FROST & SULLIVAN

BEST PRACTICES

AWARDS

D3 SECURITY

2019 GLOBAL SECURITY ORCHESTRATION & AUTOMATION RESPONSE CUSTOMER VALUE LEADERSHIP AWARD

Contents

Background and Company Performance

Industry Challenges

Data breaches are growing at an alarming rate every year. Depending on the report one chooses to read, threat intelligence companies believe data breaches have risen between 75% and 450% in 2018. Chief Information Security Officers (CISOs) invest in multiple security tools to protect confidential company and customer data. Yet, many security teams are short staffed and struggle to process all of the alerts in their queue. This shortage of cyber security talent is a worldwide phenomenon. In the United States alone, there was a shortage of 314,000 cyber security professionals in 2019. Moreover, Frost & Sullivan estimates a global shortage of 1.8 million cyber security professionals by 2022.

Putting the security challenge into context, a mid-sized enterprise receives a minimum of 300 alerts every day. A Tier 1 analyst can process up to 10 alerts per day. Thus, the average midsized enterprise would theoretically need to hire 30 Tier 1 analysts to man a security operations center (SOC). However, most midsized enterprises will never have a SOC and most SOCs have a maximum of 10 security analysts on duty. In addition, the shortage of cyber security professionals has led to high attrition rates among security professionals as a result of zero unemployment and a highly competitive market. This means many alerts go un-investigated by the SOC, leaving enterprises exposed to high levels of risk.

The situation is further complicated when security tools generate false positives. Security Incident and Event Management (SIEM) tools are good at log aggregation but often lack turnkey triage analysis or incident response/case management capabilities. In such instances, an investment in a security orchestration and automation response (SOAR) platform is imperative. SOAR platforms help SOCs increase alert handling efficiency and reduce workload. The benefits of SOAR implementation are numerous and have been thoroughly documented.

However, enterprise adoption of SOAR remains quite limited. Frost & Sullivan finds less than 2% of enterprises globally have invested in SOAR to date. Being an early growth stage market, CISOs are not fully convinced of the need for SOAR implementation. Heavy reliance on information security analysts rather than on automation comes from skepticism about the technological maturity of available options.

CISOs open to using these solutions look for scalability and interoperability in SOAR platforms. Many solutions, despite offering an API-based integration framework, do not work with most of the third party security tools. Plus, SOAR platforms typically follow a consumption-based pricing model. This means CISOs need to restrict SOAR usage to high priority cases.
The competitive landscape for the SOAR market is not well defined. Some vendors offer their SOAR platform as a standalone product. Others integrate SOAR capabilities into their security tools such as SIEM, endpoint protection platforms, firewalls, and more. This results in a competitive landscape with blurred boundaries.

In such an ecosystem, a CISO needs to engage with a partner who understands his or her concerns. At the same time, the solution should integrate seamlessly with an existing security ecosystem and be able to evolve continuously. More importantly, the vendor should provide personalized post-purchase customer engagement.

Customer Impact and Business Impact

D3 Security helps its customers streamline and automate security operations. The company began operations in 2003 as an incident management solution provider. Since then, D3 Security has evolved to become an incident automation vendor with next-generation SOAR capabilities.

A Holistic Approach to SOAR

Enterprises often deal with alerts from different tools and threat intelligence feeds. In addition, security teams analyze a large volume of incoming files and URLs looking for potential malware. In such cases, security analysts have to go through multiple applications to investigate each alert. This leads to wasted time and resources, as well as alert fatigue. D3 Security's SOAR platform consolidates all the different tools and applications into a single location. Security teams gain higher visibility of the entire network and endpoints connected to it. The platform gives a structured view into the security operations of an enterprise. It saves a security analyst from having to go through an entire report to get insight into a case. The platform has an API-based integration framework that helps significantly reduce the effort required to transition between different platforms and tools when investigating a case.

The MITRE ATT&CK framework is a knowledge base that provides an exhaustive list of cyber-attack tactics and techniques. The framework is globally accessible and evolves with the threat landscape. D3 ATTACKBOT, included in the company's SOAR platform, leverages the MITRE ATT&CK framework to proactively examine and respond to enterprise threats. D3 ATTACKBOT helps enterprises take advantage of automation and correlation capabilities. The ATTACKBOT pulls granular data from different systems including endpoint detection and response (EDR), SIEM, and others. D3 Security has embedded 213 tactics, techniques, and procedures (TTPs) into its platform.

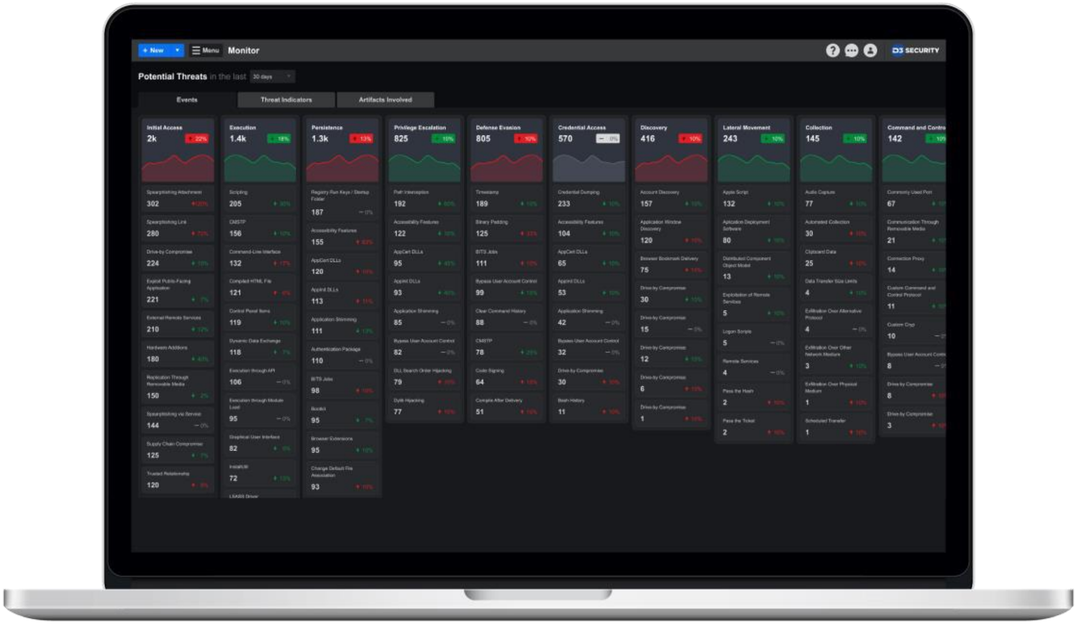


Figure 1: MITRE ATT&CK TTP Dashboard

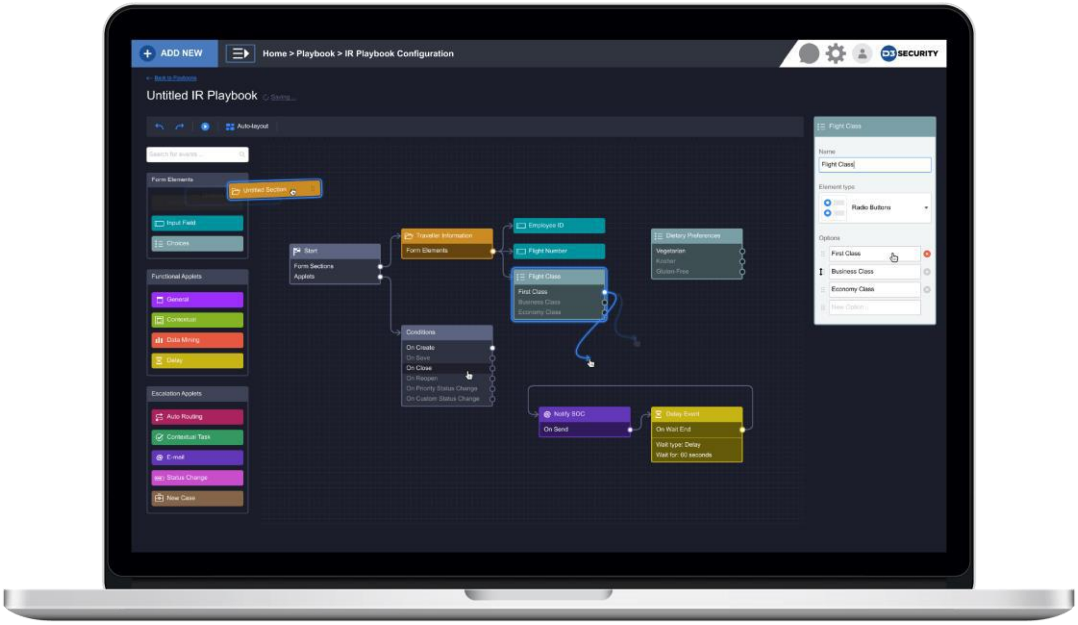


Figure 2: D3 Security Codeless Playbook Editor

Further, D3 Security goes beyond SOAR to handle the entire incident response lifecycle. The company combines SOAR with cross-departmental incident response workflows, forensics case investigation, and reporting and audit capabilities. The built-in analytical system provides analysts with a dashboard to track important metrics. Some of these include end of the week reports, log of TTPs found, stages in which the TTPs were found, and different types of timeline, relationship and cost-savings analysis. By analyzing the types of attacks against the customer's environment, the reporting platform also highlights the security operations or tooling gaps present in an enterprise's security posture—a capability that is particularly relevant to Managed Security Service Providers (MSSP) who can use the diagnosis to recommend additional tools and/or services. As seen in Figure 1, the MITRE ATT&CK TTP Dashboard includes intuitive visualization to map events to the framework. The dashboard, enabled by the ATTACKBOT automation and reporting feature, helps SOC analysts manage events with a contextual kill chain-oriented view. The dashboard helps analysts check the status of various types of events, threat indicators, and artifacts from the MITRE ATT&CK lens with the ability to drill-down to further details and commands. D3 Security is one of the few cyber security vendors with a low-code/no-code platform that specializes in enabling users to build complex business processes without having to write any code. D3's Codeless Playbook Editor allows the SOC team to create incident playbooks and task automations using drop-down menus, wizards and pre-built integration blocks. Unlike other SOAR platforms which require Python coding, the D3 Security solution allows users to change integration and data sources on the fly, or update software versions of integrated products, without any coding. The positive impact for understaffed SOCs—who otherwise would be forced to find security analysts and Python coders—is significant. All of the playbook features are rooted in D3's intuitive drag-and-drop visual canvas, which also houses libraries of out-of-the-box playbooks & integration applets. (Figure 2)

Further, D3 Security enables enterprises to run multiple parallel decision trees automatically. The platform helps provide a centralized knowledge base of incidents across the enterprise. In fact, many customers who initially purchased D3 SOAR for their SOC, have now extended its usage across other departments, including Digital Forensics, Data Privacy, Corporate Security and Anti-Fraud.

A Partnership-based Growth Strategy

D3 Security uses a hybrid sales model for customer acquisition with a rapidly growing partner program. The company has established deep relationships with a handful of major cyber security companies, channel partners, and value-added resellers. The company works with more than 150 vendor partners.

Since 2018, D3 Security has taken efforts to transition its customer acquisition strategy from a 95% direct sales model to a channel partnership-based model. The company has hired an experienced global partnership team to focus on the channel partnership approach. A competitive platform with highly differentiated features such as ATTACKBOT and the ability to go beyond SOAR makes D3 Security a preferred partner for resellers and service providers.

The company boasts a strong customer base that includes over one hundred Fortune 500 companies. Further, in a fragmented and early growth stage market, customer churn is a normal phenomenon. However, D3 Security has consistently maintained a customer retention rate of over 90% in the last three years; in 2019, D3 had an impressive customer retention rate of 96%.

D3 Security has a solid customer base that offers strong upsell potential. The platform comprises different modules such as SOAR, forensics case management, and advanced analytics. The company consistently seeks to increase its annual contract value with the existing customer base by bringing more departments and specialized user groups (e.g. Digital Forensics Investigators) on to the D3 platform. A strong customer support and customer success strategy, in which security experts with CISSP designation are embedded into the company's customer success function, helps the company to uncover more automation opportunities while providing a high level of security expertise to customers.

Customer Focused Implementation

D3 employs a combination of strategies to provide high value to customers both during and post implementation. The D3 Security team takes between 30 and 90 days to onboard a new customer. During this time, the team performs a deep dive to understand the customer's security environment and its unique challenges. The initial implementation team includes a project manager in a consultative role; this helps enterprises gain additional insights during the implementation process.

Most vendors have a customer success team to handle post implementation support. In D3 Security, in addition to a customer success team, D3's security analysts who work on the SOAR implementation provide in-house support for the enterprise. Thus, analysts providing support have intimate knowledge of the customer's security environment. This, in turn, ensures enterprises establish a relationship with the security analysts and facilitates a high level of trust between D3 and the customer, who will not hesitate to contact them in times of need. Through this process, customers are always connected to security experts inside D3.

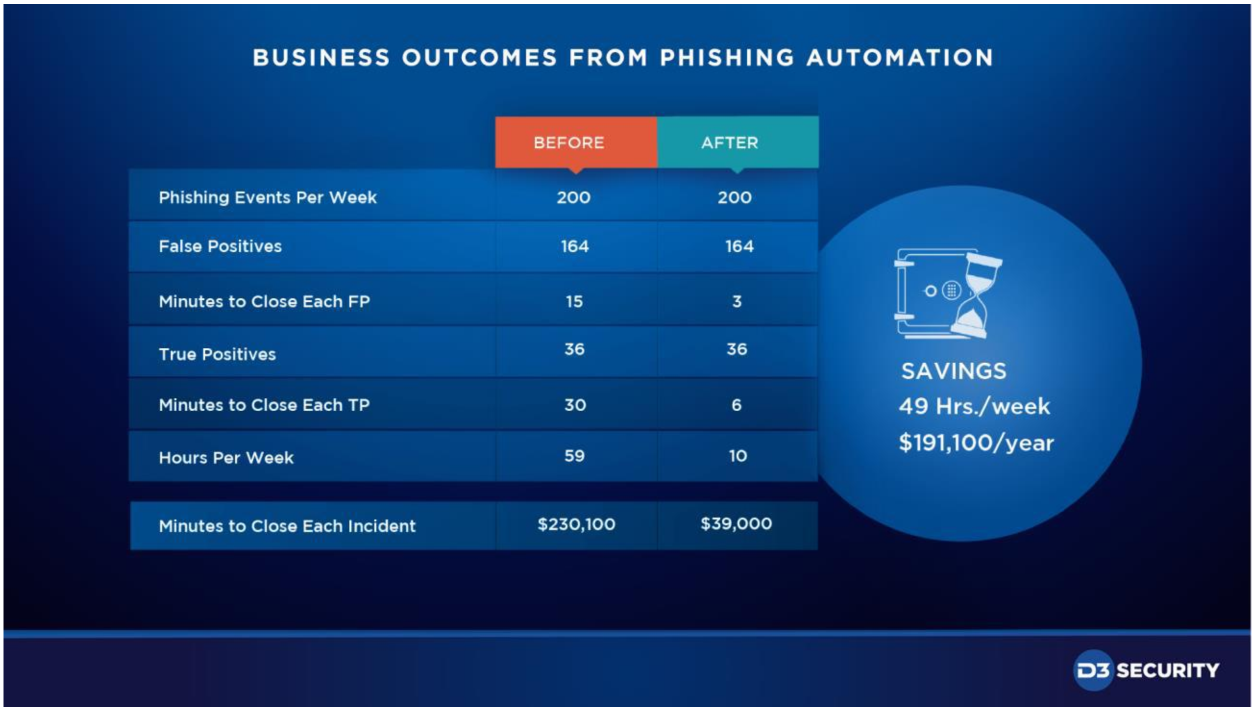
For instance, a well-known US-based healthcare provider offered a testimonial about their positive experience with the customer support capabilities of D3. The Director of Information Security at this company stated that the customer support executive he works with at D3 Security understood "the why and the how" of their security initiatives, and that the relationship was one of the SOC's most critical aspect of enterprise's security posture. This is because, having worked in the client's environment during implementation, the D3 customer support executive is intimately familiar with the customer's needs.

High Value for Money

With a consumption-based pricing model that is prevalent across the sector, costs for an enterprise can skyrocket as volume of alerts and threats grow. In response to valid customer concerns, D3 Security follows a flat pricing model; this ensures that costs remain the same for an enterprise throughout the year. With D3 Security, enterprise costs are based on number of user licenses. Standard packages typically range between $50,000 and $250,000 per year for an enterprise.

D3 Security's SOAR platform has helped companies realize substantial time *and cost* savings. For instance, one of D3 Security's customers deployed PhishMe to enable its employees to report phishing. The customer had a small security team of 4 to 5 analysts. The team handled an *average of 200 events* a *week* from alerts reported by its employees. Out of these, *about 80%* were false positives. The analysts had to manually access employee inboxes, scan the contents of the email, and take remediation actions. It took them up to 25 minutes to set up the case for investigation. Further, the security analysts had to move repeatedly between different applications and tools. A true alert required a minimum of 30 minutes to detect, investigate, remediate and close. Thus, the SOC spent an average of 59 hours every week just to handle incoming alerts from the email security tool.

After the enterprise deployed D3 Security, the SOAR platform automatically parsed the email attachments, pushed the message files, conducted a triage analysis, and set up individual investigation. Suspected phishing incidents were automatically remediated using the platform. After implementation, security analysts could detect a false positive in less than 3 minutes, saving valuable time to focus on real security threats. Automating a single workflow (phishing investigation) saved the customer nearly $200,000. Additional workflow automations have saved the customer in excess of $1M. (Figure 3 & 4)



BUSINESS OUTCOMES FROM PHISHING AUTOMATION

	BEFORE	AFTER
Phishing Events Per Week	200	200
False Positives	164	164
Minutes to Close Each FP	15	3
True Positives	36	36
Minutes to Close Each TP	30	6
Hours Per Week	59	10
Minutes to Close Each Incident	$230,100	$39,000

SAVINGS
49 Hrs./week
$191,100/year

D3 SECURITY

Figure 3: D3 SOAR Phishing Automation Outcome

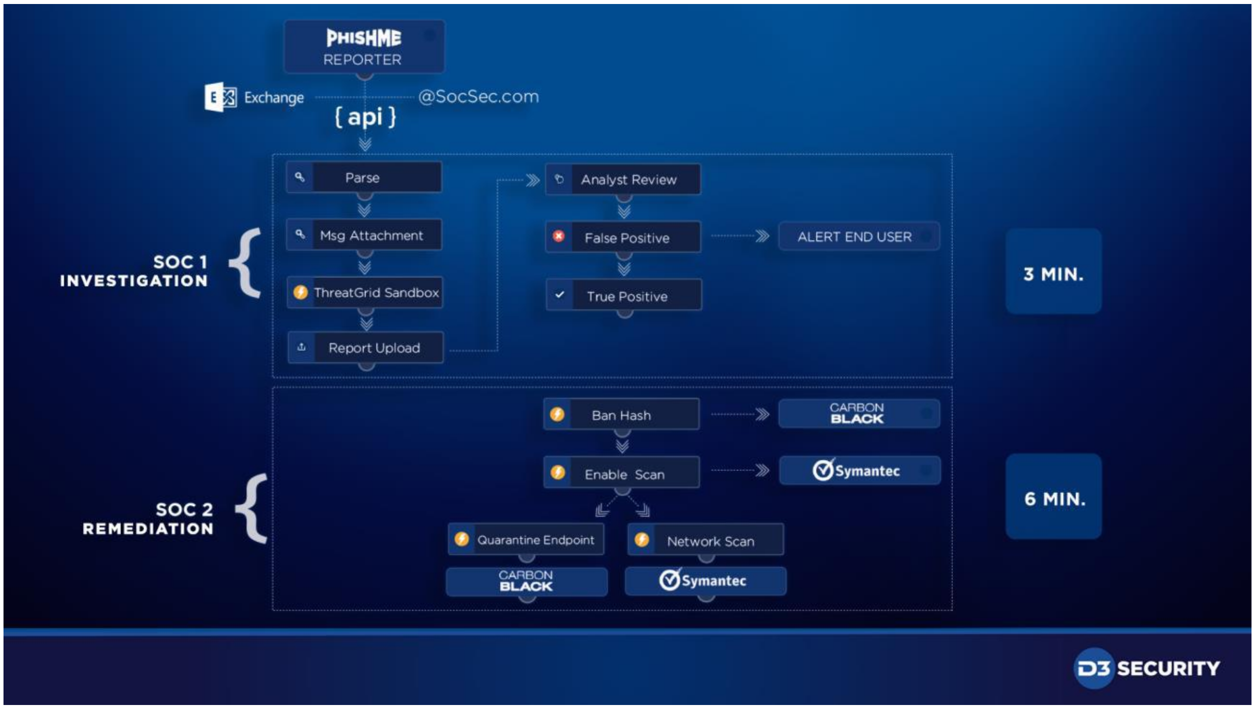


Figure 4: D3 Security Phishing Automation Process

Internal Investments to Fuel Growth – Human Capital & Brand Equity

D3 Security continues to invest in growing its human capital. Every year, the company increases its employee count by 30% - 40%. The executive team at D3 Security believes in maintaining and growing a strong team of security analysts and developers that can develop superior products for customers, and they prove that commitment through visible action instead of rhetoric.

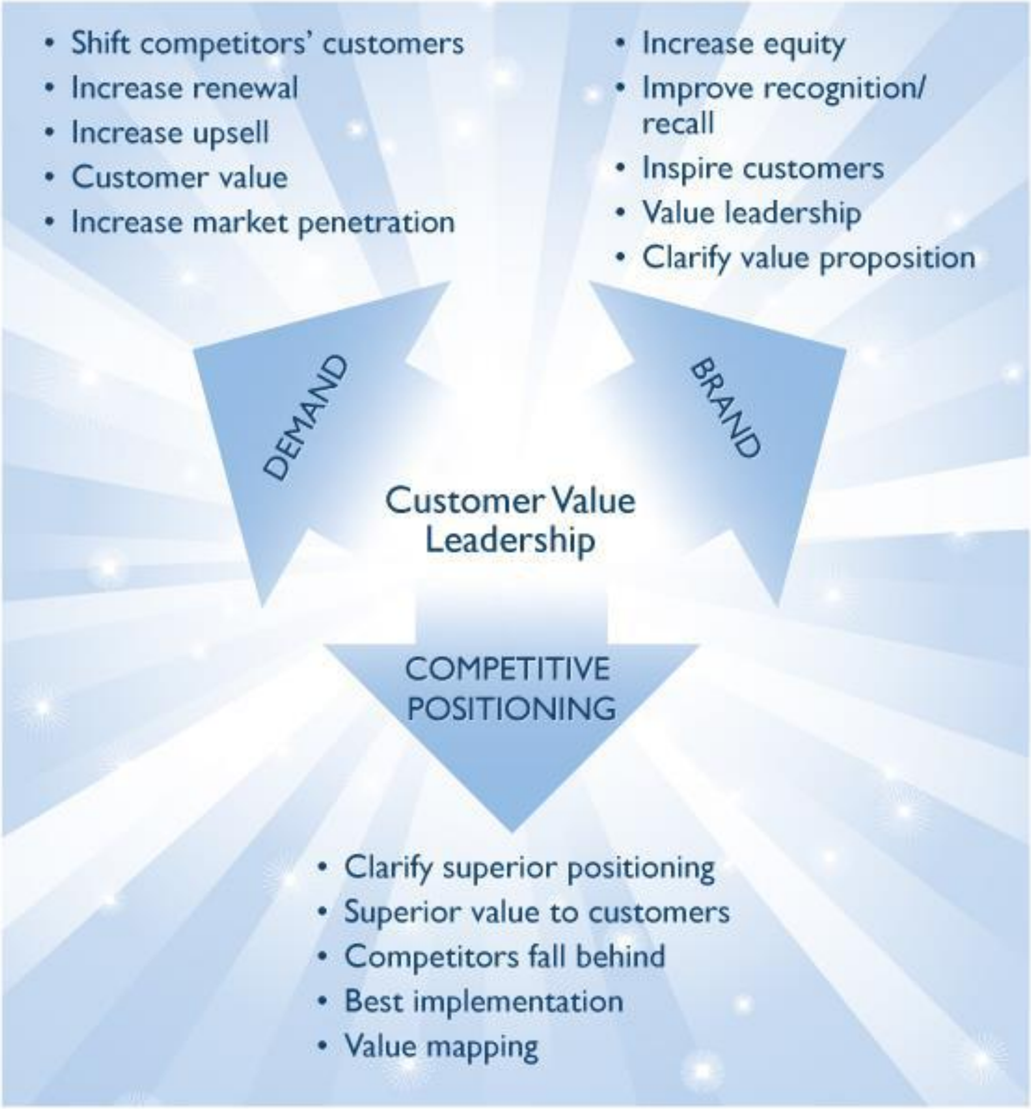
Further, research and development is a strong focus area for D3 Security. The company invests more than 50% of its revenue into R&D. As a result, D3 Security releases a product update every quarter. Further, D3 Security's sales and marketing efforts help educate the market about SOAR and show CISOs how to critically compare D3 Security to other solutions on the market.

Conclusion

CISOs are struggling with internal security operations owing to the growing volume of threats and constrained availability of an experienced cyber security workforce. A scalable and integrated technology platform that saves time and expenses is required to combat these challenges. D3 Security offers a continuously evolving solution with the capability to be scalable and inter-operable. With a combination of agility, access to security talent, and superior technology, D3 Security's Next-Generation solution is gaining market share rapidly in the SOAR market. For its strong overall performance, D3 Security is recognized with Frost & Sullivan's 2019 Customer Value Leadership Award.

Significance of Customer Value Leadership

Ultimately, growth in any organization depends on customers purchasing from a company and then making the decision to return time and again. Satisfying customers is the cornerstone of any successful growth strategy. To achieve this, an organization must be best in class in 3 key areas: understanding demand, nurturing the brand, and differentiating from the competition.



- Shift competitors' customers
- Increase renewal
- Increase upsell
- Customer value
- Increase market penetration

- Increase equity
- Improve recognition/ recall
- Inspire customers
- Value leadership
- Clarify value proposition

- Clarify superior positioning
- Superior value to customers
- Competitors fall behind
- Best implementation
- Value mapping

Understanding Customer Value Leadership

Customer Value Leadership is defined and measured by 2 macro-level categories: Customer Impact and Business Impact. These two sides work together to make customers feel valued and confident in their products' quality and performance. This dual satisfaction translates into repeat purchases and a lifetime of customer value.

Key Benchmarking Criteria

For the Customer Value Leadership Award, Frost & Sullivan analysts independently evaluated Customer Impact and Business Impact according to the criteria identified below.

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.

Business Impact

Criterion 1: Financial Performance

Requirement: Overall financial performance is strong in terms of revenue, revenue growth, operating margin, and other key financial metrics.

Criterion 2: Customer Acquisition

Requirement: Customer-facing processes support the efficient and consistent acquisition of new customers, even as it enhances retention of current customers.

Criterion 3: Operational Efficiency

Requirement: Staff is able to perform assigned tasks productively, quickly, and to a high quality standard.

Criterion 4: Growth Potential

Requirements: Customer focus strengthens brand, reinforces customer loyalty, and enhances growth potential.

Criterion 5: Human Capital

Requirement: Company culture is characterized by a strong commitment to quality and customers, which in turn enhances employee morale and retention.

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 practices criteria. The reputation and integrity of the awards are based on close adherence to this process.

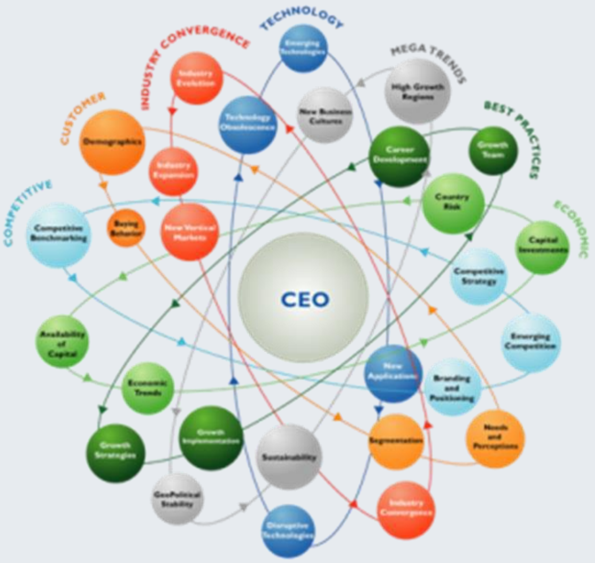
	STEP	OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify award recipient candidates from around the world	• Conduct in-depth industry research • Identify emerging industries • Scan multiple regions	Pipeline of candidates that potentially meet all best practices criteria
2	**Perform 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 recipient	Decision on which company performs best against all best practices criteria
9	**Communicate recognition**	Inform award recipient of award 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 is 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.