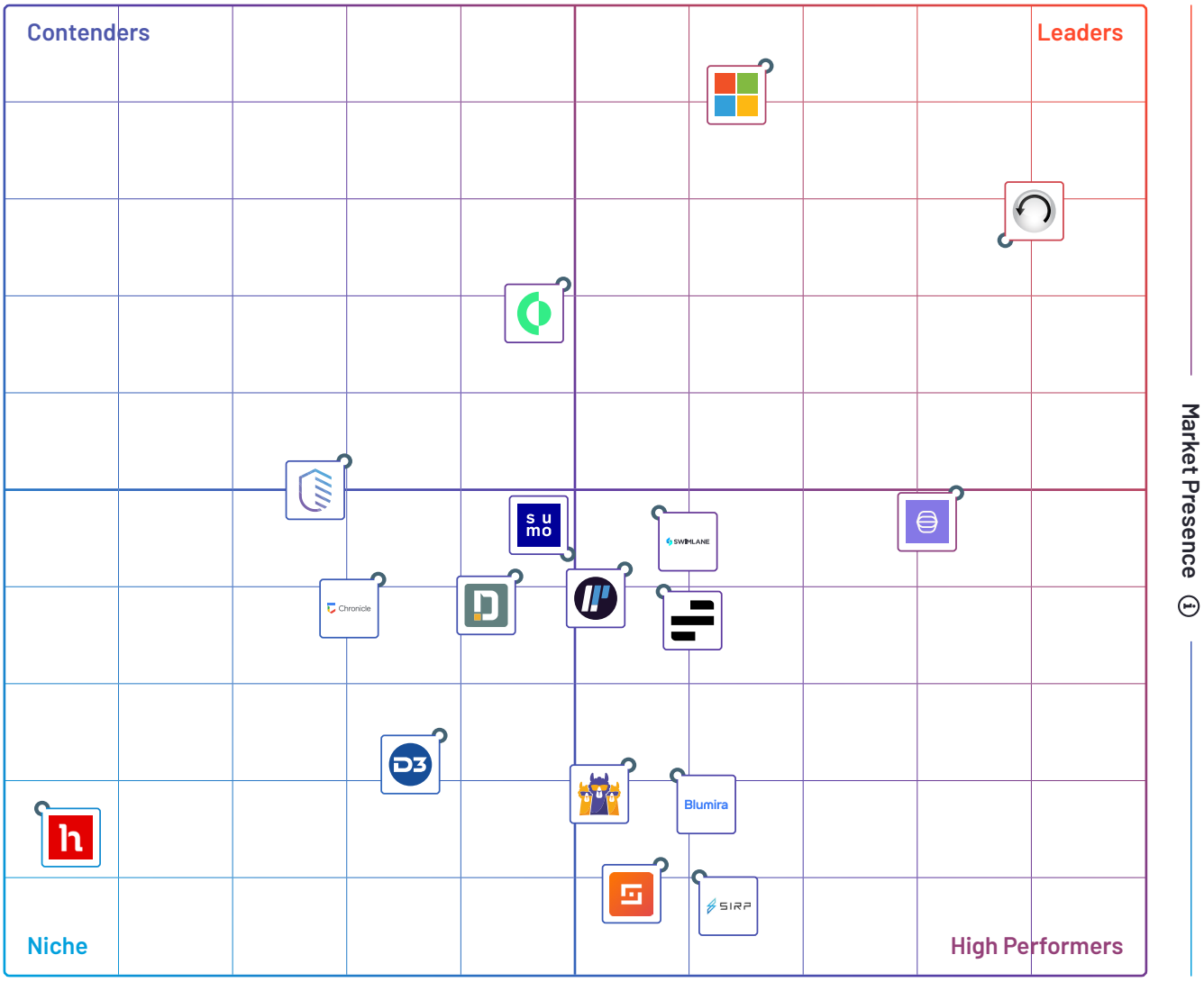
Grid® Report for Security Orchestration, Automation, and Response (SOAR) | Summer 2023

SOAR Software



G2 Grid® Scoring

(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 platforms 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 May 23, 2023. 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 and Microsoft Sentinel
- High Performing products have high customer Satisfaction scores and low Market Presence compared to the rest of the category. High Performers include: Tines, Swimlane, Torq, Logpoint, Blumira Automated Detection & Response, CrowdSec, SIRP, and Shuffle
- 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: Palo Alto Networks Cortex XSOAR and IBM Security QRadar SOAR
- 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: Sumo Logic, Demisto, Chronicle SOAR (formerly Siemplify), D3 Security, and LogicHub

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	202	90	79	84
Microsoft Sentinel	95	68	99	83

High Performers

Tines	151	86	50	68
Swimlane	25	58	47	53
Torq	18	58	38	48
Logpoint	28	55	41	48
Blumira Automated Detection & Response	23	60	17	38
CrowdSec	28	55	18	37
SIRP	19	62	5	33
Shuffle	12	58	7	33

Contenders

Palo Alto Networks Cortex XSOAR	18	49	73	61
IBM Security QRadar SOAR	14	29	53	41

(Grid® Scores for Security Orchestration, Automation, and Response (SOAR) continues on next page)

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

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

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.

Niche

	# of Reviews	Satisfaction	Market Presence	G2 Score
Sumo Logic	37	49	42	46
Demisto	14	45	40	42
Chronicle SOAR (formerly Siemplify)	23	32	40	36
D3 Security	42	37	22	29
LogicHub	11	0	13	7

* 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) | Summer 2023 is based on scores calculated using the G2 algorithm v3.0 from reviews collected through May 23, 2023. 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. For more details on Grid® Scoring, please view the G2 Scoring Methodology here.

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.

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 May 23, 2023. 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.

(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)

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.

G2 may occasionally offer incentives for honest reviews to help us gather a full and accurate data set. These incentives are offered as thank-yous for approved reviews. Incentives are never conditioned upon the substance of the review, positive or negative. Each such incentivized review is disclosed with an "Incentivized Review" banner.

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.

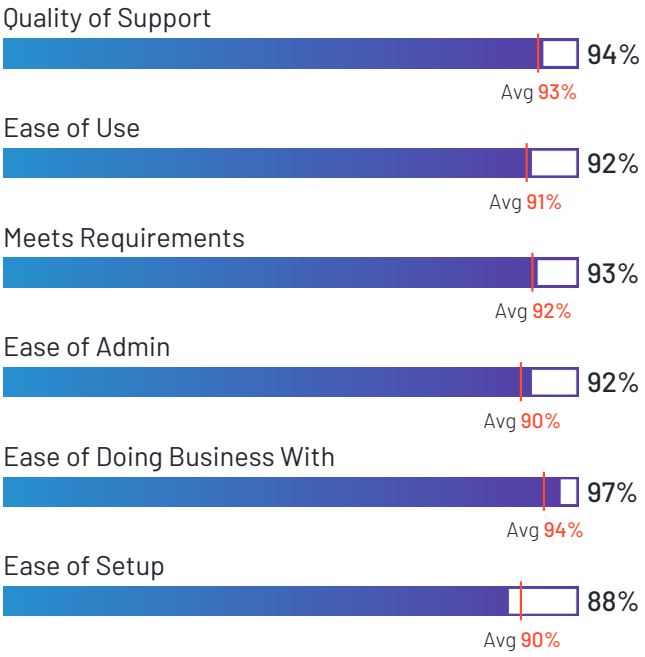
PhishER

4.6 ★★★★½ (278)

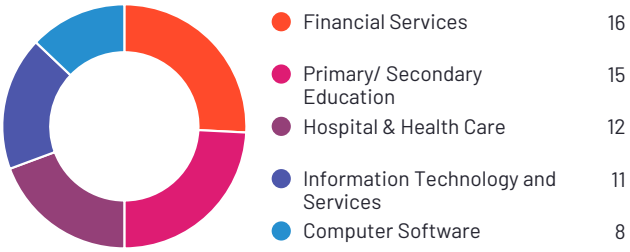
Leader SUMMER 2023

PhishER has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. PhishER received the highest Satisfaction score among products in Security Orchestration, Automation, and Response (SOAR). 99% 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.

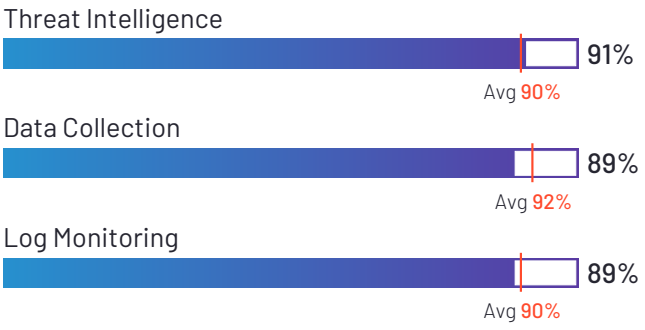
Satisfaction Ratings



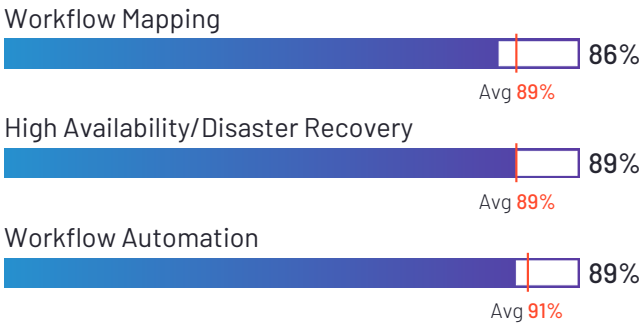
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
KnowBe4, Inc.

HQ Location
Clearwater, FL

Year Founded
2010

Employees (Listed On Linkedin)
1,756

Company Website
knowbe4.com

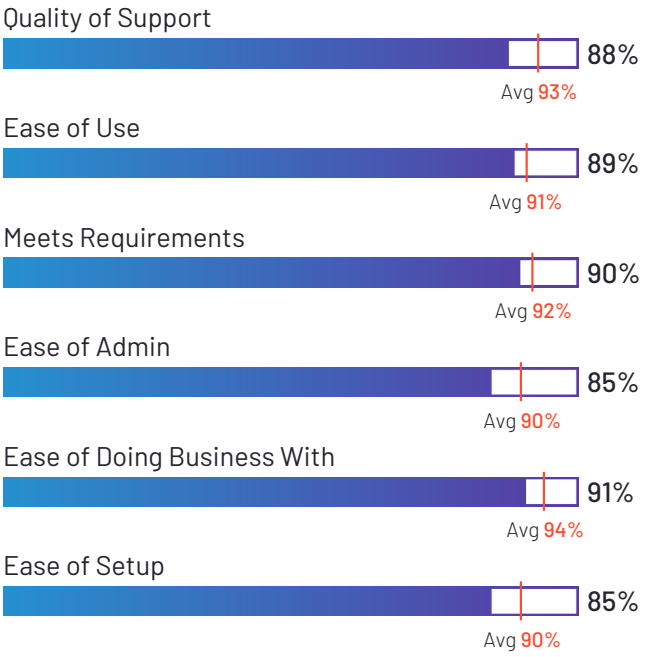
Microsoft Sentinel

4.4 ★★★★½ (182)

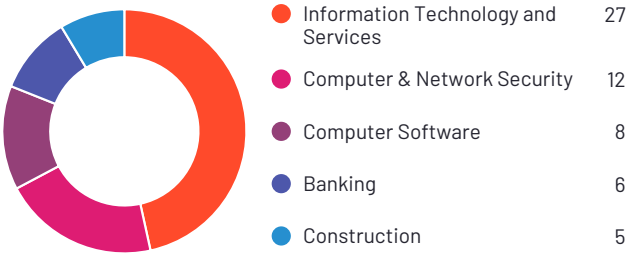
Leader SUMMER 2023

Microsoft Sentinel has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. Microsoft Sentinel has the largest Market Presence among products in Security Orchestration, Automation, and Response (SOAR). 98% of users rated it 4 or 5 stars, 93% 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.

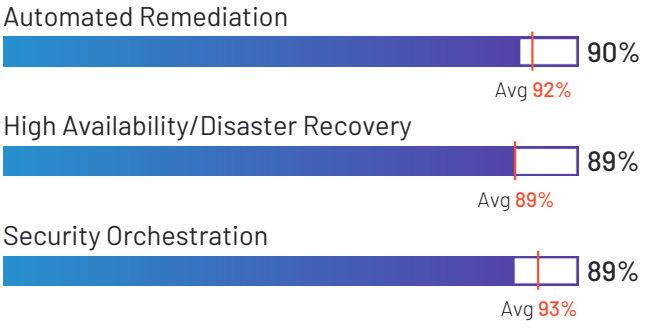
Satisfaction Ratings



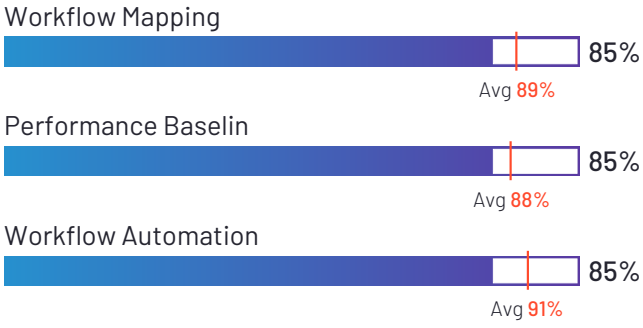
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Microsoft

HQ Location
Redmond, WA

Year Founded
1975

Employees (Listed On Linkedin)
224,717

Company Website
microsoft.com

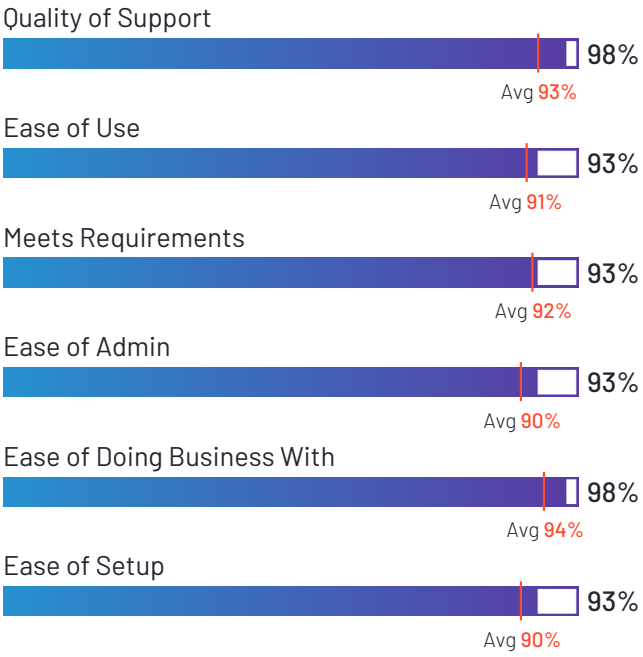
Tines

4.8 ★★★★★ (168)

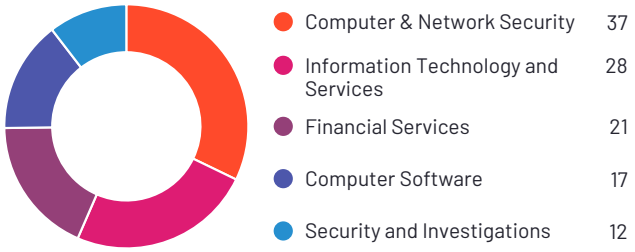
High Performer SUMMER 2023

Tines 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, 98% 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.

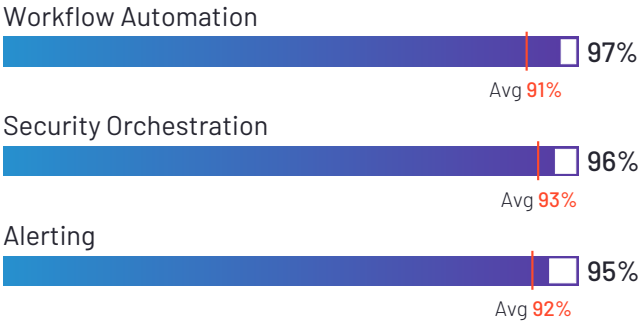
Satisfaction Ratings



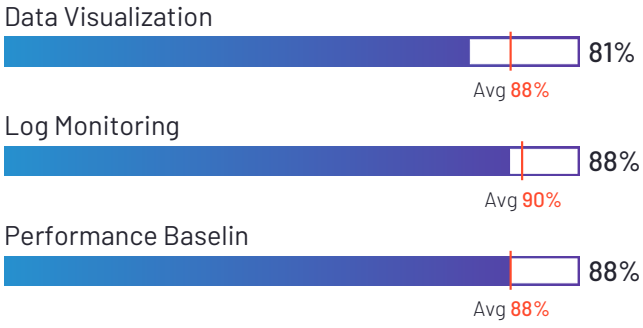
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Tines

HQ Location
Dublin, County Dublin

Year Founded
2018

Employees (Listed On Linkedin)
177

Company Website
www.tines.com

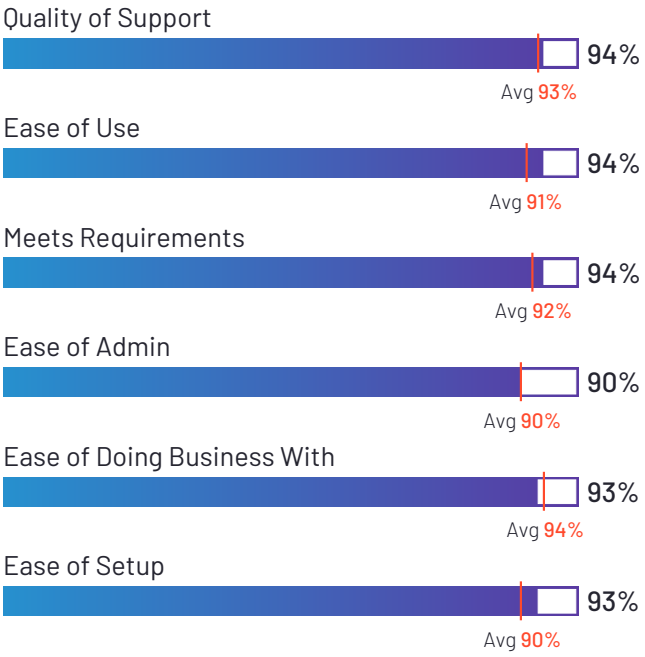
Swimlane

4.5 (30)

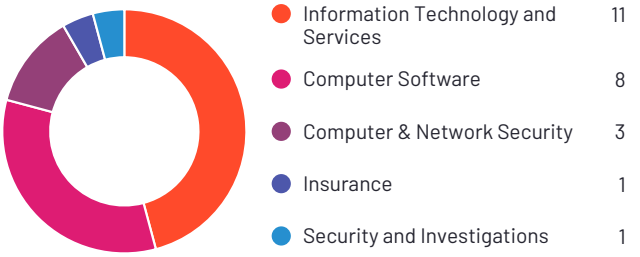
High Performer SUMMER 2023

Swimlane 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, 96% 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.

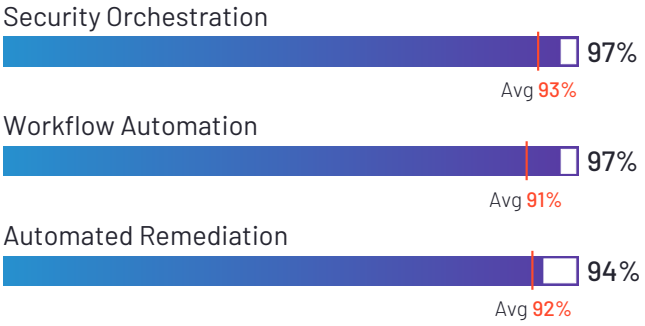
Satisfaction Ratings



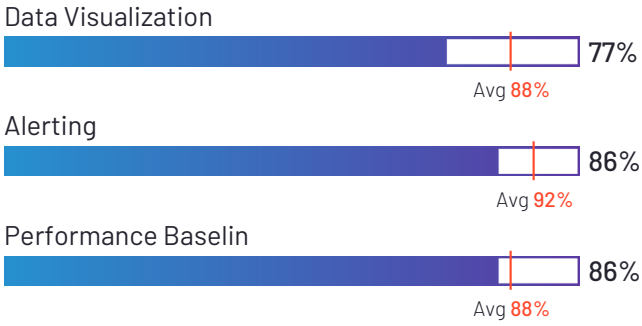
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Swimlane

HQ Location
Louisville, CO

Year Founded
2014

Employees (Listed On Linkedin)
219

Company Website
swimlane.com

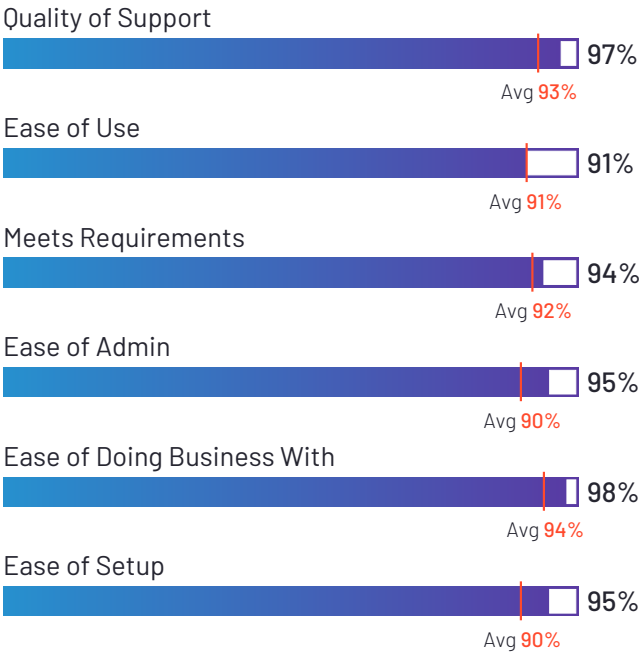
Torq

4.7 ★★★★½ (18)

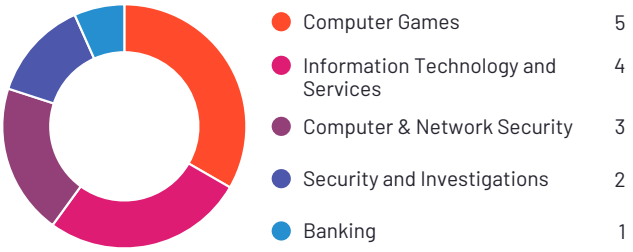
High Performer SUMMER 2023

Torq 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 Torq at a rate of 94%.

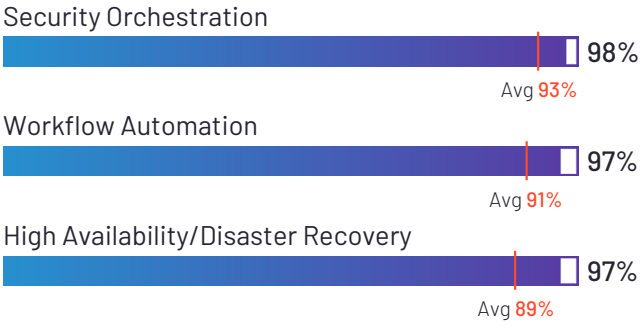
Satisfaction Ratings



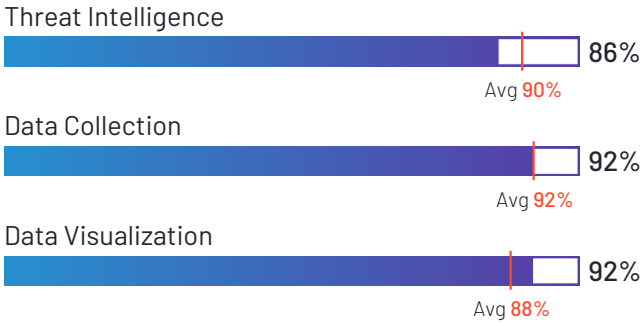
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
torq

Year Founded
2020

Employees (Listed On Linkedin)
126

Company Website
torq.io

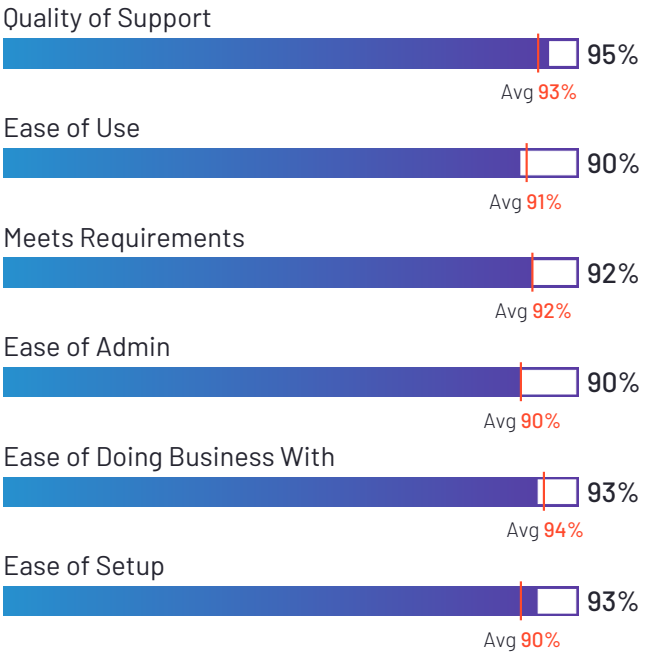
Logpoint

4.4 ★★★★½ (86)

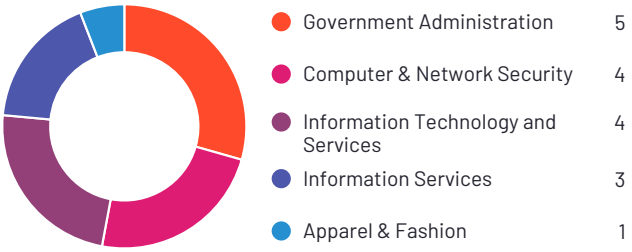
High Performer SUMMER 2023

Logpoint 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 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, User and Entity Behavior Analytics (UEBA), and SAP Store categories.

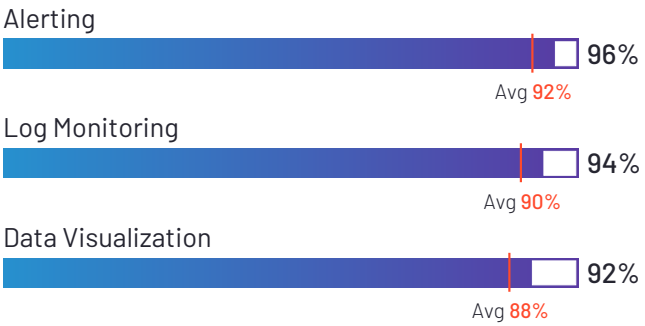
Satisfaction Ratings



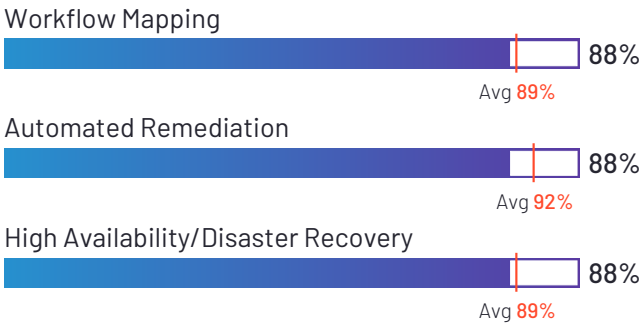
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Logpoint

HQ Location
Copenhagen, Capital Region

Year Founded
2001

Employees (Listed On Linkedin)
305

Company Website
logpoint.com

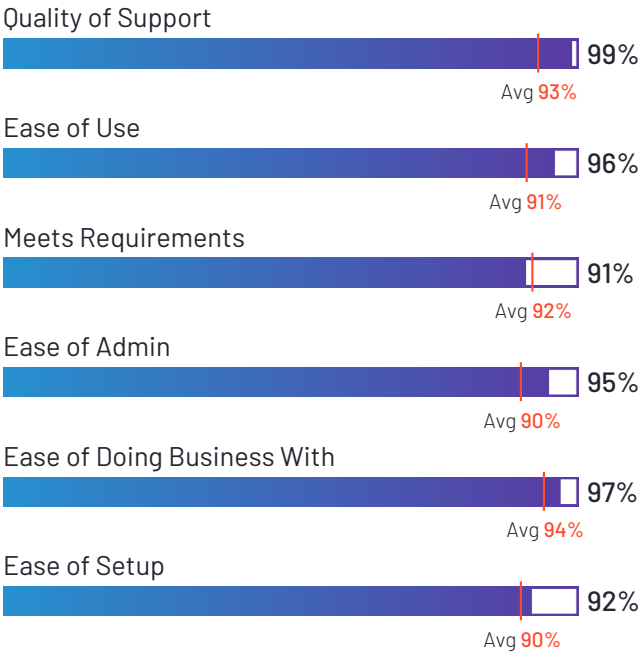
Blumira Automated Detection & Response

4.7 ★★★★½ (85)

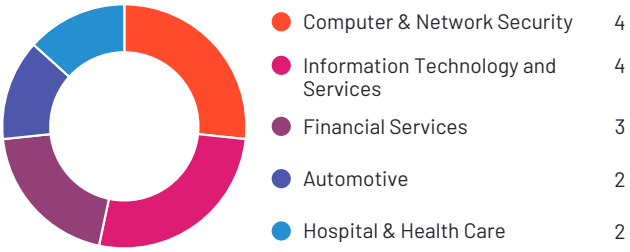
High Performer SUMMER 2023

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



Ownership
Blumira

HQ Location
Ann Arbor, Michigan

Year Founded
2018

Employees (Listed On Linkedin)
53

Company Website
blumira.com

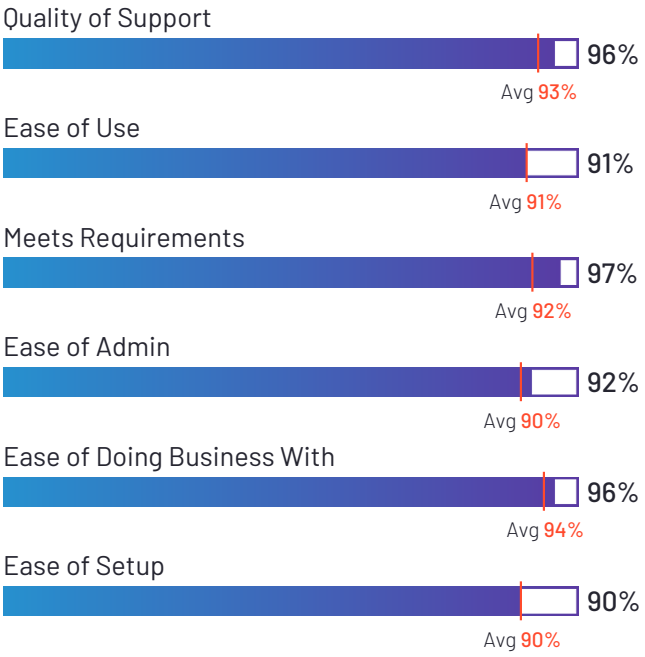
CrowdSec

4.7 ★★★★½ (74)

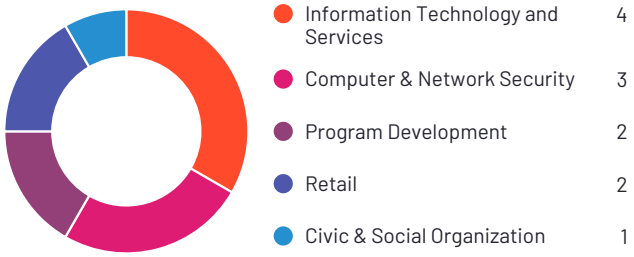
High Performer SUMMER 2023

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, 92% of users believe it is headed in the right direction, and users said they would be likely to recommend CrowdSec at a rate of 95%. CrowdSec is also in the Intrusion Detection and Prevention Systems (IDPS), Container Security, Endpoint Detection & Response (EDR), Threat Intelligence, and Firewall Software categories.

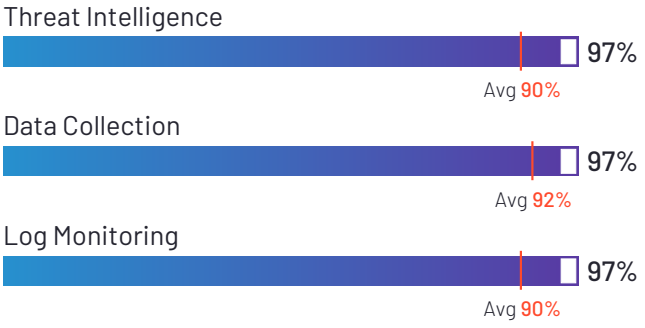
Satisfaction Ratings



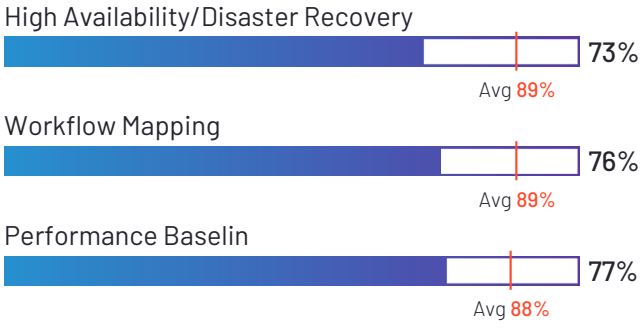
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
CrowdSec

HQ Location
Paris

Year Founded
2019

Employees (Listed On Linkedin)
32

Company Website
crowdsec.net

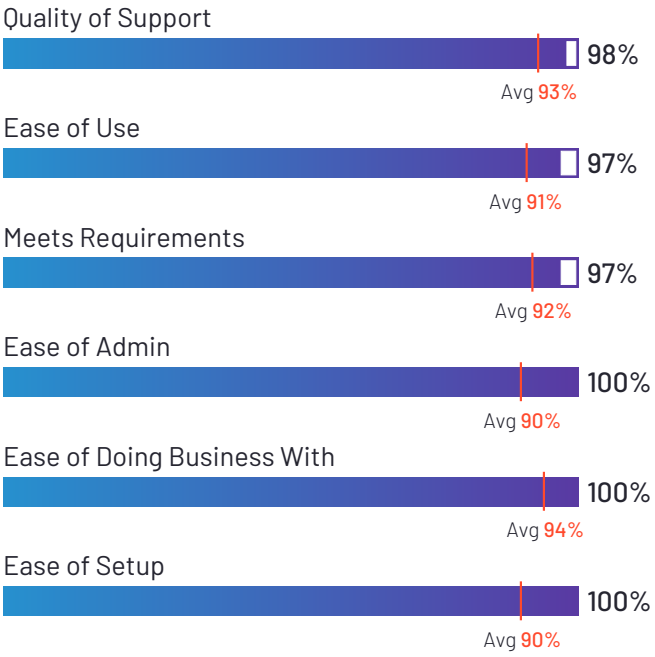
SIRP

4.7 ★★★★½ (27)

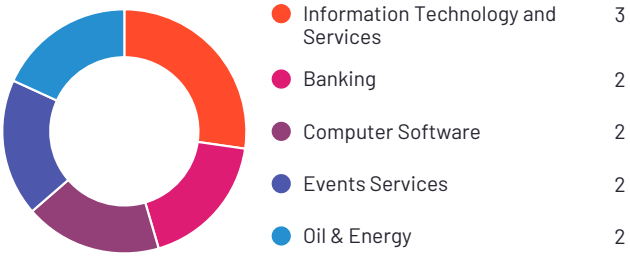
High Performer SUMMER 2023

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. 95% 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 SIRP at a rate of 94%. 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)
14

Company Website
www.sirp.io

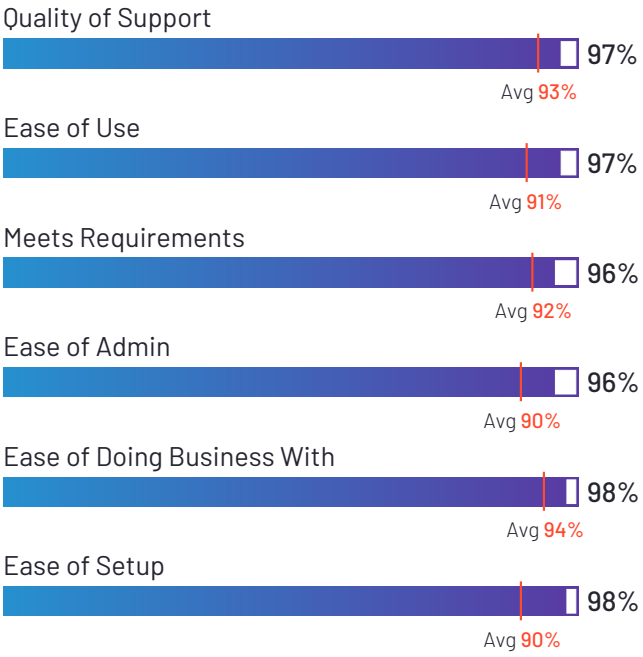
Shuffle

4.8 ★★★★★ (12)

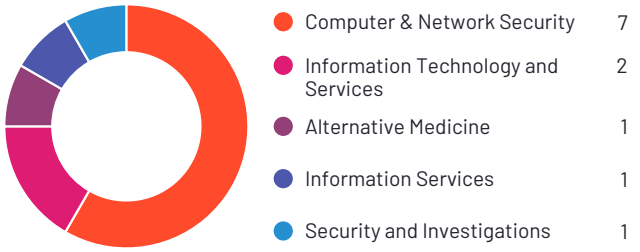
High Performer SUMMER 2023

Shuffle 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, 91% of users believe it is headed in the right direction, and users said they would be likely to recommend Shuffle at a rate of 96%.

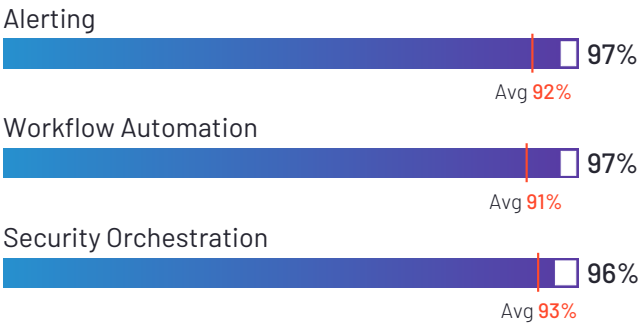
Satisfaction Ratings



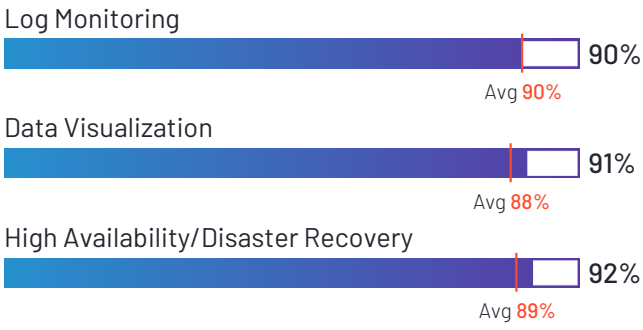
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Shuffle AS

HQ Location
San Francisco, CA

Employees (Listed On Linkedin)
6

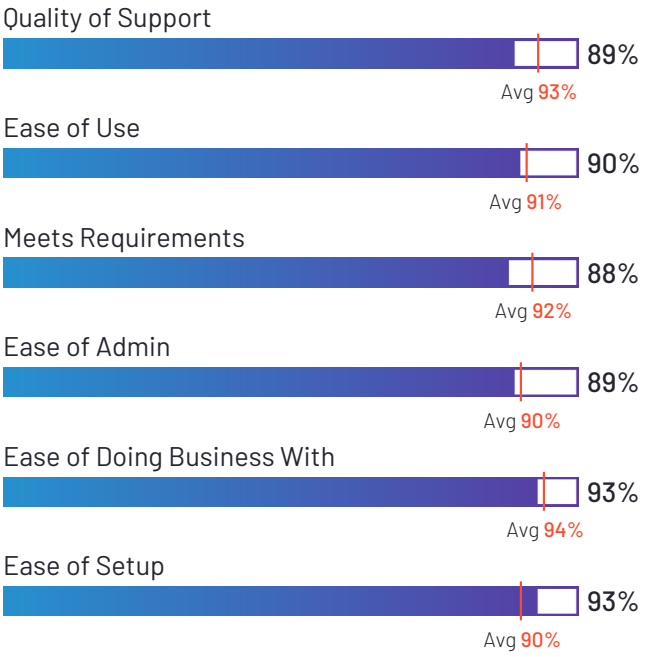
Company Website
shuffler.io

Palo Alto Networks Cortex XSOAR

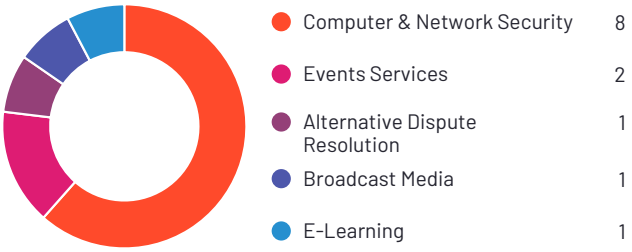
4.5 ★★★★½ (18)

Palo Alto Networks Cortex XSOAR 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. 100% 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 Palo Alto Networks Cortex XSOAR at a rate of 90%.

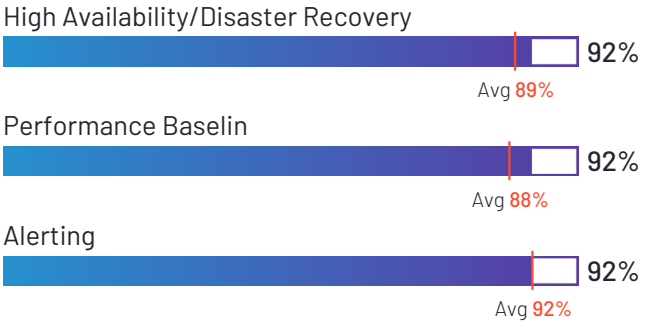
Satisfaction Ratings



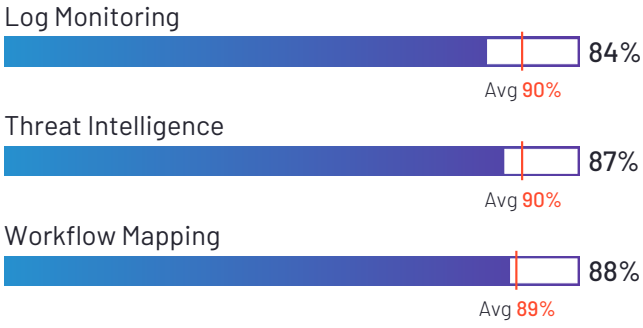
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Palo Alto Networks

HQ Location
Santa Clara, CA

Year Founded
2005

Employees (Listed On Linkedin)
13,928

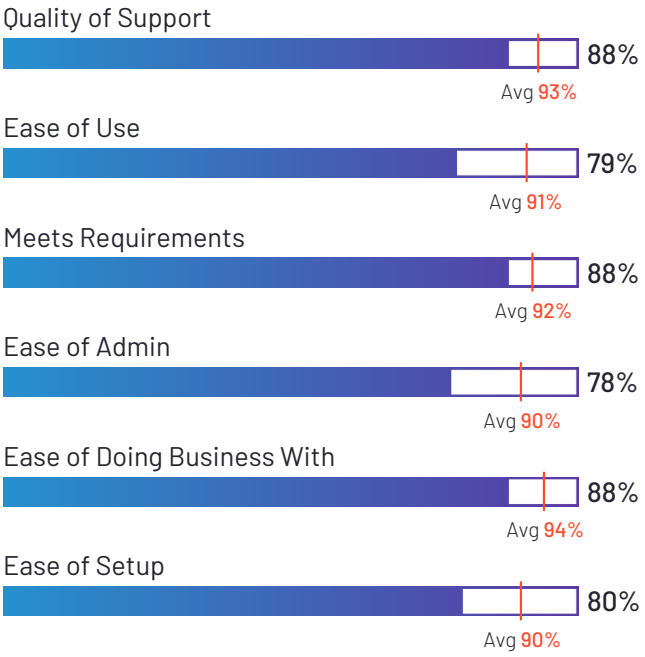
Company Website
paloaltonetworks.com

IBM Security QRadar SOAR

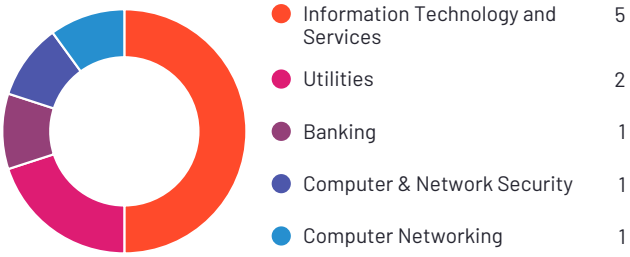
4.3 ★★★★½ (18)

IBM Security QRadar SOAR 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. 93% 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 Security QRadar SOAR at a rate of 85%. IBM Security QRadar SOAR 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

Employees (Listed On Linkedin)
301,650

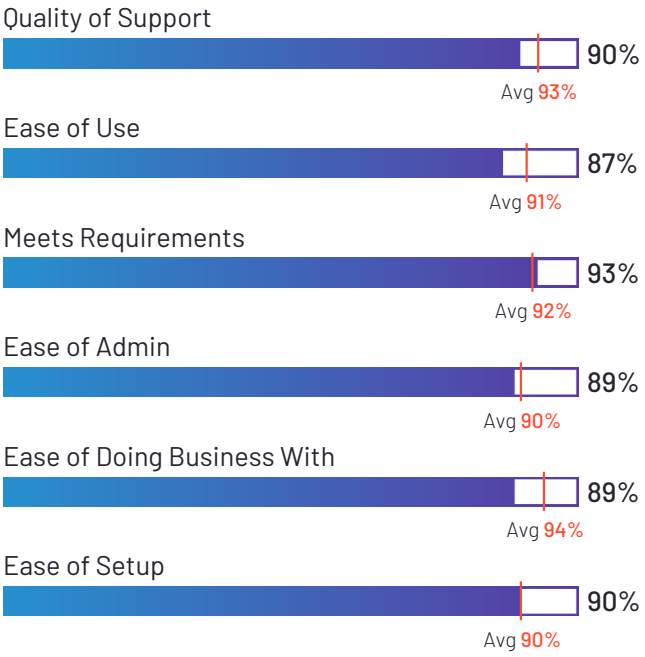
Company Website
www.ibm.com

Sumo Logic

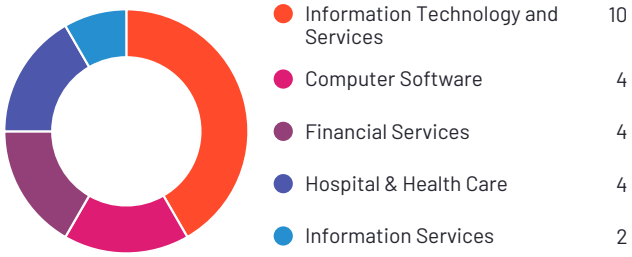
4.3 ★★★★½ (271)

Sumo Logic 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. 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)
1,077

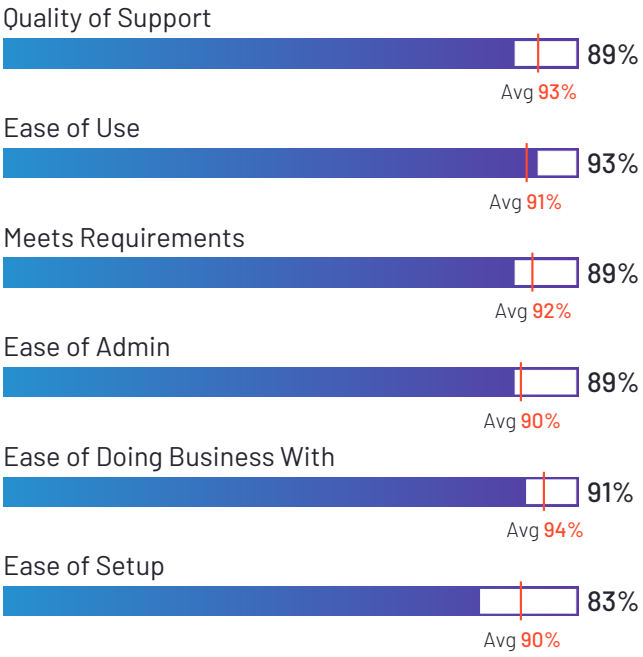
Company Website
sumologic.com

Demisto

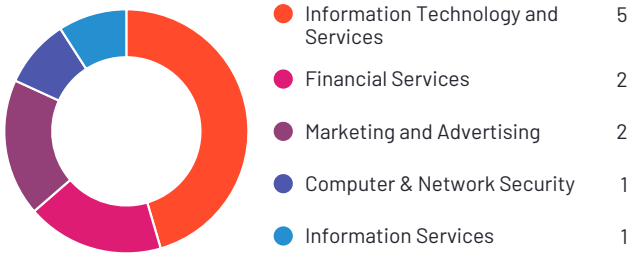
4.5 ★★★★½ (14)

Demisto 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. 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

Employees (Listed On Linkedin)
13,928

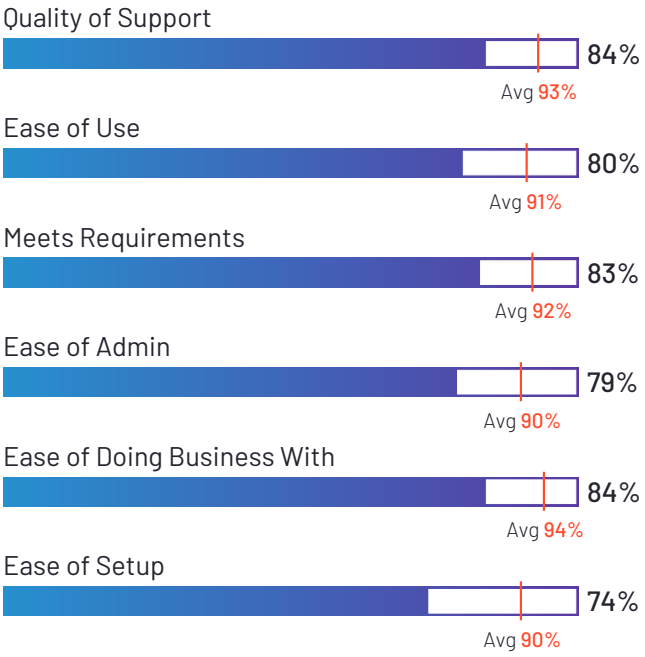
Company Website
paloaltonetworks.com

Chronicle SOAR (formerly Siemplify)

4.4 ★★★★½ (33)

Chronicle SOAR (formerly Siemplify) 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. 96% 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 Chronicle SOAR (formerly Siemplify) at a rate of 88%.

Satisfaction Ratings



Top Industries Represented

Ownership
Google Cloud

HQ Location
Mountain View, CA

Year Founded
1998

Employees (Listed On Linkedin)
23

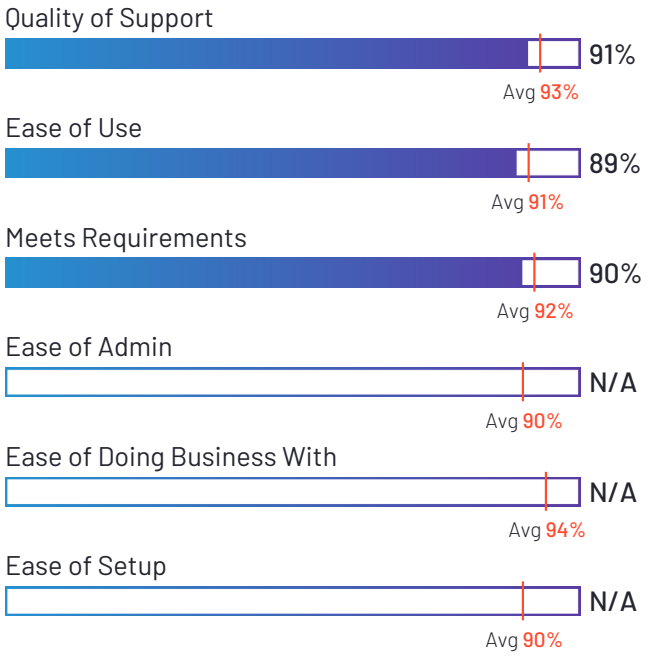
Company Website
cloud.google.com

D3 Security

4.2 ★★★★☆ (69)

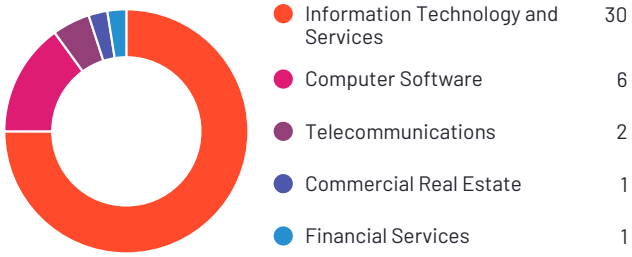
D3 Security has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 95% of users rated it 4 or 5 stars, 95% of users 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)
157

Company Website
d3security.com

LogicHub

4.7 ★★★★½ (11)

LogicHub 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, 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 93%

Ease of Use
N/A
Avg 91%

Meets Requirements
N/A
Avg 92%

Ease of Admin
N/A
Avg 90%

Ease of Doing Business With
N/A
Avg 94%

Ease of Setup
N/A
Avg 90%

*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
Devo

HQ Location
Cambridge, Massachusetts

Year Founded
2011

Employees (Listed On Linkedin)
582

Company Website
www.devo.com

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%	93%	92%	97%	94%	88%	92%	81
Microsoft Sentinel	89%	93%	90%	85%	91%	88%	85%	89%	68
Tines	97%	98%	93%	93%	98%	98%	93%	93%	94
Swimlane	91%	96%	94%	90%	93%	94%	93%	94%	76
Torq	94%	100%	94%	95%	98%	97%	95%	91%	94
Logpoint	91%	100%	92%	90%	93%	95%	93%	90%	67
Blumira Automated Detection & Response	97%	100%	91%	95%	97%	99%	92%	96%	95
CrowdSec	95%	92%	97%	92%	96%	96%	90%	91%	85
SIRP	94%	89%	97%	100%	100%	98%	100%	97%	78
Shuffle	96%	91%	96%	96%	98%	97%	98%	97%	91
Palo Alto Networks Cortex XSOAR	90%	92%	88%	89%	93%	89%	93%	90%	72
IBM Security QRadar SOAR	85%	100%	88%	78%	88%	88%	80%	79%	50
Sumo Logic	87%	86%	93%	89%	89%	90%	90%	87%	62
Demisto	89%	92%	89%	89%	91%	89%	83%	93%	64
Chronicle SOAR (formerly Siemplify)	88%	95%	83%	79%	84%	84%	74%	80%	60
D3 Security	87%	95%	90%	N/A	N/A	91%	N/A	89%	54
LogicHub	95%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	100
Average	92%	94%	92%	90%	94%	93%	90%	91%	76

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

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

Feature Comparison for Security Orchestration, Automation, and Response (SOAR)

G2 users have evaluated the following products by feature. Feature ratings are representative of reviewers overall satisfaction with each feature and do not necessarily take into account the breadth of individual product features. The results are shown below.

Automation

	Workflow Mapping	Workflow Automation	Automated Remediation
PhishER	86%	89%	89%
Microsoft Sentinel	85%	85%	90%
Tines	95%	97%	93%
Swimlane	91%	97%	94%
Torq	95%	97%	93%
Logpoint	88%	90%	88%
Blumira Automated Detection & Response		N/A	N/A
CrowdSec	76%	81%	93%
SIRP	N/A	N/A	N/A
Shuffle	96%	97%	95%
Palo Alto Networks Cortex XSOAR	88%	88%	90%
IBM Security QRadar SOAR	N/A	N/A	N/A
Sumo Logic	N/A	N/A	N/A
Demisto	N/A	N/A	N/A
Chronicle SOAR (formerly Siemplify)	N/A	N/A	N/A
D3 Security	N/A	N/A	N/A
LogicHub	N/A	N/A	N/A
Average	89%	91%	92%

(Feature Comparison for Security Orchestration, Automation, and Response (SOAR) continues on next page)

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

**A blank box indicates that a seller has selected that they do not offer that feature.

Feature Comparison for Security Orchestration, Automation, and Response (SOAR) (continued)

G2 users have evaluated the following products by feature. Feature ratings are representative of reviewers overall satisfaction with each feature and do not necessarily take into account the breadth of individual product features. The results are shown below.

Orchestration

	Security Orchestration	Threat Intelligence	Data Visualization
PhishER	89%	91%	89%
Microsoft Sentinel	89%	86%	86%
Tines	96%	88%	81%
Swimlane	97%	89%	77%
Torq	98%	86%	92%
Logpoint	92%	90%	92%
Blumira Automated Detection & Response	N/A	N/A	N/A
CrowdSec	87%	97%	90%
SIRP	N/A	N/A	N/A
Shuffle	96%	96%	91%
Palo Alto Networks Cortex XSOAR	92%	87%	92%
IBM Security QRadar SOAR	N/A	N/A	N/A
Sumo Logic	N/A	N/A	N/A
Demisto	N/A	N/A	N/A
Chronicle SOAR (formerly Siemplify)	N/A	N/A	N/A
D3 Security	N/A	N/A	N/A
LogicHub	N/A	N/A	N/A
Average	93%	90%	88%

(Feature Comparison for Security Orchestration, Automation, and Response (SOAR) continues on next page)

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

**A blank box indicates that a seller has selected that they do not offer that feature.

Feature Comparison for Security Orchestration, Automation, and Response (SOAR) (continued)

G2 users have evaluated the following products by feature. Feature ratings are representative of reviewers overall satisfaction with each feature and do not necessarily take into account the breadth of individual product features. The results are shown below.

Response

	Alerting	Performance Baselin
PhishER	89%	
Microsoft Sentinel	88%	85%
Tines	95%	88%
Swimlane	86%	86%
Torq	93%	93%
Logpoint	96%	89%
Blumira Automated Detection & Response	N/A	N/A
CrowdSec	94%	77%
SIRP	N/A	N/A
Shuffle	97%	93%
Palo Alto Networks Cortex XSOAR	92%	92%
IBM Security QRadar SOAR	N/A	N/A
Sumo Logic	N/A	N/A
Demisto	N/A	N/A
Chronicle SOAR (formerly Siemplify)	N/A	N/A
D3 Security	N/A	N/A
LogicHub	N/A	N/A
Average	92%	88%

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

**A blank box indicates that a seller has selected that they do not offer that feature.

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	12%	79%	9%
Microsoft Sentinel	21%	35%	44%
Tines	22%	41%	37%
Swimlane	28%	56%	16%
Torq	11%	28%	61%
Logpoint	29%	50%	21%
Blumira Automated Detection & Response	14%	68%	18%
CrowdSec	70%	15%	15%
SIRP	42%	26%	32%
Shuffle	25%	75%	0%
Palo Alto Networks Cortex XSOAR	22%	22%	56%
IBM Security QRadar SOAR	7%	7%	86%
Sumo Logic	11%	46%	43%
Demisto	36%	43%	21%
Chronicle SOAR (formerly Siemplify)	9%	17%	74%
D3 Security	26%	29%	45%
LogicHub	18%	27%	55%
Average	24%	39%	37%

(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	86%	14%	1.4	83%	12%	2%	3%	75	25
Microsoft Sentinel	83%	17%	2.6	61%	12%	17%	10%	12	16
Tines	79%	21%	0.6	80%	9%	3%	9%	7	8
Swimlane	60%	40%	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Torq	100%	0%	0.7	83%	0%	0%	17%	12	10
Logpoint	8%	92%	2	46%	23%	8%	23%	7	8
Blumira Automated Detection & Response	87%	13%	0.4	80%	13%	7%	0%	7	13
CrowdSec	50%	50%	0.4	89%	0%	0%	11%	3	0
SIRP	71%	29%	0.7	N/A	N/A	N/A	N/A	N/A	N/A
Shuffle	100%	0%	0.1	57%	29%	14%	0%	12	10
Palo Alto Networks Cortex XSOAR	33%	67%	2.1	13%	75%	0%	13%	17	26
IBM Security QRadar SOAR	71%	29%	4.7	80%	20%	0%	0%	17	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
Chronicle SOAR (formerly Siemplify)	11%	89%	3.7	38%	62%	0%	0%	7	24
D3 Security	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
LogicHub	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

(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	74%	14
Microsoft Sentinel	57%	20
Tines	42%	6
Swimlane	N/A	N/A
Torq	51%	14
Logpoint	35%	26
Blumira Automated Detection & Response	76%	7
CrowdSec	70%	3
SIRP	N/A	N/A
Shuffle	55%	19
Palo Alto Networks Cortex XSOAR	31%	15
IBM Security QRadar SOAR	53%	N/A
Sumo Logic	79%	N/A
Demisto	N/A	N/A
Chronicle SOAR (formerly Siemplify)	54%	32
D3 Security	N/A	N/A
LogicHub	N/A	N/A
Average	56%	16

(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 products impact and influence in the category.

Market Presence

	Seller Name	Year Founded	Employees on LinkedIn (Seller)	LinkedIn Followers	Twitter Followers (Seller)	Glassdoor Rating
PhishER	KnowBe4, Inc.	2010	1,756	183,366	14,766	5.0
Microsoft Sentinel	Microsoft	1975	224,717	19,659,603	12,875,576	4.4
Tines	Tines	2018	177	16,986	1,974	4.9
Swimlane	Swimlane	2014	219	9,935	1,608	4.4
Torq	torq	2020	126	5,975	1,830	3.5
Logpoint	Logpoint	2001	305	18,147	990	3.8
Blumira Automated Detection & Response	Blumira	2018	53	5,361	0	5
CrowdSec	CrowdSec	2019	32	6,431	19,778	N/A
SIRP	SIRP	2017	14	1,987	66	N/A
Shuffle	Shuffle AS		6	276	0	N/A
Palo Alto Networks Cortex XSOAR	Palo Alto Networks	2005	13,928	911,581	121,365	4.7
IBM Security QRadar SOAR	IBM	1911	301,650	15,377,210	715,022	4.2
Sumo Logic	Sumo Logic	2010	1,077	101,684	6,726	3.8
Demisto	Palo Alto Networks	2005	13,928	911,581	121,365	4.7
Chronicle SOAR (formerly Siemplify)	Google Cloud	1998	23	17,280	9,348	4.3
D3 Security	D3 Security Management Systems	2004	157	16,642	1,106	4.3
LogicHub	Devo	2011	582	29,538	6,435	3.6

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