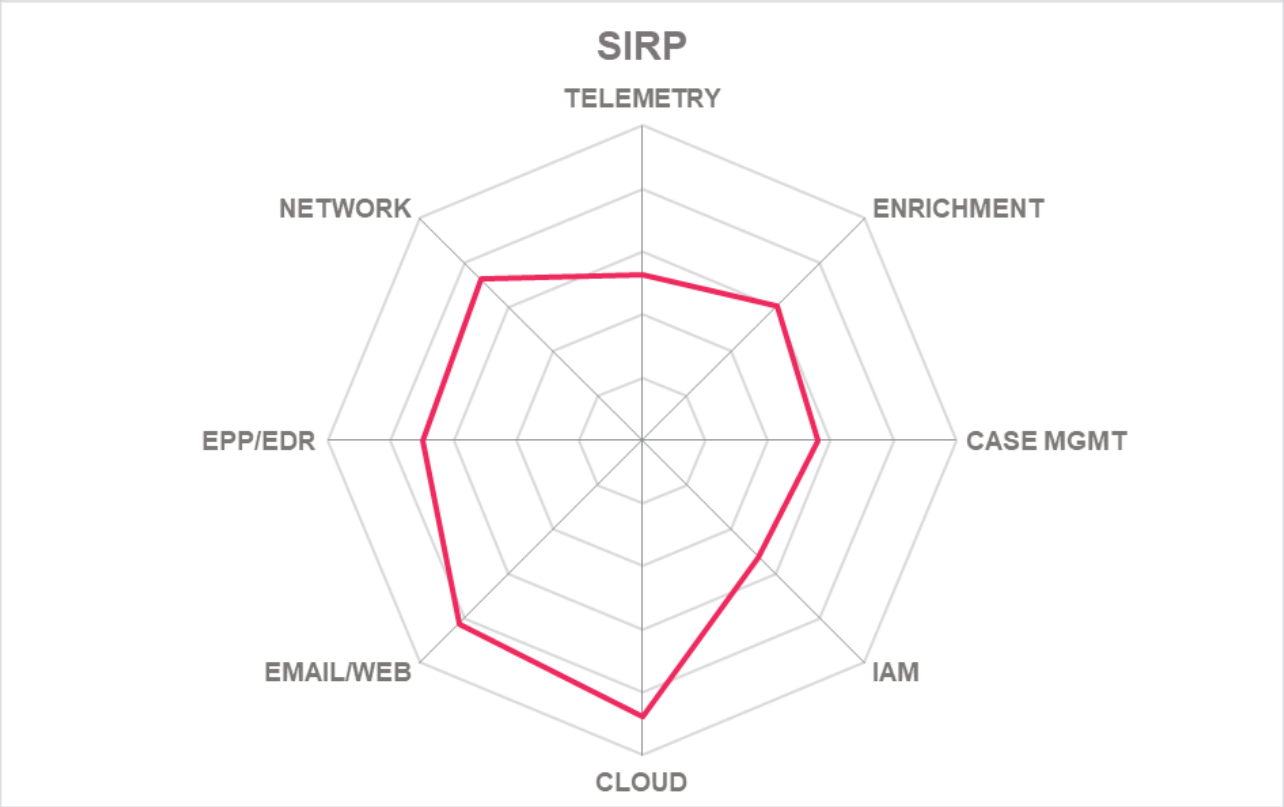
Security	●●●●○
Functionality	●●●●○
Interoperability	●●○○○
Usability	●●●●○
Deployment	●●●●○

Strengths

- Correlation of incidents, vulnerabilities, threat intelligence and assets
- Risk scoring
- Good integration with AWS
- Threat intel source curation shows focus on credential abuse and phishing prevention

Challenges

- No outlier analysis or event correlation
- Smaller company
- Missing integrations with EU cybersecurity products
- Needs more integrations with IAM, ITSM, and endpoint and network security tools


SIRP
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

5.11 ThreatConnect

ThreatConnect is a mid-stage equity-backed security firm headquartered in Arlington, VA. They were founded in 2011. Their solution encompasses threat intelligence management and SOAR. They have servers and services deployed both on-premises and in the cloud. A number of MSSPs use their software. Licensing is per user/year and by number of servers.

ThreatConnect works on top of SIEMs such as Fortinet, IBM QRadar, LogRhythm, McAfee, Micro Focus ArcSight, Microsoft Azure Sentinel, RSA, Securonix, and Splunk. It can take in log files and review packets captured by network systems, but that is not a primary function.

ThreatConnect provides an interface for guiding investigations and managing incidents. It also integrates with IR and ITSM solutions including DFLabs, FireEye Helix, IBM Resilient, Jira, RSA Archer, and SlashNext. ThreatConnect curates anonymized security analytics across its customer base in their Collective Analytics Layer (CAL) service and has innovative approaches to identifying Algorithmically Generated Domains (AGDs). Some examples of other intel sources incorporated are Accenture iDefense, Attivo Networks Deception, BAE Systems, Bitdefender, Cisco, Cofense, Crowdstrike, Digital Shadows, Dragos, Farsight, FireEye, Intel471, Kaspersky, McAfee, MISP, OPSWAT, Palo Alto, ProofPoint, Recorded Future, ReversingLabs, RiskIQ, and Shodan. ThreatConnect supports STIX/TAXII. With the recent acquisition of Nehemiah Security, they will add cyber risk quantization to their platform.

ThreatConnect comes with hundreds of playbooks covering use cases from evidence gathering to enrichment to manual and automated responses. Analysts can use their specialized query language to search across all connected sources. Journaling enables collaboration. In terms of responses, ThreatConnect can get info and disable/enable users in Azure AD, Cisco, and Okta; initiate scans/quarantine files/isolate nodes in endpoint products such as Carbon Black, Crowdstrike, Cybereason, Symantec, and Tanium; execute changes on network security tools by Cisco, Fidelis, Palo Alto, and ZScaler. Response capabilities depend on each downstream product's APIs.

MITRE ATT&CK mapping to the sub-technique level is built-in. TOTP is supported for strong authentication, and SAML is available for federated authentication.

ThreatConnect has achieved ISO 27001 certification. ThreatConnect's strengths align with their origins in threat intelligence consolidation and enrichment. Additional integrations with major products in ITSM, endpoint and network security will benefit customers, as will planned functionality in IaaS and MITRE alignment. Organizations looking for strong threat intelligence management plus SOAR will want to consider ThreatConnect's capabilities.

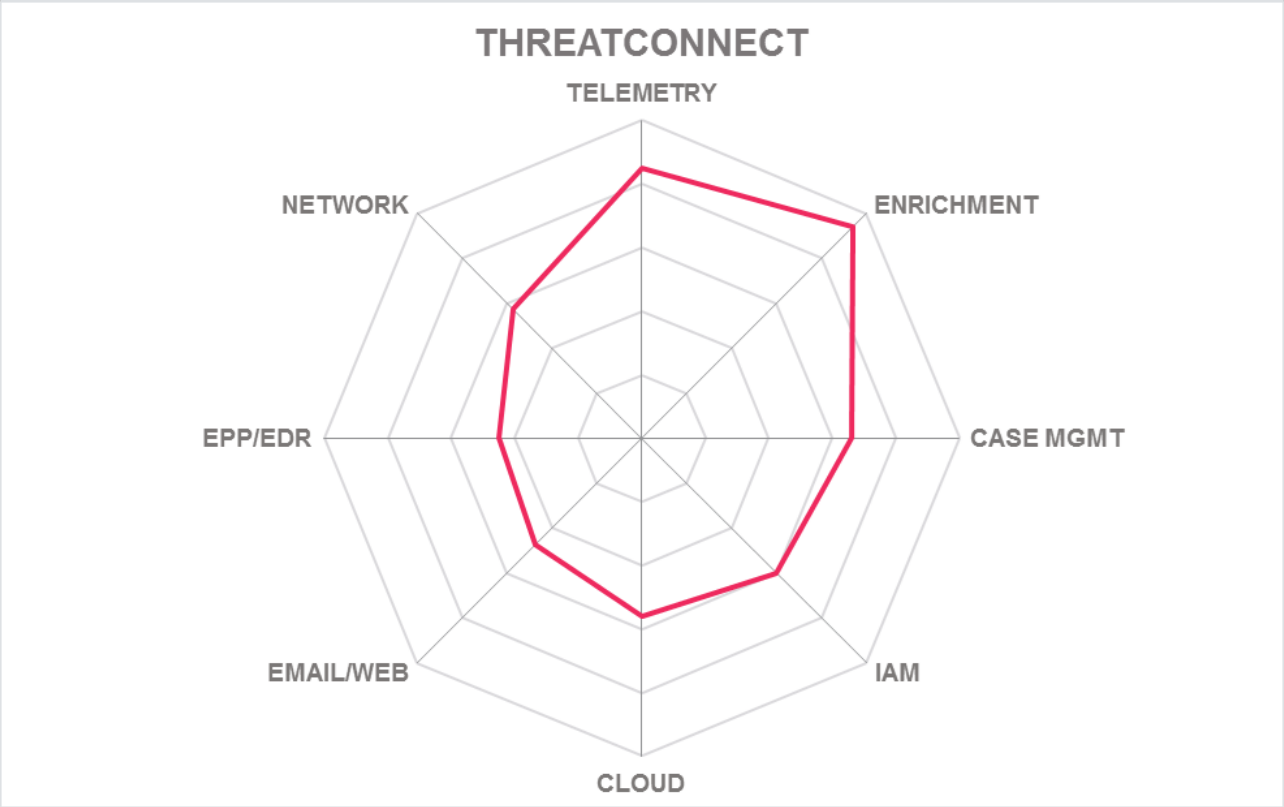
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○

Strengths

- Extensive list of threat intel sources allows some customers to de-duplicate intelligence subscriptions
- ThreatConnect is OEM'd into other security operations platforms
- Interface shows per-playbook ROI
- Cyber risk quantification

Challenges

- Response actions for AWS and GCP not present but planned
- Missing integrations for a few key ITSM products
- Missing integrations for some endpoint and network security products, including EU vendors
- More MFA methods needed


THREATCONNECT
TELEMETRY
ENRICHMENT
CASE MGMT
IAM
CLOUD
EMAIL/WEB
EPP/EDR
NETWORK

6 Vendors and Market Segments to watch

Aside from the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors but do not fully fit into the SOAR market segment or are not yet mature enough to be considered in this evaluation. We provide short abstracts below on these vendors.

6.1 LogRhythm

LogRhythm was founded in Denver in 2003 and was acquired by Thoma Bravo in 2018. As the name implies, they started with log management and SIEM. Today they also have UBA and NDR/NTA. Their SOAR solution works on top of their next gen SIEM.

LogRhythm SOAR has response-focused integrations with a variety of granular actions available via playbooks. Details on the playbooks and integrations were not available. LogRhythm did not respond to our request for information for this report.

6.2 Rapid7

Boston-based Rapid7 was established in 2000. They have a suite of interrelated security products covering UBA, SIEM, patch and vulnerability management, application security, cloud security, penetration testing, and SOAR. Insight Connect is their SOAR product.

For cloud services, they have deep integration with IaaS platforms, services, and containers; for IAM, InsightConnect can integrate various IDaaS providers, offering granular response actions; for endpoint and network security, integrations exist for several of the product lines by leading vendors.

Rapid7 did not respond to our request for information for this report.

6.3 Securonix

Securonix was formed in 2008 and is headquartered in Dallas. Their security analytics platform includes Data Lake, NDR (NTA), SIEM, and UBA. Securonix SOAR integrates with these components.

Securonix SOAR reportedly ships with more than 3,000 playbook actions and up to 275 possible product integrations. Details on playbook actions and integrations were not available. Securonix did not respond to our request for information for this report.

6.4 Swimlane

Swimlane is a mid-stage security specialist that launched in 2014 in Denver. Swimlane is a SOAR specialist.

Swimlane has almost 150 integrations covering many of the major SIEMs and other data sources, threat intelligence and data enrichment sources, and downstream endpoint/network security, IAM, and ITSM tools.

6.5 ThreatQuotient ThreatQ and Threat Investigations

ThreatQuotient is a venture-backed threat intelligence and SOAR specialist headquartered in Reston, VA, outside Washington, DC. The company was founded in 2013. ThreatQuotient's two main products are often deployed together to provide SOAR capabilities. For high security requirements, ThreatQ can operate in air-gapped environments.

ThreatQ & Investigations is a complement to SIEM solutions. ThreatQuotient can facilitate case management and synchronize with Best Practical RTIR, IBM Resilient, and ServiceNow ITSM. ThreatQ is well-known as a threat intel source, and the solution incorporates **>100 OSINT and commercial sources**. Customers can implement additional feeds as needed, and ThreatQuotient supports STIX and TAXII. ThreatQuotient does not use the playbook paradigm but does allow for automated searches for event data across underlying SIEMs, as well as disseminating threat information to other components in the security architecture.

7 Related Research

Leadership Compass: Network Detection and Response – 80126
Market Compass: Endpoint Protection Detection and Response – 80508
Market Compass: Cloud Access Security Brokers – 80079
Market Compass: Cloud Backup and Disaster Recovery – 71176
Leadership Brief: Incident Response Management - 80344
Leadership Brief: Responding to Cyber Incidents - 80209

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.