FROST & SULLIVAN

BEST PRACTICES AWARDS

SIXGILL

Deep, Dark & Beyond

2020 EUROPEAN & ISRAELI CYBER INTELLIGENCE TECHNOLOGY INNOVATION AWARD

Contents

Background and Company Performance 3

Industry Challenges 3

Technology Attributes and Future Business Value 3

Conclusion 6

Significance of Technology Innovation 7

Understanding Technology Innovation 7

Key Benchmarking Criteria 8

Technology Attributes 8

Future Business Value 8

Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices 9

The Intersection between 360-Degree Research and Best Practices Awards 10

Research Methodology 10

About Frost & Sullivan 10

Background and Company Performance

Industry Challenges

Today's companies are digitizing their businesses and this transformation is generating volumes of sensitive data such as employee credentials, customer information, and intellectual property. All of this data is stored across connected endpoints, in the cloud, and at data centers. The critical nature of this data makes it quite attractive to hackers and cybercriminals.

For years, the cybersecurity industry has maintained its status quo wherein both security vendors and cyber criminals are constantly updating tactics to achieve their respective objectives. Over time, cyber criminals have managed to create a widespread ecosystem and numerous business models around cybercrime. With approaches such as ransomware and cybercrime-as-a-service, hackers have been able to inflict heavy losses upon enterprises. The success of cyber criminals is partly attributable to the fact that security vendors have been heavily focused on protecting their clients from attacks rather than on actively neutralizing attackers. Activities such as tracing attacks back to hackers and identifying them have traditionally been left to law enforcement agencies, which have proven inefficient.

Investment in security solutions is on the rise, and with more investment, large-scale enterprises are looking for innovative solutions that can work cohesively with their existing infrastructure to increase visibility into how exposed they are on the Internet. Many hacks and security breaches begin with employee credentials that get compromised or from vulnerabilities in the software solutions that enterprises use. In most cases, companies only discover vulnerabilities and compromised credentials after they have been exploited.

Companies are thus searching for tools that help them assess their risk and exposure to proactively address issues before getting hacked. Also, many large enterprises face hackers that try to breach a targeted set of company assets. Such attacks are regularly faced by companies in the healthcare and banking, financial services, and insurance (BFSI) industries, which are generally characterized by the presence of sensitive information and critical assets. Companies in such industries need to identify their most vulnerable employees and assets as well as make efforts to identify their attackers.

Frost & Sullivan feels that today's cyber threat intelligence (CTI) industry needs to go above and beyond simply safeguarding clients from cyberattacks; it must introduce more efficient, proactive ways to thwart cyberattacks at the source. In addition to making enterprise systems more secure, next-generation cybersecurity solutions must discourage hackers from designing and executing attacks to begin with.

Technology Attributes and Future Business Value

Industry Impact

Sixgill, an Israel-based cybersecurity startup, has designed a unique CTI platform to extract intelligence related to imminent cyber threats by continually gathering intelligence

associated with cybercrime activity. The company delivers impressive visibility into the dark web where significant cybercrime is rooted and helps companies in multiple industries to identify, track, and neutralize hackers targeting their critical assets. Unlike competitors in the industry that have primarily focused on detection or prediction of attacks, Sixgill has gone one step further to automatically monitor and investigate the threat actors. Sixgill's solutions have played a pivotal role in helping companies frame a proactive and automated CTI strategy.

Sixgill was established in 2014 with a vision to track cybercriminals, their activities, and conversations in the ecosystem, gathering data it uses to anticipate cyberattacks. The company has designed proprietary algorithms that extract data from a wide range of sources, such as dark web social networks, forums, and marketplaces. The algorithm has deep visibility that penetrates channels such as Twitter, Telegram, QQ, and instant relay chats (IRC); a massive trove of data thus captured is further utilized to create profiles and patterns of dark web threat actors and their interactions with peers across platforms, which otherwise remain invisible or inaccessible to enterprises.

Sixgill works extensively with its clients to assess their level of exposure on the deep, dark and clear web to identify vulnerabilities, which they can use to mitigate risks to their organization. While Sixgill's CTI platform provides automated and actionable intelligence to help protect its clients against possible attacks and hacks, in the process the company generates a large database of active cybercriminals, trending CVEs, attacks in planning, and exposed credentials.

Remarkably, in an industry that is highly focused on combatting cyberattacks, Sixgill has taken the initiative to mount stronger, more proactive intelligent defenses against cybercrime. Frost & Sullivan applauds Sixgill's consistent efforts in unearthing hard-to-extract data and to uncover criminal activity, which has contributed immensely to the industry's understanding of how cybercrime works.

Product Impact & Application Diversity

In the continuous cycle of iteration and improvement of both security solutions and hacking tactics, the advantage largely remains on the hackers' side. In response, Sixgill's security system enables clients to monitor the quickly evolving threat landscape in real time. This allows companies to prioritize their valuable defensive resources towards the most relevant threat vectors to them. As such, it has become imperative for companies to adopt a proactive approach in addition to their defensive techniques. On top of protecting itself from attacks, a company gains tremendous insight by knowing which of its assets are being targeted by cybercriminals.

Companies, large or small, regularly face cyberattacks and keep updating their security infrastructure to defend themselves. But in particular, large corporations fall victim to targeted attacks. These attacks are conducted by individual hackers, criminal groups, and at times, even by state-sponsored actors. Fighting such attacks requires companies to develop investigative capabilities so as to identify their attackers and work with law enforcement to neutralize them.

Furthermore, organizations are flooded with data that is mostly irrelevant and lacks context. With an approach that focuses on manual and generic reporting that is not tailored to the organization's Priority Intelligence Requirements (PIRs), security teams are acting on obsolete data – failing to provide comprehensive and efficient solution to their organizations.

Sixgill firmly believes that the only way to handle information overload and to scale intelligence analysis is through automation. By utilizing artificial intelligence and machine learning algorithms, Sixgill automates the production cycle of cyber intelligence - from monitoring through extraction to production, significantly increasing ROI for its customers and partners. Sixgill provides its customers' security teams with a powerful set of tools that can help them uncover patterns in cyberattacks directed at them and the conversations in the dark web related to their assets. The Sixgill platform positions security teams to extract granular details of instances in which their company or any of their companies' clients have been mentioned as part of a hacker's activity on the dark web. Also, the platform has built-in optical character recognition (OCR) capabilities to help companies make sense of data represented in pictorial format or in foreign languages. The robust data collection mechanism thus leaves security teams with data such as a threat actors' usernames, activity log, social network, active times, and languages known, among other details. These details can be used by law enforcement officials to zero down on criminals and their networks. For companies, this information can help them understand the patterns between attacks they face. Apart from keeping a close watch on conversations mentioning their own company, security analysts can also use the Sixgill platform to closely monitor vulnerabilities in software solutions that are widely deployed across their organization and on CVEs that could be exploited in future attacks.

Security operations teams in large enterprises deal with numerous tools in order to manage security functions for a complex security infrastructure. Consequently, this leads to alert fatigue, a situation where security teams do not deal with security alerts efficiently as they are overwhelmed by the sheer number of alerts that lack actionable insights into how to remediate them. Sixgill, to improve the user friendliness of its platform, has taken steps to ensure that it has well-designed graphic user interface (GUI) components and that alerts are sorted and organized as per their criticality. This way, security teams can prioritize remediation of the alerts. Moreover, users are provided with a clear point-to-point action plan to ensure appropriate steps are taken.

Sixgill's solutions have been implemented widely and have helped companies in a variety of industries fight cybercrime. Some notable deployments of the Sixgill platform are from the finance, government and law enforcement sectors. As an example earlier in 2019, the company uncovered organized underground networks focused on credit card fraud in the gaming industry (Fortnite).

Frost & Sullivan finds that Sixgill has enabled a novel, holistic security posture assessment through its threat intelligence platform and has provided its clients with the unmatched ability to track and stop attackers in their tracks.

Scalability and Customer Acquisition

At its core, Sixgill relies heavily on big data analytics techniques and thus thrives on large data sets that can feed into creation of actionable insights. The platform is built to serve, among others, large institutions and law enforcement agencies, both of which have a vast geographical presence and thus also have complex security infrastructure. To serve clients with such deployment scenarios, Sixgill encourages them to feed the platform with a detailed list of keywords related to their brand, product, customers, and even details about software that they use. Each time activity around any keyword is detected, the platform assesses its relevance and delivers the alert and recommendations in accordance with its priority to the client. In deployments where security teams have updated the platform with a detailed list of keywords, the platform can extract a comprehensive list of activities that will provide the security team with visibility into the entire cybercrime cycle from target selection, reconnaissance, and planning to the actual sale of information goods.

Sixgill's platform is generally offered to clients as SaaS-hosted over secure cloud infrastructure with no need for software or hardware installation at the client end, so as to enable easy deployment. For clients whose operations are highly sensitive, the platform is provided on-premise, which can be supported by Sixgill analysts. Moreover, the company has developed internal capabilities to support clients and their security teams in understanding the deep and dark web and making the best use of the tools at their disposal.

Frost & Sullivan appreciates that the company has designed its solution to meet the needs of MSSPs (managed security service providers) serving larger companies in designing their cyber defense strategies. Moreover, Sixgill recently signed a partnership agreement with Anomali, a threat management and collaboration solutions provider to reach a wider client base, and it has inked partnerships with MSSPs around the world, enabling numerous companies to navigate through a complex security ecosystem.

Conclusion

In a remarkably short time, Sixgill has emerged as one of the most innovative CTI vendors in the region and among the few companies that has gone above and beyond protecting clients from cyberattacks,by offering automated and actionable intelligence allowing companies to take a proactive approach in cybersecurity initiatives.

Sixgill's efforts have provided the industry with impressive visibility into the inner functioning of the cybercrime industry, diving deeply into the dark web and the business models fuelling its growth. For its strong overall performance, Sixgill is recognized with Frost & Sullivan's 2020 Technology Innovation Award.

Significance of Technology Innovation

Ultimately, growth in any organization depends on finding new ways to excite the market and maintaining a long-term commitment to innovation. At its core, technology innovation, or any other type of innovation, can only be sustained with leadership in 3 key areas: understanding demand, nurturing the brand, and differentiating from the competition.

Understanding Technology Innovation

Technology innovation begins with a spark of creativity that is systematically pursued, developed, and commercialized. That spark can result from a successful partnership, a productive in-house innovation group, or a bright-minded individual. Regardless of the source, the success of any new technology is ultimately determined by its innovativeness and its impact on the business as a whole.

Key Benchmarking Criteria

For the Technology Innovation Award, Frost & Sullivan analysts independently evaluated 2 key factors—Technology Attributes and Future Business Value—according to the criteria identified below.

Technology Attributes

Criterion 1: Industry Impact
Requirement: Technology enables the pursuit of groundbreaking ideas, contributing to the betterment of the entire industry.

Criterion 2: Product Impact
Requirement: Specific technology helps enhance features and functionalities of the entire product line for the company.

Criterion 3: Scalability
Requirement: Technology is scalable, enabling new generations of products over time, with increasing levels of quality and functionality.

Criterion 4: Visionary Innovation
Requirement: Specific new technology represents true innovation based on a deep understanding of future needs and applications.

Criterion 5: Application Diversity
Requirement: New technology serves multiple products, multiple applications, and multiple user environments.

Future Business Value

Criterion 1: Financial Performance
Requirement: Potential is high for strong financial performance in terms of revenue, operating margins, and other relevant financial metrics.

Criterion 2: Customer Acquisition
Requirement: Specific technology enables acquisition of new customers, even as it enhances value to current customers.

Criterion 3: Technology Licensing
Requirement: New technology displays great potential to be licensed across many verticals and applications, thereby driving incremental revenue streams.

Criterion 4: Brand Loyalty
Requirement: New technology enhances the company's brand, creating and/or nurturing brand loyalty.

Criterion 5: Human Capital
Requirement: Customer impact is enhanced through the leverage of specific technology, translating into positive impact on 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 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.