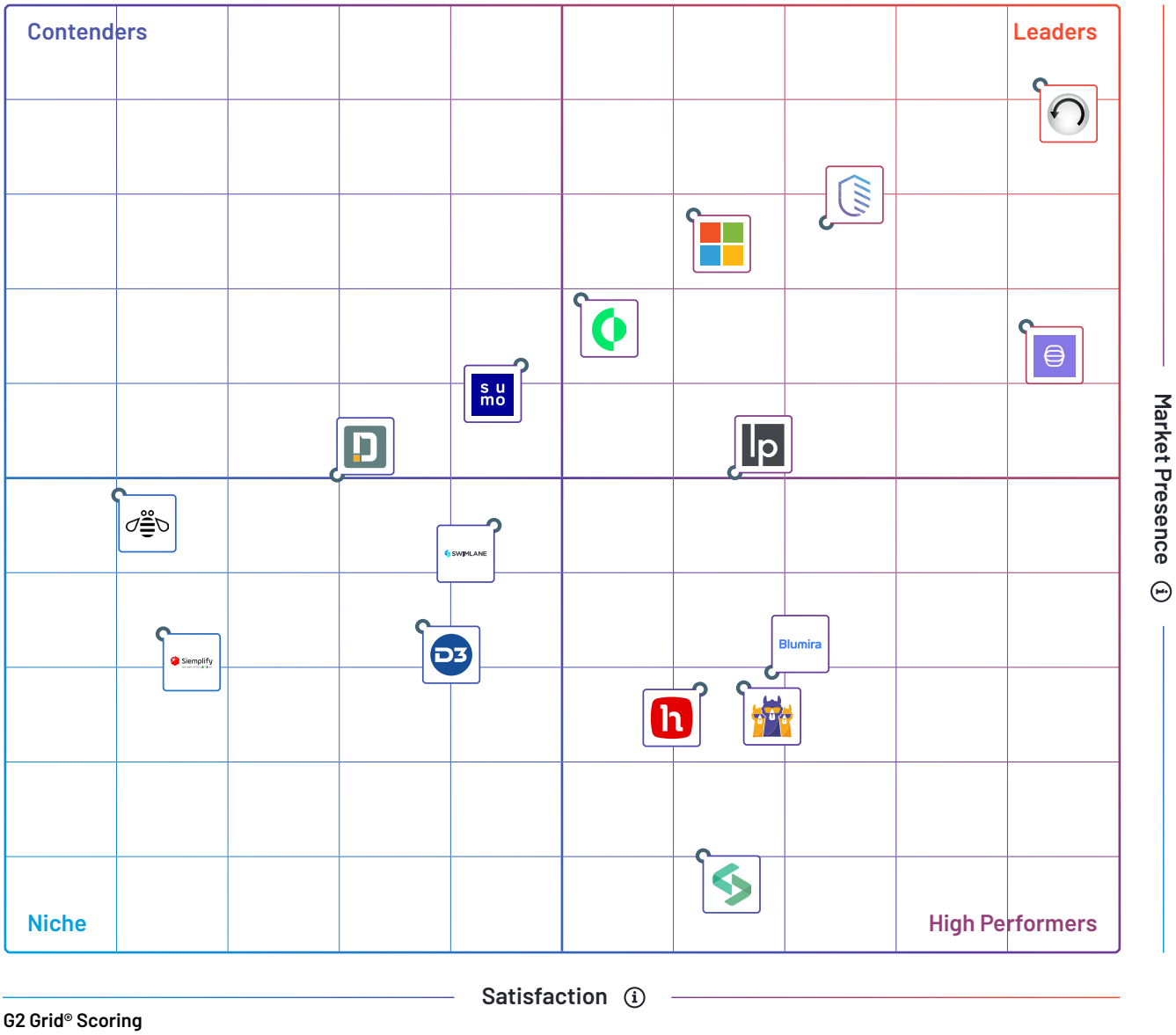
Grid® Report for Security Orchestration, Automation, and Response (SOAR) | Fall 2022

Security Orchestration, Automation, and Response (SOAR) Software



(Security Orchestration, Automation, and Response (SOAR) Software continues on next page)

Security Orchestration, Automation, and Response (SOAR) Software (continued)

Security Orchestration, Automation, and Response (SOAR) Software Definition

Security orchestration, automation, and response (SOAR) software products are tools used to help integrate security technologies and automate incident-related tasks. These tools integrate with a company's existing security solutions to help users build and automate workflows, simplifying the incident response process and reducing the amount of human intervention necessary to handle security incidents. Companies use these tools to create a centralized system complete with visibility into a company's security software and operational processes. These tools also reduce the time it takes to respond to incidents, as well as the potential for human error in remediating security threats and vulnerabilities.

SOAR tools combine aspects of vulnerability management, incident response, and security information and event management (SIEM) solutions. SOAR products are designed to provide some of each tool's respective functionality or integrate with third-party tools. Once integrated, processes can be designed to identify incidents and automate remediation tasks.

To qualify for inclusion in the Security Orchestration, Automation, and Response (SOAR) category, a product must:

- Integrate security information and incident response tools
- Allow security professionals to build response workflows
- Automate incident management and response tasks within workflows
- Provide formalized incident, workflow, and performance reports

Security Orchestration, Automation, and Response (SOAR) Grid® Scoring Description

Products shown on the Grid® for Security Orchestration, Automation, and Response (SOAR) have received a minimum of 10 reviews/ratings in data gathered by August 30, 2022. Products are ranked by customer satisfaction (based on user reviews) and market presence (based on market share, seller size, and social impact) and placed into four categories on the Grid®:

- Products in the Leader quadrant are rated highly by G2 users and have substantial Market Presence scores. Leaders include: PhishER, Tines, IBM Security QRadar, Microsoft Sentinel, Palo Alto Networks Cortex XSOAR, and LogPoint
- High Performing products have high customer Satisfaction scores and low Market Presence compared to the rest of the category. High Performers include: Blumira Automated Detection & Response, CrowdSec, LogicHub, and SIRP
- Contender products have relatively low customer Satisfaction scores and high Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. Contenders include: Sumo Logic, and Demisto
- Niche products have relatively low Satisfaction scores and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. Niche products include: Swimlane, D3 Security, IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform, and Siemplify - Google Cloud

Grid® Scores for Security Orchestration, Automation, and Response (SOAR) Software

The table below shows the Satisfaction and Market Presence scores that determine product placement on the Grid®. To learn more about each of the products, please see the profile section.

Leaders

	# of Reviews	Satisfaction	Market Presence	G2 Score
PhishER	123	96	96	96
Tines	78	94	68	81
IBM Security QRadar	88	75	80	78
Microsoft Sentinel	50	63	81	72
Palo Alto Networks Cortex XSOAR	13	52	71	61
LogPoint	20	67	51	59

High Performers

Blumira Automated Detection & Response	21	70	27	49
CrowdSec	26	67	25	46
LogicHub	11	63	25	44
SIRP	18	64	6	35

Contenders

Sumo Logic	37	46	63	55
Demisto	14	29	51	40

Niche

Swimlane	20	43	45	44
D3 Security	41	37	33	35
IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform	13	8	48	28
Siemplify - Google Cloud	22	12	32	22

* Products are ordered by G2 Score. Satisfaction score is used as a tiebreaker if two products have the same G2 Score.

Grid® Methodology

Grid® Rating Methodology

The Grid® represents the democratic voice of real software users, rather than the subjective opinion of one analyst. G2 rates products from the Security Orchestration, Automation, and Response (SOAR) category algorithmically based on data sourced from product reviews shared by G2 users and data aggregated from online sources and social networks.

Technology buyers can use the Grid® to help them quickly select the best products for their businesses and to find peers with similar experiences. For sellers, media, investors, and analysts, the Grid® provides benchmarks for product comparison and market trend analysis.

Grid® Scoring Methodology

G2 rates products and sellers based on reviews gathered from our user community, as well as data aggregated from online sources and social networks. We apply a unique algorithm (v3.0) to this data to calculate the Satisfaction and Market Presence scores in real time. The Grid® Report for Security Orchestration, Automation, and Response (SOAR) | Fall 2022 is based on scores calculated using the G2 algorithm v3.0 from reviews collected through August 30, 2022. To view the Security Orchestration, Automation, and Response (SOAR) Grid® with the most recent data, please visit the Security Orchestration, Automation, and Response (SOAR) page.

Satisfaction

The Satisfaction rating is affected by the following (in order of importance):

- Customer satisfaction with end user-focused product attributes based on user reviews
- Popularity and statistical significance based on the number of reviews received by G2
- Quality of reviews received (reviews that are more thoroughly completed will be weighted more heavily)
- Age of reviews (more-recent reviews provide relevant and up-to-date information that is reflective of the current state of a product)
- Customers' satisfaction with administration-specific product attributes based on user reviews
- Overall customer satisfaction and Net Promoter Score® (NPS) based on ratings by G2 users

Note: The customer satisfaction score is normalized for each Grid®, meaning the scores are relative.

(Grid® Methodology continues on next page)

** Net Promoter, Net Promoter System, Net Promoter Score, NPS and the NPS-related emoticons are registered trademarks of Bain & Company, Inc., Fred Reichheld and Satmetrix Systems, Inc.

Grid® Methodology (continued)

Market Presence

The Market Presence score is affected by the following (in order of importance):

- Market presence is a combination of 15 metrics from G2's reviews, publicly available information, and third-party sources
- Both the software sellers and the individual products are measured on various criteria. The criteria are listed in order of importance. Products metric receive greater weight than seller metrics

Criteria	Measured For		Metrics
	Product	Seller	
Number of Employees	✓	✓	Employee Count (based on social networks and public sources)
Reviews	✓		Review Count (weighted by recency)
Web Presence	✓	✓	
Social Presence	✓	✓	
Growth	✓	✓	Employee Growth, Web Presence Growth
Seller Age		✓	
Employee Satisfaction and Engagement		✓	

- Each input is normalized by category and segment. This means that scores are relative to other products in the category/segment and may change from segment to segment
- The scores are then scaled from 0-100

Grid® Categorization Methodology

Making G2 research relevant and easy for people to use as they evaluate and select business software products is one of our most important goals. In support of that goal, organizing products and software companies in a well-defined structure that makes capturing, evaluating, and displaying reviews and other research in an orderly manner is a critical part of the research process.

To manage the process of categorizing the software products and the related reviews in the G2 community, G2 follows a publicly available categorization methodology. All products appearing on the Grid® have passed through G2's categorization methodology and meet G2's category standards.

Many terms that appear regularly across G2 and are used to aid in product categorization warrant a definition to facilitate buyer understanding. These terms may be included within reviews from the G2 community or in executive summaries for products included on the Grid®. A list of standard definitions is available to G2 users to eliminate confusion and ease the buying process.

(Grid® Methodology continues on next page)

Grid® Methodology (continued)

Rating Changes and Dynamics

The ratings in this report are based on a snapshot of the user reviews and social data collected by G2 up through August 30, 2022. The ratings may change as the products are further developed, the sellers grow, and as additional opinions are shared by users. G2 updates the ratings on its website in real time as additional data is received, and this report will be updated as significant data is received. By improving their products and support and/or by having more satisfied customer voices heard, Contenders may become Leaders and Niche sellers may become High Performers.

Trust

Keeping our ratings unbiased is our top priority. We require the use of a LinkedIn account or verified business email address to validate a G2 user's identity and employer. We also validate users by partnering with sellers and organizations to securely authenticate users through select platforms. We do not allow users to review their current or former employers' products, or those of their employers' competitors. Additionally, all reviews are manually checked by our team after our algorithm filters out reviews that don't meet our submission requirements. All reviews must pass our moderation process before they are published.

Our G2 staff does not add any subjective input to the ratings, which are determined algorithmically based on data aggregated from publicly available online sources and social networks. Sellers cannot influence their ratings by spending time or money with us. Only the opinion of real users and data from public sources factor into the ratings.

Grid® Inclusion Criteria

All products in a G2 category that have at least 10 reviews from real users of the product are included on the Grid®. Inviting other users, such as colleagues and peers, to join G2 and share authentic product reviews will accelerate this process.

If a product is not yet listed on G2 and it fits the market definition above, then users are encouraged to suggest its addition to our Security Orchestration, Automation, and Response (SOAR) category.

Product Profiles

Product profiles and detailed charts are included for products with 10 or more reviews.

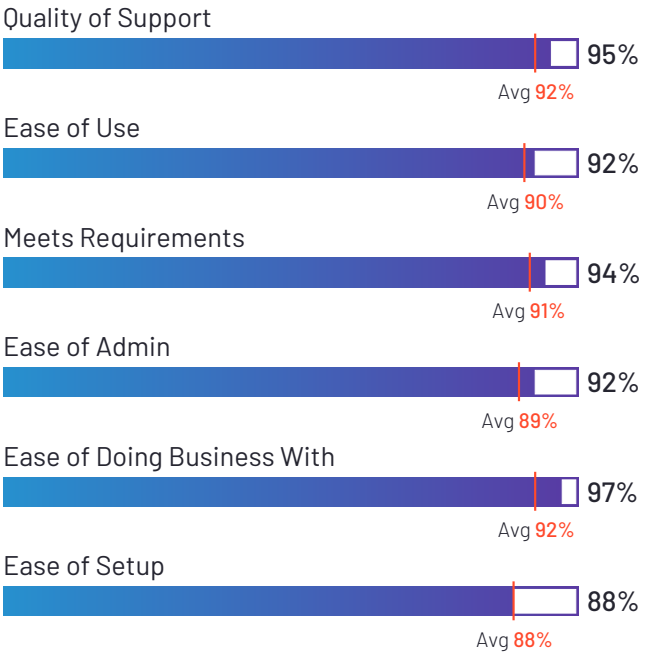
PhishER

4.7 ★★★★½ (155)

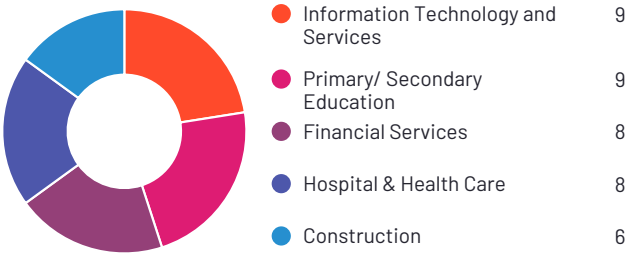
Leader FALL 2022

PhishER has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. PhishER has the largest Market Presence and received the highest Satisfaction score among products in Security Orchestration, Automation, and Response (SOAR). 98% of users rated it 4 or 5 stars, 94% of users believe it is headed in the right direction, and users said they would be likely to recommend PhishER at a rate of 93%. PhishER is also in the Incident Response category.

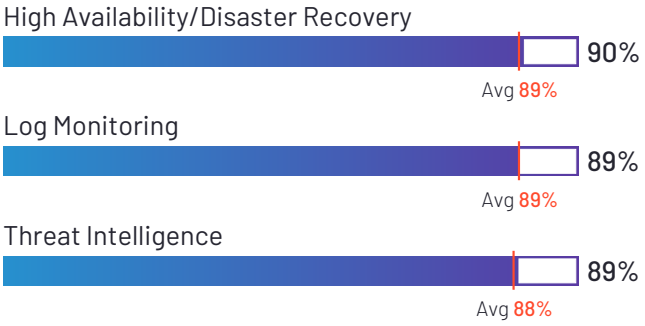
Satisfaction Ratings



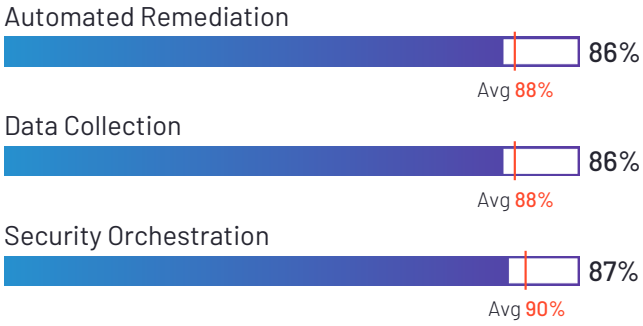
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
KnowBe4, Inc.

HQ Location
Clearwater, FL

Year Founded
2010

Employees (Listed On Linkedin)
1,654

Company Website
knowbe4.com

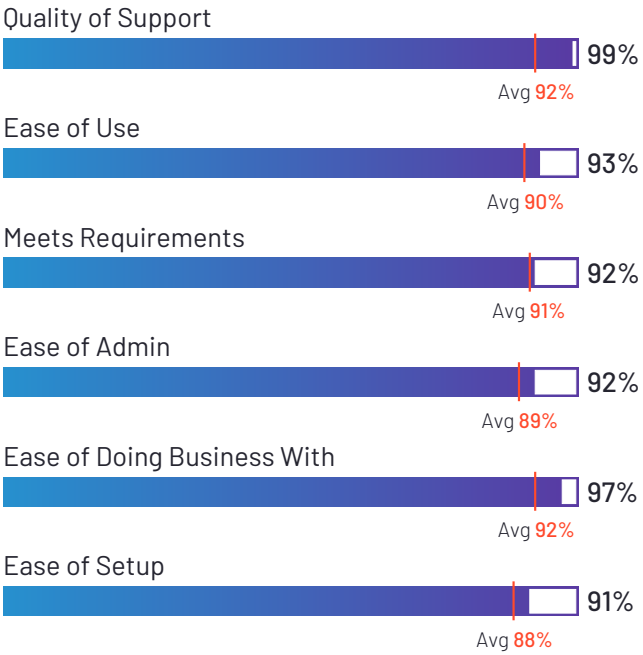
Tines

4.8 ★★★★★ (83)

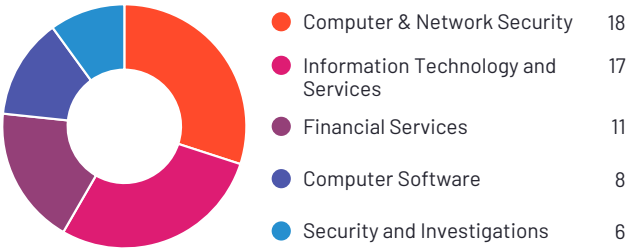
Leader FALL 2022

Tines has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 100% of users rated it 4 or 5 stars, 95% of users believe it is headed in the right direction, and users said they would be likely to recommend Tines at a rate of 97%. Tines is also in the iPaaS and Other Process Automation categories.

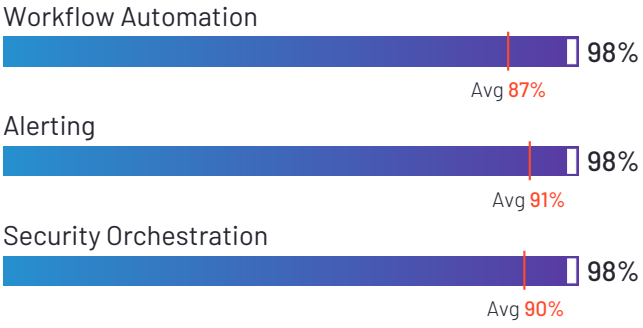
Satisfaction Ratings



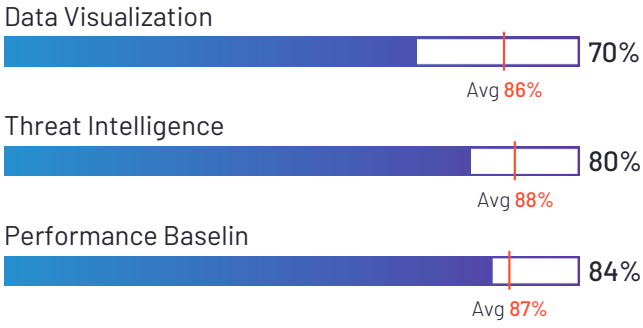
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Tines

HQ Location
Dublin, County Dublin

Year Founded
2018

Employees (Listed On Linkedin)
152

Company Website
www.tines.com

IBM Security

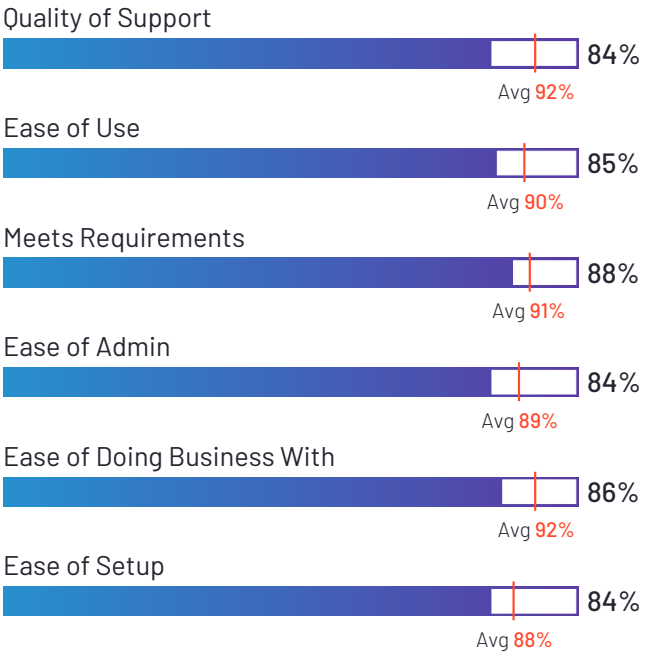
IBM Security QRadar

4.4 ★★★★½ (352)

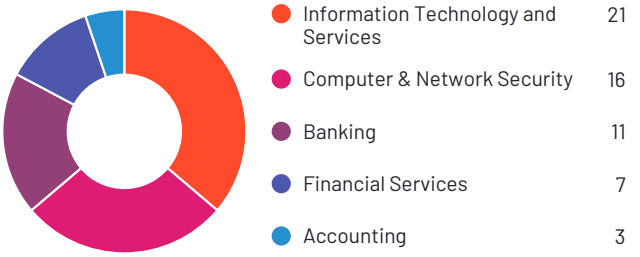
Leader FALL 2022

IBM Security QRadar has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 91% of users rated it 4 or 5 stars, 82% of users believe it is headed in the right direction, and users said they would be likely to recommend IBM Security QRadar at a rate of 87%. IBM Security QRadar is also in the Extended Detection and Response (XDR) Platforms, Cloud Security Monitoring and Analytics, User and Entity Behavior Analytics (UEBA), Digital Forensics, Network Traffic Analysis (NTA), Incident Response, and Security Information and Event Management (SIEM) categories.

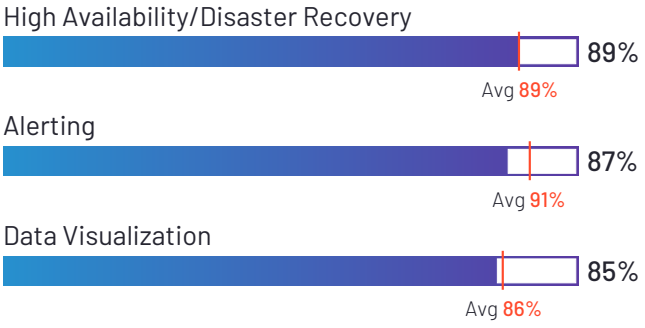
Satisfaction Ratings



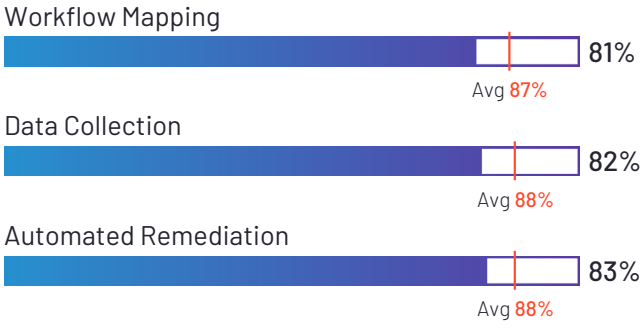
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
IBM

HQ Location
Armonk, NY

Year Founded
1911

Total Revenue
$73,621 (USD MM)

Employees (Listed On Linkedin)
531,710

Company Website
www.ibm.com

Microsoft Sentinel

4.4 ★★★★½ (97)

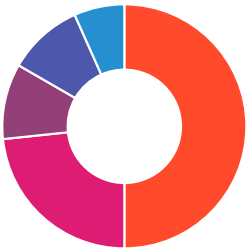
Leader FALL 2022

Microsoft Sentinel has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 98% of users rated it 4 or 5 stars, 89% of users believe it is headed in the right direction, and users said they would be likely to recommend Microsoft Sentinel at a rate of 89%. Microsoft Sentinel is also in the Security Information and Event Management (SIEM) category.

Satisfaction Ratings

		Avg
Quality of Support	84%	92%
Ease of Use	89%	90%
Meets Requirements	86%	91%
Ease of Admin	85%	89%
Ease of Doing Business With	88%	92%
Ease of Setup	84%	88%

Top Industries Represented



Information Technology and Services	15
Computer & Network Security	7
Banking	3
Computer Software	3
Accounting	2

Highest-Rated Features

		Avg
Security Orchestration	88%	90%
Log Monitoring	88%	89%
Alerting	87%	91%

Lowest-Rated Features

		Avg
Workflow Mapping	83%	87%
Workflow Automation	84%	87%
Data Visualization	85%	86%

Ownership
Microsoft

HQ Location
Redmond, WA

Year Founded
1975

Total Revenue
$143,015 (USD MM)

Employees (Listed On Linkedin)
223,768

Company Website
microsoft.com

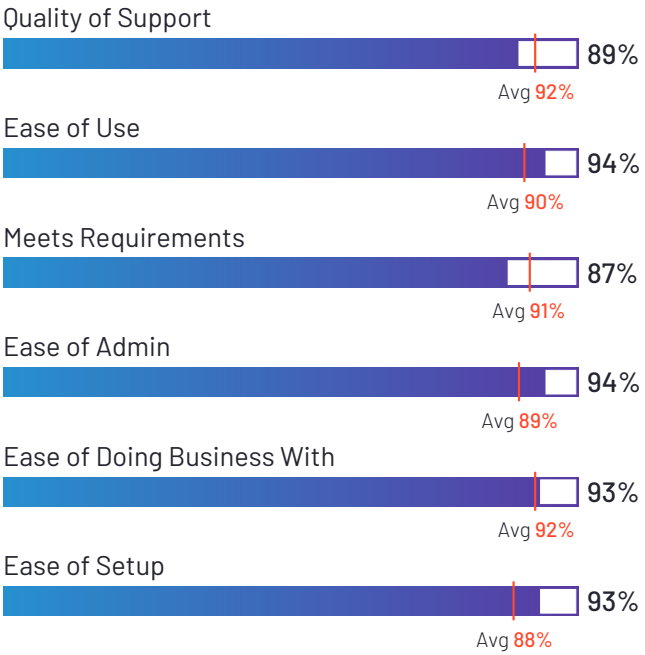
Palo Alto Networks Cortex XSOAR

4.5 ★★★★½ (13)

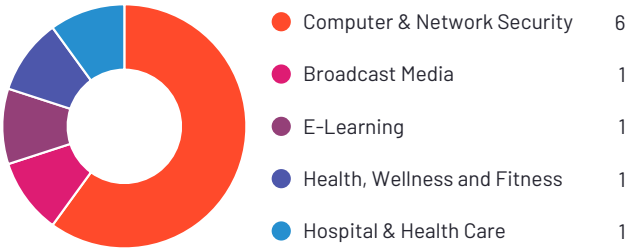
Leader FALL 2022

Palo Alto Networks Cortex XSOAR has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 100% of users rated it 4 or 5 stars, 89% of users believe it is headed in the right direction, and users said they would be likely to recommend Palo Alto Networks Cortex XSOAR at a rate of 91%.

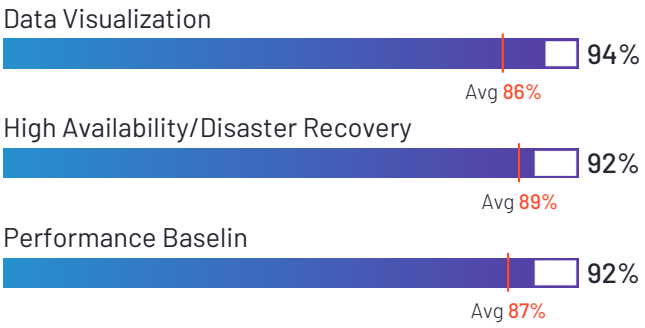
Satisfaction Ratings



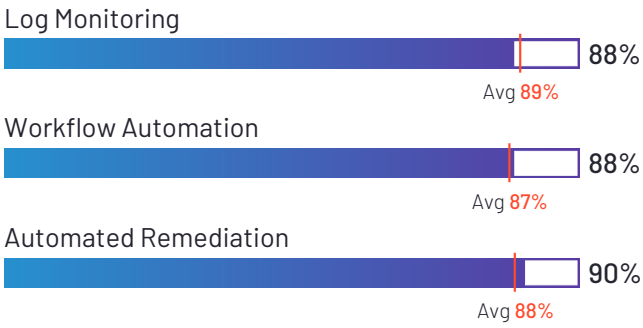
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Palo Alto Networks

HQ Location
Santa Clara, CA

Year Founded
2005

Total Revenue
$3,408 (USD MM)

Employees (Listed On Linkedin)
13,509

Company Website
paloaltonetworks.com

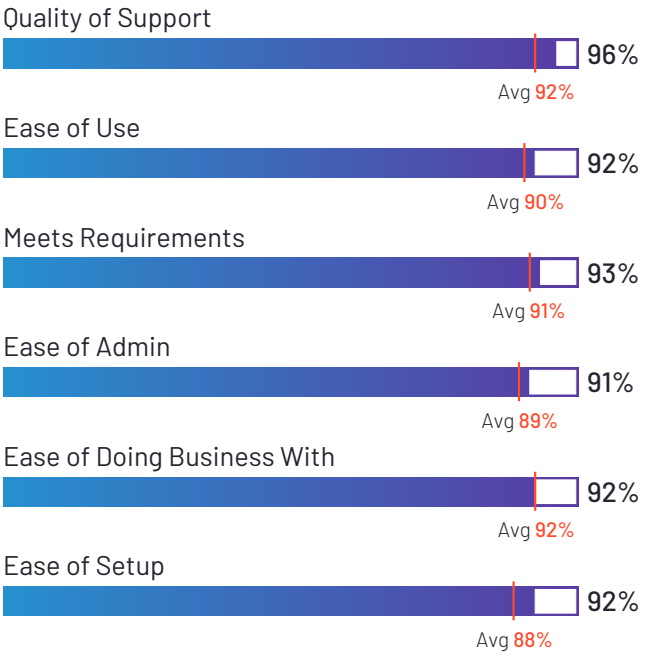
LogPoint

4.4 ★★★★½ (56)

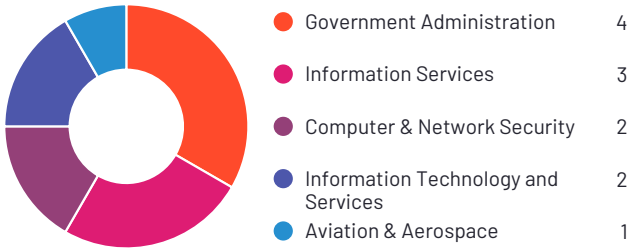
Leader FALL 2022

LogPoint has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend LogPoint at a rate of 91%. LogPoint is also in the Log Monitoring, Log Analysis, Security Information and Event Management (SIEM), Incident Response, Threat Intelligence, and User and Entity Behavior Analytics (UEBA) categories.

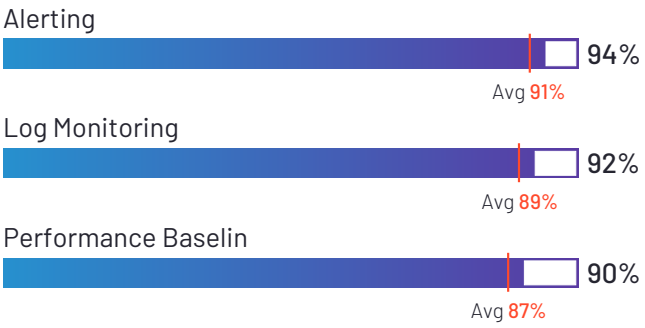
Satisfaction Ratings



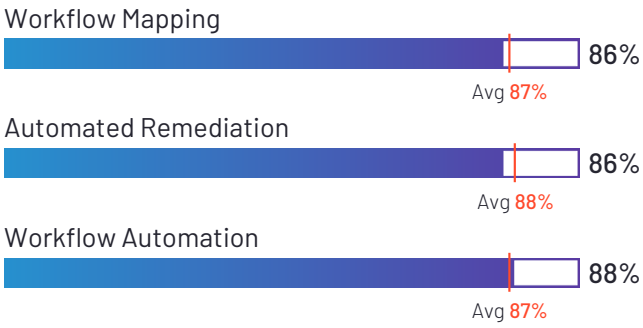
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Logpoint

HQ Location
Copenhagen, Capital Region

Year Founded
2001

Employees (Listed On Linkedin)
317

Company Website
logpoint.com

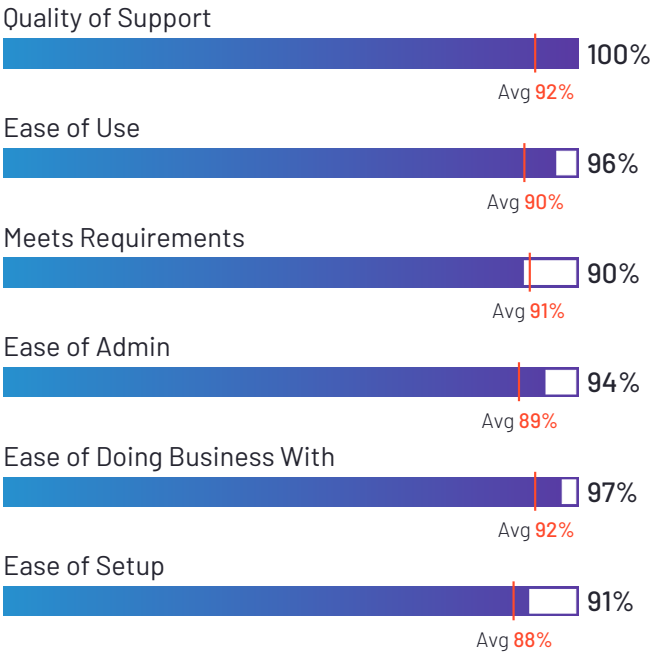
Blumira Automated Detection & Response

4.8 ★★★★★ (46)

High Performer FALL 2022

Blumira Automated Detection & Response has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Blumira Automated Detection & Response at a rate of 97%. Blumira Automated Detection & Response is also in the Network Detection and Response (NDR), Cloud Security Monitoring and Analytics, Log Monitoring, Intrusion Detection and Prevention Systems (IDPS), Cloud Infrastructure Monitoring , Incident Response, Security Information and Event Management (SIEM), and Managed Detection and Response (MDR) categories.

Satisfaction Ratings



Top Industries Represented

Information Technology and Services	4
Computer & Network Security	3
Financial Services	3
Automotive	2
Hospital & Health Care	2

Ownership
Blumira

HQ Location
Ann Arbor, Michigan

Year Founded
2018

Employees (Listed On Linkedin)
52

Company Website
blumira.com

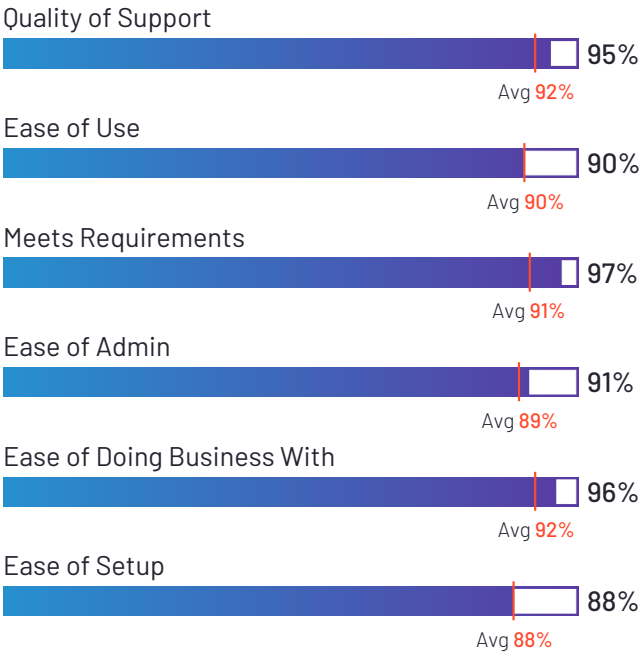
CrowdSec

4.7 ★★★★½ (62)

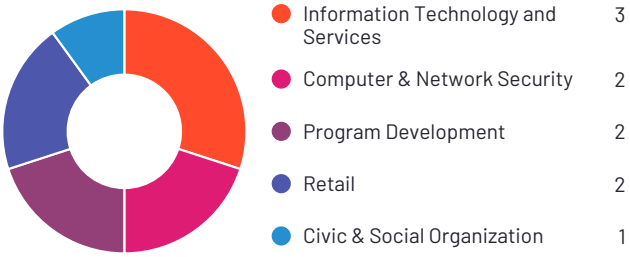
High Performer FALL 2022

CrowdSec has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 96% of users rated it 4 or 5 stars, 91% of users believe it is headed in the right direction, and users said they would be likely to recommend CrowdSec at a rate of 94%. CrowdSec is also in the Container Security, Endpoint Detection & Response (EDR), Threat Intelligence, Firewall Software, and Intrusion Detection and Prevention Systems (IDPS) categories.

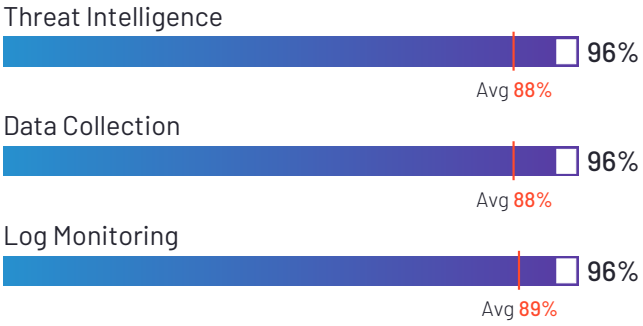
Satisfaction Ratings



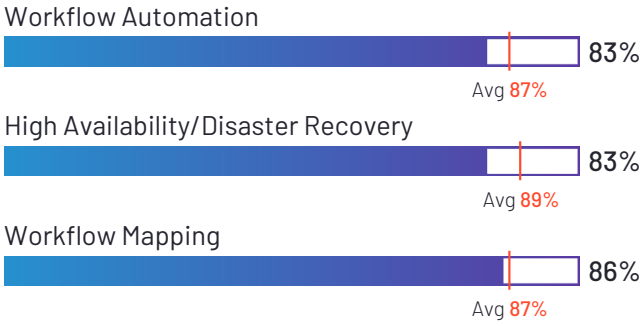
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
CrowdSec

HQ Location
Paris

Year Founded
2019

Employees (Listed On Linkedin)
21

Company Website
crowdsec.net

LogicHub

4.7 ★★★★½ (11)

High Performer FALL 2022

LogicHub has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend LogicHub at a rate of 95%. LogicHub is also in the Incident Response and Managed Detection and Response (MDR) categories.

Satisfaction Ratings

Quality of Support
N/A
Avg 92%

Ease of Use
N/A
Avg 90%

Meets Requirements
N/A
Avg 91%

Ease of Admin
N/A
Avg 89%

Ease of Doing Business With
N/A
Avg 92%

Ease of Setup
N/A
Avg 88%

*N/A is displayed when fewer than five responses were received for the question.

Top Industries Represented

Computer & Network Security	2
Electrical/ Electronic Manufacturing	2
Information Technology and Services	2
Airlines/ Aviation	1
Chemicals	1

Ownership
LogicHub

HQ Location
Mountain View, California

Year Founded
2016

Employees (Listed On Linkedin)
72

Company Website
logichub.com

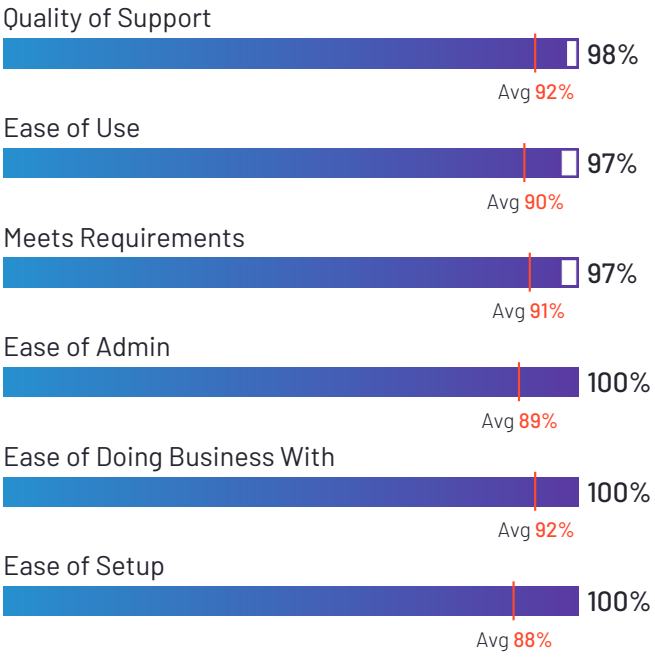
SIRP

4.7 ★★★★½ (26)

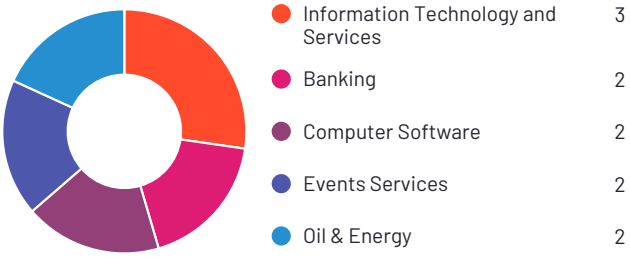
High Performer FALL 2022

SIRP has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 94% of users rated it 4 or 5 stars, 88% of users believe it is headed in the right direction, and users said they would be likely to recommend SIRP at a rate of 93%. SIRP is also in the Incident Response and Threat Intelligence categories.

Satisfaction Ratings



Top Industries Represented



Ownership
SIRP

HQ Location
London

Year Founded
2017

Employees (Listed On Linkedin)
16

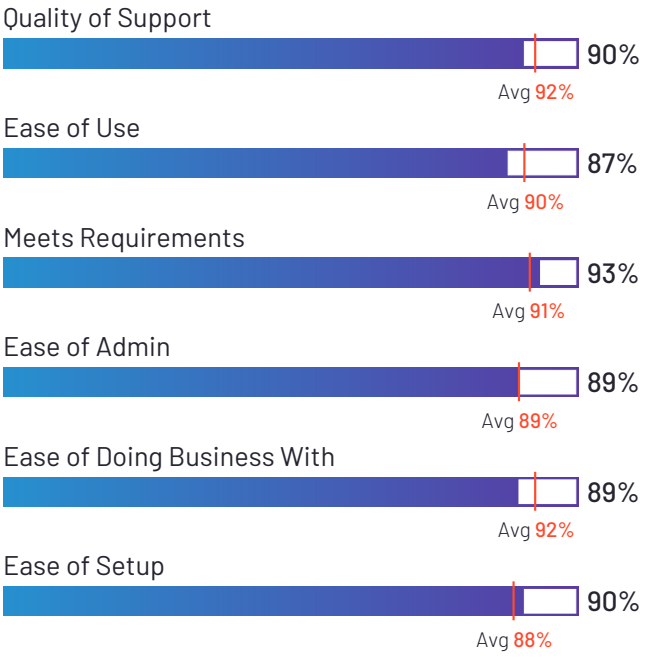
Company Website
www.sirp.io

Sumo Logic

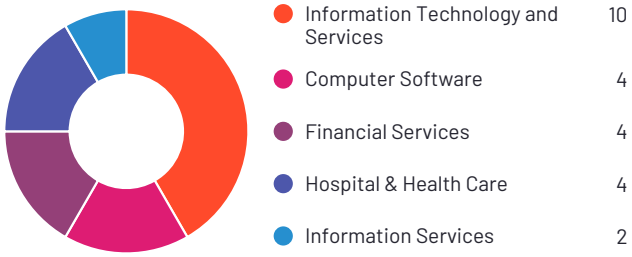
4.3 ★★★★½ (254)

Sumo Logic has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 97% of users rated it 4 or 5 stars, 86% of users believe it is headed in the right direction, and users said they would be likely to recommend Sumo Logic at a rate of 87%. Sumo Logic is also in the Cloud Security Monitoring and Analytics, Log Monitoring, Cloud Infrastructure Monitoring , Container Monitoring, Log Analysis, Incident Response, Security Information and Event Management (SIEM), Application Performance Monitoring (APM), and Observability Solution Suites categories.

Satisfaction Ratings



Top Industries Represented



Ownership
Sumo Logic

HQ Location
Redwood City, CA

Year Founded
2010

Employees (Listed On Linkedin)
1,064

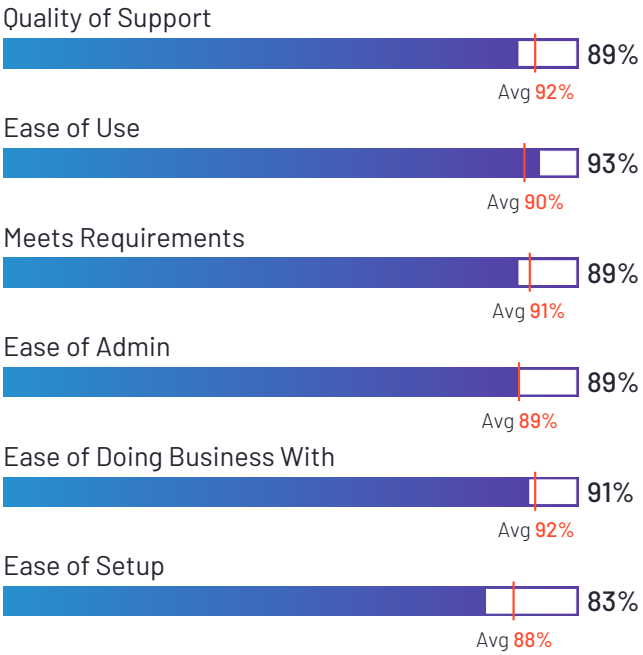
Company Website
sumologic.com

Demisto

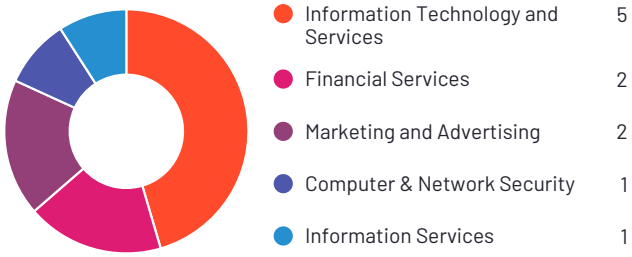
4.5 ★★★★½ (14)

Demisto has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 86% of users rated it 4 or 5 stars, 92% of users believe it is headed in the right direction, and users said they would be likely to recommend Demisto at a rate of 89%. Demisto is also in the Incident Management category.

Satisfaction Ratings



Top Industries Represented



Ownership
Palo Alto Networks

HQ Location
Santa Clara, CA

Year Founded
2005

Total Revenue
$3,408 (USD MM)

Employees (Listed On Linkedin)
13,509

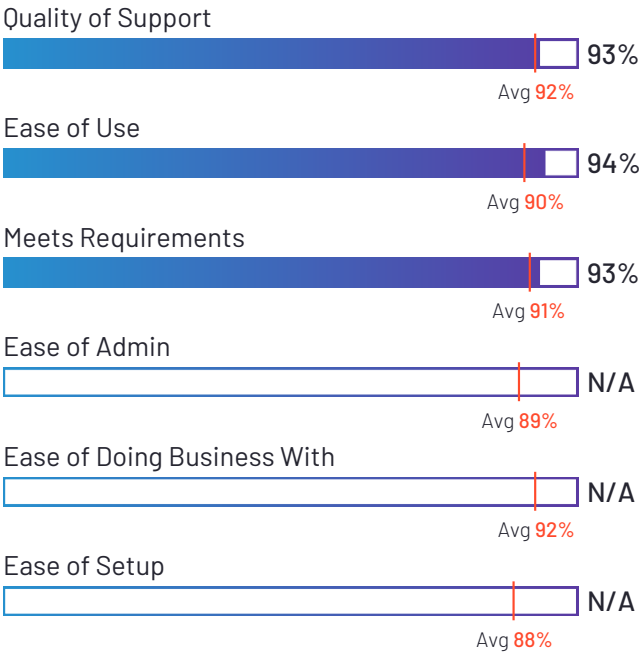
Company Website
paloaltonetworks.com

Swimlane

4.4 ★★★★½ (24)

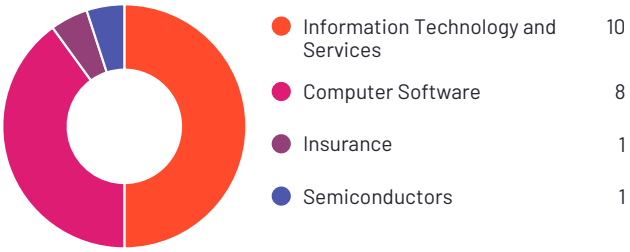
Swimlane has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars, 95% of users believe it is headed in the right direction, and users said they would be likely to recommend Swimlane at a rate of 91%. Swimlane is also in the Incident Response category.

Satisfaction Ratings



*N/A is displayed when fewer than five responses were received for the question.

Top Industries Represented



Ownership
Swimlane

HQ Location
Louisville, CO

Year Founded
2014

Employees (Listed On Linkedin)
166

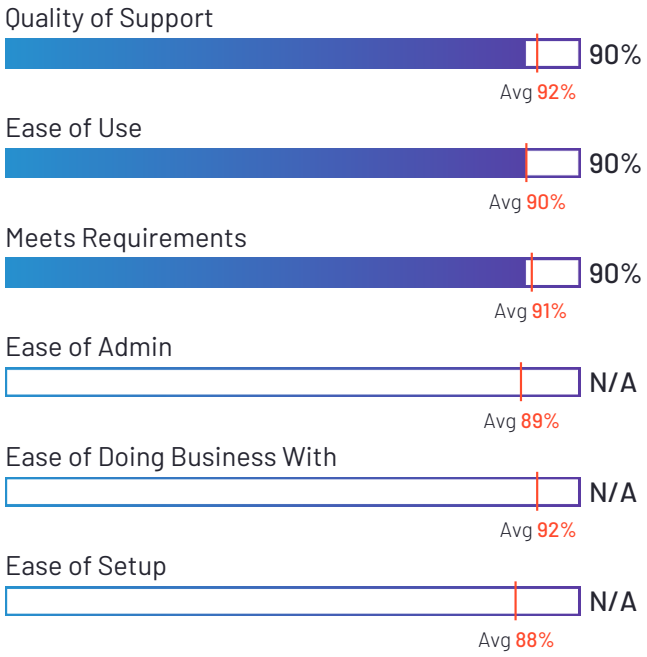
Company Website
swimlane.com

D3 Security

4.2 ★★★★☆ (68)

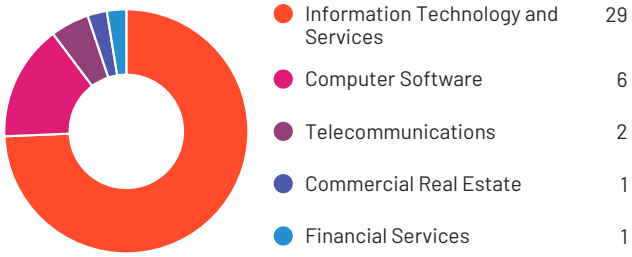
D3 Security has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 95% of users rated it 4 or 5 stars, 95% of users believe it is headed in the right direction, and users said they would be likely to recommend D3 Security at a rate of 87%. D3 Security is also in the Incident Response and Protective Intelligence Platforms categories.

Satisfaction Ratings



*N/A is displayed when fewer than five responses were received for the question.

Top Industries Represented



Ownership
D3 Security Management Systems

HQ Location
Vancouver, British Columbia

Year Founded
2004

Employees (Listed On Linkedin)
131

Company Website
d3security.com

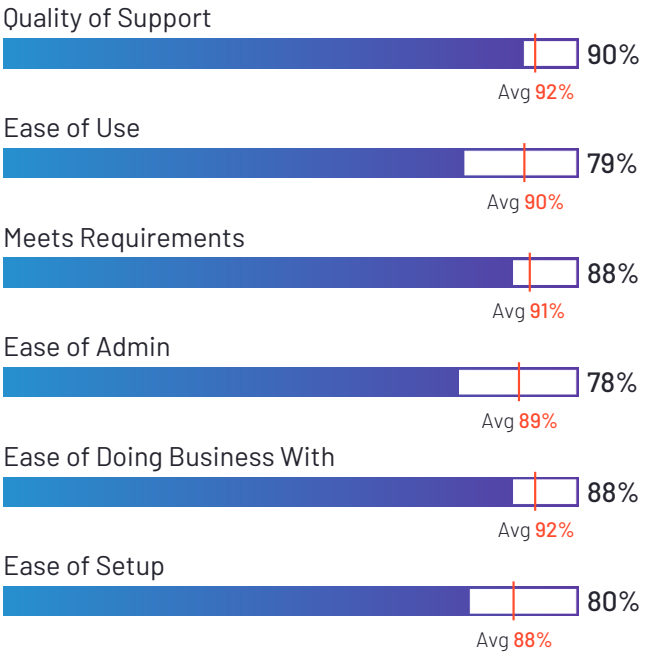
IBM Security

IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform

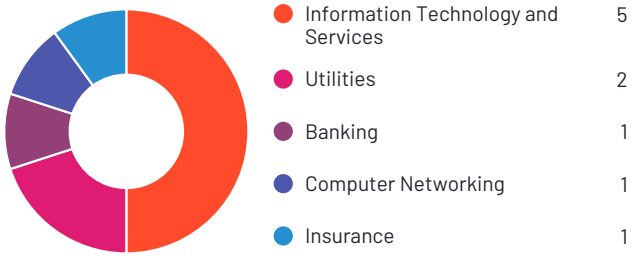
4.3 ★★★★½ (16)

IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 92% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform at a rate of 85%. IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform is also in the ServiceNow Store Apps, Data Breach Notification, and Incident Response categories.

Satisfaction Ratings



Top Industries Represented



Ownership
IBM

HQ Location
Armonk, NY

Year Founded
1911

Total Revenue
$73,621 (USD MM)

Employees (Listed On Linkedin)
531,710

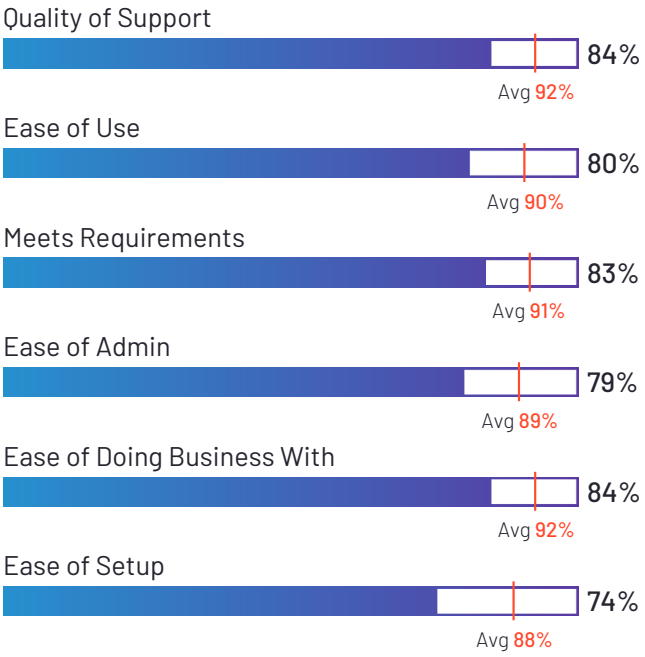
Company Website
www.ibm.com

Siemplify - Google Cloud

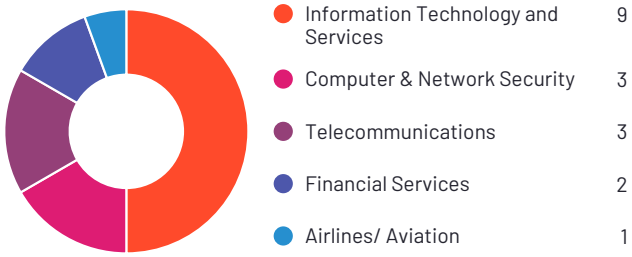
4.4 (32)

Siemplify - Google Cloud has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 95% of users rated it 4 or 5 stars, 95% of users believe it is headed in the right direction, and users said they would be likely to recommend Siemplify - Google Cloud at a rate of 88%.

Satisfaction Ratings



Top Industries Represented



Ownership
Siemplify

HQ Location
New York, NY

Year Founded
2015

Employees (Listed On Linkedin)
64

Company Website
siemplify.co

Satisfaction Ratings for Security Orchestration, Automation, and Response (SOAR)

G2 reviewers rated software sellers' ability to satisfy their needs as shown in the table below.

	Satisfaction		Satisfaction by Category						Net Promoter Score (NPS)
	Likelihood to Recommend	Product Going in Right Direction?	Meets Requirements	Ease of Admin	Ease of Doing Business With	Quality of Support	Ease of Setup	Ease of Use	Net Promoter Score (NPS) (Range from -100 to +100)
PhishER	93%	94%	94%	92%	97%	95%	88%	92%	81
Tines	97%	95%	92%	92%	97%	99%	91%	93%	92
IBM Security QRadar	87%	82%	88%	84%	86%	84%	84%	85%	55
Microsoft Sentinel	89%	89%	86%	85%	88%	84%	84%	89%	60
Palo Alto Networks Cortex XSOAR	91%	89%	87%	94%	93%	89%	93%	94%	76
LogPoint	91%	100%	93%	91%	92%	96%	92%	92%	65
Blumira Automated Detection & Response	97%	100%	90%	94%	97%	100%	91%	96%	90
CrowdSec	94%	91%	97%	91%	96%	95%	88%	90%	84
LogicHub	95%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	100
SIRP	93%	88%	97%	100%	100%	98%	100%	97%	77
Sumo Logic	87%	86%	93%	89%	89%	90%	90%	87%	62
Demisto	89%	92%	89%	89%	91%	89%	83%	93%	64
Swimlane	91%	95%	93%	N/A	N/A	93%	N/A	94%	75
D3 Security	87%	95%	90%	N/A	N/A	90%	N/A	90%	53
IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform	85%	100%	88%	78%	88%	90%	80%	79%	46
Siemplify - Google Cloud	88%	95%	83%	79%	84%	84%	74%	80%	59
Average	91%	93%	91%	89%	92%	92%	88%	90%	71

*N/A is displayed when fewer than five responses were received for the question.

**Net Promoter Score ranges from -100 to +100

Additional Data for Security Orchestration, Automation, and Response (SOAR)

The table below includes a breakdown of the customer segments for each product, as represented by G2 reviewers.

Customers by Size

	Small Business (50 or fewer emp.)	Mid-Market (51-1000 emp.)	Enterprise (>1000 emp.)
PhishER	11%	80%	9%
Tines	25%	42%	34%
IBM Security QRadar	20%	20%	59%
Microsoft Sentinel	30%	30%	40%
Palo Alto Networks Cortex XSOAR	23%	23%	54%
LogPoint	20%	65%	15%
Blumira Automated Detection & Response	15%	65%	20%
CrowdSec	68%	16%	16%
LogicHub	18%	27%	55%
SIRP	44%	22%	33%
Sumo Logic	11%	46%	43%
Demisto	36%	43%	21%
Swimlane	25%	65%	10%
D3 Security	24%	29%	46%
IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform	8%	8%	85%
Siemplify - Google Cloud	9%	18%	73%
Average	24%	37%	38%

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR)(continued)

The table below highlights implementation and deployment data as indicated in real user reviews on G2.

Implementation

	Deployment		Implementation Time	Implementation Method				Number of Users Purchased	Contract Term
	Cloud	On-Premises	Avg. Months to Go Live	In-House Team	Seller Services Team	Third-Party Consultant	Don't know	Median Number of Users Bought	Avg. Contract Term (Months)
PhishER	83%	17%	1.4	91%	7%	0%	2%	75	26
Tines	82%	18%	0.5	93%	7%	0%	0%	3	7
IBM Security QRadar	33%	67%	3.2	44%	44%	8%	5%	17	27
Microsoft Sentinel	78%	22%	3.2	52%	14%	24%	10%	12	16
Palo Alto Networks Cortex XSOAR	38%	63%	2.4	13%	75%	0%	13%	17	26
LogPoint	9%	91%	2.1	36%	27%	9%	27%	7	9
Blumira Automated Detection & Response	92%	8%	0.5	83%	17%	0%	0%	17	13
CrowdSec	50%	50%	0.2	86%	0%	0%	14%	17	0
LogicHub	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SIRP	71%	29%	0.7	N/A	N/A	N/A	N/A	N/A	N/A
Sumo Logic	75%	25%	1.1	75%	25%	0%	0%	12	N/A
Demisto	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Swimlane	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
D3 Security	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform	71%	29%	4.7	80%	20%	0%	0%	17	N/A
Siemplify - Google Cloud	11%	89%	3.7	38%	62%	0%	0%	7	24

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR) (continued)

The table below highlights the average user adoption of each product as indicated in real user reviews on G2.

User Adoption and Return on Investment (ROI)

	User Adoption	Payback Period
	Average User Adoption	Estimated ROI (payback period in months)
PhishER	75%	16
Tines	35%	7
IBM Security QRadar	59%	29
Microsoft Sentinel	47%	22
Palo Alto Networks Cortex XSOAR	34%	15
LogPoint	34%	29
Blumira Automated Detection & Response	73%	6
CrowdSec	61%	3
LogicHub	N/A	N/A
SIRP	N/A	N/A
Sumo Logic	79%	N/A
Demisto	N/A	N/A
Swimlane	N/A	N/A
D3 Security	N/A	N/A
IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform	53%	N/A
Siemplify - Google Cloud	54%	32
Average	55%	17

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR)(continued)

The table below highlights third-party market presence data used to inform the G2's Market Presence Score that highlights each product's impact and influence in the category.

Market Presence

	Seller Name	Year Founded	Revenue ($MM)	Employees on LinkedIn (Seller)	LinkedIn Followers	Twitter Followers (Seller)	Glassdoor Rating
PhishER	KnowBe4, Inc.	2010	N/A	1,654	122,592	13,390	4.2
Tines	Tines	2018	N/A	152	9,600	1,685	4.9
IBM Security QRadar	IBM	1911	$73,621	531,710	14,296,858	696,414	4.1
Microsoft Sentinel	Microsoft	1975	$143,015	223,768	17,587,038	11,472,744	4.4
Palo Alto Networks Cortex XSOAR	Palo Alto Networks	2005	$3,408	13,509	745,841	119,476	4.1
LogPoint	Logpoint	2001	N/A	317	14,542	1,002	N/A
Blumira Automated Detection & Response	Blumira	2018	N/A	52	4,367	0	5.0
CrowdSec	CrowdSec	2019	N/A	21	4,305	20	N/A
LogicHub	LogicHub	2016	N/A	72	2,932	356	4.7
SIRP	SIRP	2017	N/A	16	1,630	69	N/A
Sumo Logic	Sumo Logic	2010	N/A	1,064	84,245	6,762	3.9
Demisto	Palo Alto Networks	2005	$3,408	13,509	745,841	119,476	4.1
Swimlane	Swimlane	2014	N/A	166	8,046	1,578	4.5
D3 Security	D3 Security Management Systems	2004	N/A	131	14,119	1,093	3.9
IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform	IBM	1911	$73,621	531,710	14,296,858	696,414	4.1
Siemplify - Google Cloud	Siemplify	2015	N/A	64	12,840	2,832	4.2

*N/A is displayed when data is not publicly available.