FROST & SULLIVAN
BEST PRACTICES
AWARDS

FROST & SULLIVAN

2019 BEST PRACTICES AWARD

RAPID7

2019
GLOBAL SOAR
COMPANY OF THE YEAR AWARD

Content

Background and Company Performance

Industry Challenges

For enterprises, speed is of the essence when remediating cybersecurity threats. However, security operations centers (SOC) often lack the resources needed to deliver speedy threat detection and remediation. A study by Frost & Sullivan puts the global cybersecurity workforce shortage at 1.8 million by 2022.

Further, SOCs increasingly invest in numerous point solutions for various information security use cases. Each of these tools generates threat alerts, the majority of them being false positives. An information security analyst spends hours processing alerts, identifying true incidents, switching between different tools to investigate, and finally remediating.

Security orchestration, automation, and response (SOAR) tools save precious analyst time by integrating with security tools and automating threat detection and remediation. Growing adoption of SOAR platforms underlines the pressure placed on enterprises to balance security robustness and speed of incident resolution. A recent Frost & Sullivan study estimates the global SOAR market will grow at a CAGR of 18.1% between 2018 and 2021, generating revenues of $595.2 million by the end of this period.

At the same time, SOAR platforms are often developed for large enterprises with a moderate to high level of security maturity. Indeed, Frost & Sullivan's research finds that only 0.03% of global small and medium enterprises (SMEs) used a SOAR platform in 2018. In contrast, 2.6% of large and very large enterprises have implemented SOAR.

The common premise is that organizations need to have a well-defined security process in place in order for SOAR implementation to be effective. In addition, the price points of SOAR solutions do not make sense for a SOC with just a detection stack or a ticketing tool set up. However, in SMEs, an average of 2 to 10 full-time employees share both IT and security responsibilities, leaving little time and scope for a well-defined IT or security process. Therefore, mid-market SOCs commonly settle for compliance-based security, deploying tools that address the basic security demands of regulators and customers.

There are few SOAR solutions that address the needs of SMEs looking to scale up their security maturity levels. Some vendors collaborate with managed security services providers (MSSPs) to enable mid-market organizations to improve security operations. This approach, albeit a sensible one, still has its limitations and restricts the company's options to explore automation.

The ability to enjoy the benefits of SOAR is a distant dream for most mid-market organizations. While the majority of SOAR vendors offer an MSSP-based solution, Rapid7's SOAR solution helps organizations to achieve smarter and faster security operations, irrespective of company size.

Visionary Innovation and Performance/Customer Impact

Rapid7, founded in 2000, was one of the early players in the security automation space. The company's Insight cloud helps to drive cybersecurity risk management through contextual data analysis and management.

A Mid-Market Friendly SOAR Platform

Rapid7's InsightConnect SOAR solution builds on Insight's capabilities to drive automation and optimization of security operations in organizations. Rapid7's InsightConnect differentiates from rival solutions by being agnostic to security maturity level, enterprise size, or low security budget. Rapid7's SOAR solution can be deployed by small organizations with a basic detection stack, as well as high maturity enterprises with existing automation programs in place. Therefore, even mid-market firms can deploy InsightConnect.

The solution offers three primary functionalities:

1. **Orchestration** – InsightConnect acts as the integration layer, tying together different point solutions of an enterprise technology stack. The solution has over 300 integrations that include open source, partner-developed, and custom-built plug-ins to connect to different tools.

2. **Automation** – With an intuitive visual workflow builder and easily customizable workflow templates, InsightConnect enables organizations to automate security tasks. The solution also allows security analysts to add human decision points throughout the incident detection and response process.

3. **Acceleration** – Rapid7 places a lot of emphasis on saving time. The customers can increase their level of automation by identifying gaps or bottlenecks and building custom workflows to achieve a higher security maturity level.

As an example of timesaving, a typical phishing investigation takes about 75 minutes, from creating a ticket to alerting employees and DNS blackholing. With InsightConnect, this entire process takes about 2 minutes. InsightConnect goes beyond phishing investigation – the most common use case that most SOAR vendors offer. The solution supports a wide variety of use cases such as automation-assisted patching, threat hunting, malware investigation & containment, privilege escalation & investigations and alert data enrichment.

User-based access management is a tedious process for organizations, especially when an employee is hired or fired. The issue is amplified when there is bulk onboarding or attrition, with each employee requiring different access policies. InsightConnect enables organizations to build automated workflows that reduce workload and improve efficiency.

Using InsightConnect, one of Rapid7's customers designed an automated workflow to create user accounts based on first and last names, assign the right permissions to each user based on his / her role, and add the user to the right security group. With this workflow, the customer was able to save 80 hours per week, equivalent to the work of two full-time employees.

Feature-rich and Scalable Product

InsightConnect's visual workflow builder helps security analysts realize the 'low code or no code' promise. Security analysts can import connect-and-go workflow templates for the most common IR processes. They can also develop custom plugins and modify existing

plugins to meet their business needs. The analyst can select a trigger source, configure actions, and automate processes without a single line of code. Further, the analyst can also introduce human decision points to enable detailed analysis by the team.

InsightConnect's ChatOps integrations allow security teams to build workflows with communication and collaboration tools, such as Slack and Microsoft Teams. The ChatOps user experience allows analysts to trigger and interact with workflows from Slack, work on the go, get security alerts directly to the user device, collaborate with team members, and improve flexibility. The platform enables extensibility to add communication tools like FB Workplace.

InsightConnect's dashboards help security analysts view all metrics on a single page. The dashboards collect data from tools across the network. Further, analysts can create custom widgets to display metrics tailored to specific business needs. For instance, the dashboard gives insight into the utilization level of various tools in the organization. This in turn can help SOCs make data-based decisions to build a different workflow or reconsider investment priorities.

Rapid7 Insight cloud has integrations with leading threat intelligence solutions such as Anomali ThreatStream and Recorded Future as well as open-source feeds. Together, these tools execute hash lookups, domain lookups, geographical IP lookups, and more to keep the enterprise up to date with threat intelligence.

Rapid Onboarding and Superior Customer Experience

InsightConnect is comprised of hybrid architecture. Rapid7 deploys an on-premises software component, the orchestrator, which acts as the execution layer. Its multi-tenant cloud-based servers host the workflows, investigations, and job data. At the same time, customer credentials are encrypted locally on-premises using the HMACSHA256 algorithm, thereby addressing concerns around cloud-based deployment. At the proof-of-concept level, InsightConnect can be deployed in less than two business days.

Rapid7 offers a subscription-based model to its customers. The pricing structure is based on the number of workflows used and places no limits on users, actions, integrations, or API calls. Rapid7's pricing model is designed to cater to the budget constraints of SMEs. Rapid7 also offers an enterprise license agreement to meet the needs of larger organizations looking to scale.

Stellar Growth Fueled by High Customer Satisfaction

Rapid7 has recorded impressive growth across numerous metrics. For instance, in 2018, the company generated revenue of $244.1 million, representing a Year-on-Year (YoY) growth rate of 21.5%. In 2019, the company is on the way to achieving a 30% YoY growth rate. Further, 87% of its total revenue comes from the recurring revenue model, thereby providing a sound foundation for future growth.

Rapid7 currently serves about 8,500 customers globally. It uses a "land and expand" model to expand the business. In the last year, the company has exhibited a compelling

track record of customer retention and expansion. As an indicator of customer satisfaction, Rapid7's renewal rate has grown by 113% over the past 12 months.

Conclusion

The SOAR market is highly focused on large enterprises with high security maturity. Mid-market enterprises that have an equal need for automation gathers little attention from vendors; Rapid7 has designed its SOAR product to also account for the needs of such organizations. Further, the feature-rich solution helps customers to improve their security operations with simple connect-and-go visual workflows in a no-code environment. With its strong vision, the company has exhibited impressive financial growth and high levels of customer satisfaction. For its strong overall performance, Rapid7 is recognized with Frost & Sullivan's 2019 Company of the Year Award.

Significance of Company of the Year

To receive the Company of the Year Award (i.e., to be recognized as a leader not only in your industry, but among non-industry peers) requires a company to demonstrate excellence in growth, innovation, and leadership. This excellence typically translates into superior performance in three key areas—demand generation, brand development, and competitive positioning—that serve as the foundation of a company's future success and prepare it to deliver on the 2 factors that define the Company of the Year Award: Visionary Innovation and Performance, and Customer Impact).

Understanding Company of the Year

Driving demand, brand strength, and competitive differentiation all play critical roles in delivering unique value to customers. This three-fold focus, however, must ideally be complemented by an equally rigorous focus on Visionary Innovation and Performance to enhance Customer Impact.

Key Benchmarking Criteria

For the Company of the Year Award, Frost & Sullivan analysts independently evaluated each factor according to the criteria identified below.

Visionary Innovation & Performance

Criterion 1: Addressing Unmet Needs
Requirement: Implementing a robust process to continuously unearth customers' unmet or underserved needs, and creating the products or solutions to address them effectively.

Criterion 2: Visionary Scenarios through Mega Trends
Requirement: Incorporating long-range, macro-level scenarios into the innovation strategy, thereby enabling first-to-market growth opportunity solutions.

Criterion 3: Implementation of Best Practices
Requirement: Best-in-class strategy implementation characterized by processes, tools, or activities that generate a consistent and repeatable level of success.

Criterion 4: Blue Ocean Strategy
Requirement: Strategic focus on creating a leadership position in a potentially uncontested market space, manifested by stiff barriers to entry for competitors.

Criterion 5: Financial Performance
Requirement: Strong overall business performance in terms of revenue, revenue growth, operating margin, and other key financial metrics.

Customer Impact

Criterion 1: Price/Performance Value
Requirement: Products or services offer the best value for the price compared to similar offerings in the market.

Criterion 2: Customer Purchase Experience
Requirement: Customers feel they are buying the optimal solution that addresses both their unique needs and their unique constraints.

Criterion 3: Customer Ownership Experience
Requirement: Customers are proud to own the company's product or service and have a positive experience throughout the life of the product or service.

Criterion 4: Customer Service Experience
Requirement: Customer service is accessible, fast, stress-free, and of high quality.

Criterion 5: Brand Equity
Requirement: Customers have a positive view of the brand and exhibit high brand loyalty.

Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan analysts follow a 10-step process to evaluate award candidates and assess their fit with select best practice criteria. The reputation and integrity of the awards are based on close adherence to this process.

STEP		OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify award recipient candidates from around the world	• Conduct in-depth industry research • Identify emerging industries • Scan multiple regions	Pipeline of candidates that potentially meet all best practices criteria
2	**Perform 360-degree research**	Perform comprehensive, 360-degree research on all candidates in the pipeline	• Interview thought leaders and industry practitioners • Assess candidates' fit with best practices criteria • Rank all candidates	Matrix positioning of all candidates' performance relative to one another
3	**Invite thought leadership in best practices**	Perform in-depth examination of all candidates	• Confirm best practices criteria • Examine eligibility of all candidates • Identify any information gaps	Detailed profiles of all ranked candidates
4	**Initiate research director review**	Conduct an unbiased evaluation of all candidate profiles	• Brainstorm ranking options • Invite multiple perspectives on candidates' performance • Update candidate profiles	Final prioritization of all eligible candidates and companion best practices positioning paper
5	**Assemble panel of industry experts**	Present findings to an expert panel of industry thought leaders	• Share findings • Strengthen cases for candidate eligibility • Prioritize candidates	Refined list of prioritized award candidates
6	**Conduct global industry review**	Build consensus on Award candidates' eligibility	• Hold global team meeting to review all candidates • Pressure-test fit with criteria • Confirm inclusion of all eligible candidates	Final list of eligible award candidates, representing success stories worldwide
7	**Perform quality check**	Develop official award consideration materials	• Perform final performance benchmarking activities • Write nominations • Perform quality review	High-quality, accurate, and creative presentation of nominees' successes
8	**Reconnect with panel of industry experts**	Finalize the selection of the best practices award recipient	• Review analysis with panel • Build consensus • Select winner	Decision on which company performs best against all best practices criteria
9	**Communicate recognition**	Inform award recipient of recognition	• Present award to the CEO • Inspire the organization for continued success • Celebrate the recipient's performance	Announcement of award and plan for how recipient can use the award to enhance the brand
10	**Take strategic action**	Upon licensing, company able to share award news with stakeholders and customers	• Coordinate media outreach • Design a marketing plan • Assess award's role in strategic planning	Widespread awareness of recipient's award status among investors, media personnel, and employees

The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of the research process. It offers a 360-degree view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often companies make important growth decisions based on a narrow understanding of their environment, resulting in errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry participants and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, helps clients accelerate growth and achieve best-in-class positions in growth, innovation, and leadership. The company's Growth Partnership Service provides the CEO and the CEO's growth team with disciplined research and best practices models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages nearly 60 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on 6 continents. To join Frost & Sullivan's Growth Partnership, visit http://www.frost.com.

Copyright