YL VENTURES

The CISO Current Report

Q3, 2019

ABOUT YL VENTURES

YL Ventures funds and supports Israeli tech entrepreneurs from seed to lead. Based in Silicon Valley and Tel Aviv, the firm currently manages $260 million and exclusively invests in cybersecurity.

YL Ventures' focused strategy allows it to conduct a rapid and efficient evaluation process and support each of its portfolio companies, both strategically and tactically, across multiple functions post-investment. The firm is uniquely focused on supporting the U.S. go-to-market of early stage companies and leverages a vast network of industry experts, CISOs and U.S.-based technology companies as advisors, prospective customers, and acquirers of its portfolio businesses.

The firm's global network and footing in the U.S. has always counted among its most powerful assets: YL Ventures bridges the gap between Israeli innovation and the U.S. market. The firm has formalized and amplified this core competitive advantage through the launch of the YL Ventures Advisory Board.

The Venture Advisory Board is comprised of over 60 security professionals from leading multinationals, including Akamai, Walmart, Netflix, Nike, Spotify, CrowdStrike, and Aetna. The firm's relationship with its advisors, as well as its extended network, is symbiotic in nature: the advisors bolster the YL Venture investment team's due diligence process and provide the firm's portfolio companies continuous support across a multitude of functions throughout their lifecycles. In return, network members benefit from exposure to pre-vetted Israeli cybersecurity innovations and receive direct exposure to a market second only to the U.S. in cybersecurity innovation.

Active portfolio

orca security · Hunters. · VULCAN · MEDIGATE · AXONIUS · Karamba Security · RIDEVISION

Exited/acquired

Twistlock · HEXADITE · Seculert · BlazeMeter · FIRELAYERS · clicktale · AcceloWeb

YL VENTURES
The CISO Current

TABLE OF CONTENTS

INTRODUCTION

YL Ventures frequently confers with an extended network of prominent cybersecurity professionals, including our Venture Advisory Board and industry executives, to assess our portfolio prospects, fine-tune market predictions, and facilitate portfolio company business development. As such, we have established direct lines of communication with the global market's preeminent CISOs and cybersecurity experts for ongoing insights into their thoughts, priorities, and opinions about the state of their organizational cybersecurity.

We recognize the value this information presents to entrepreneurs, especially those wishing to enter the U.S. cybersecurity market, and to the cybersecurity community as a whole. For this reason, YL has launched 'The CISO Current', under which we will publish reports containing gathered intelligence for general use. This document constitutes the launch of the initiative, and contains data gathered from direct interviews surveying over 30 cybersecurity executives at leading enterprises.

Our distinguished participants responded to a series of questions (see Appendix) to provide our analysts with insights into the cybersecurity market's concerns and opportunities. They were very candid throughout the information-gathering phase and were keen to stress exactly which challenges future solutions ought to meet and which sectors are disproportionately addressed by the market.

We extracted the particularly illuminating conclusion that CISOs are primarily focused on bolstering operational cohesiveness, efficiency, and effectiveness in terms of human capital in complex, large-scale environments. As such, CISOs are significantly more inclined to invest in management solutions that can achieve this end than simply investing in platforms that secure new technological frontiers. We hope the observations compiled in this report will prove to be a useful resource for aspiring cybersecurity entrepreneurs and the entire cybersecurity community.

THREE LEADING ISSUES IN TODAY'S CYBER SECURITY OPERATIONS

We began this quarter's interview process by asking our experts about the single biggest obstacle they face in their daily line of work. We extracted three major concerns from their responses.

Human Capital

The majority of respondents are primarily concerned with a broad range of operational issues relating to human capital. They are classified as follows:

Recruiting quality personnel: The current market shortage of cybersecurity expertise is hampering cybersecurity departmental efforts to find seasoned and talented personnel^. This challenge only intensifies for those looking for industry-specific specialists. Further exacerbating the issue is the "strong seller's market" for experts and new talent alike^^. Many CISOs currently bring in consultants to mitigate their sourcing issues.

Training personnel and closing skill set gaps: This issue exists in tandem with the factors that have led to talent sourcing difficulties. Many cybersecurity specializations are new; The literature documenting those specialties and related best practices are still in development. As a result, many candidates are forced to learn on the job. Further, the cybersecurity sector is rife with turnover due to the high attrition rates associated with mundane and repetitive first-tier tasks. Consequently, CISOs are forced to invest in many extensive, resource-intensive training and onboarding processes. Such costly investments are also required whenever companies move into new spaces or make new acquisitions in which security personnel are expected to develop new capabilities and execute novel, unfamiliar tasks.

Reining in non-security employees: Engaging, training, and increasing the awareness of non-security personnel in cybersecurity matters is difficult. Many non-security employees often view cybersecurity protocols as nuisances instead of critical functions and are unmotivated to implement them. Companies with high turnover experience this challenge more intensely, as each new hire requires a new security onboarding process. Meaningfully overseeing the few processes that non-security employees do manage to implement presents an additional challenge. Unfortunately, CISOs cannot afford to acquiesce, as cyber-attacks often begin by targeting the most vulnerable component of an organization – its people.

Tool Management

Cybersecurity tool management is an increasing concern, as cybersecurity stacks grow in complexity and volume.

Several of the experts in our network are concerned about issues arising from hosting multiple point solutions, which has resulted in overlapping capabilities and an exceedingly high volume of threat data and alerts. Many have experienced or anticipate inevitable alert fatigue and worry that they are unable to maximize outcomes from their data. Moreover, many indicate that they have difficulty managing and prioritizing alerts, struggle to keep installed systems updated, and are lacking holistic visibility across all of their security assets.

^The 2018 (ISC)2 Cybersecurity Workforce Study placed the overall gap at 2.93 million. ((ISC)2. Cybersecurity Workforce Study 2018, 2018). Moreover, the ISACA 2019 State of Cybersecurity reports that nearly 60 percent of organizations "experience at least three months of unfilled cybersecurity positions when hiring new staff". (ISACA. State of Cybersecurity 2019. Part 1: Current Trends in Workforce Development, 2019, p.7)
^^The ISACA also noted that "[t]he environment of need in the cybersecurity field has led to a strong seller's market for cybersecurity professionals, creating a retention problem for enterprises". They moreover discovered that 82 percent of organizations have indicated that most cybersecurity professionals left their organizations for better financial incentives, such as salaries or bonuses, at other organizations". (ISACA. State of Cybersecurity 2019. Part 1: Current Trends in Workforce Development, 2019, p.11)

They voiced interest in acquiring a solution or tool that can help them map and prioritize tooling investments.

Overall Security Program Management

Many CISOs experience difficulty in attempting to quantify risk to inform their cybersecurity investments. Several executives felt that the industry has yet to develop standards of methodologies, toolsets, and practitioner guidelines to carry out ROI analyses. This gap begs the question of whether cyber practices actually add value to an organization—and if they do, exactly what that value translates into financially. A related problem arises from discrepancies in business expertise between many CISOs and their peers. As the industry matures and moves away from its current compliance focus to a more risk-based approach, there will be an increased need for toolsets and methodologies to manage cybersecurity programs and investments.

FUTURE PAIN POINTS

In this portion of the interview process, we asked CISOs to share their projections of future cybersecurity issues. Many tied their responses to existing issues that have yet to be resolved or that they anticipate will worsen over time.

IoT

The most recurring concern about future cyber challenges pertains to the Internet of Things (IoT). Connected devices are proliferating with no signs of stopping^^^. These devices have become integrated into nearly every facet of life, from refrigerators to cars to medical devices. As there are different cybersecurity offerings for different IoT devices, managing the security of all of these devices in concert is a challenge. This is exacerbated by the fact that many enterprises still hesitate to make IoT security investments. Our respondents voiced a need to better tackle IoT cybersecurity for their respective enterprises as a whole, instead of relying on silos of solutions.

Data Governance and Security

There is a growing desire for tools that can create a holistic view of organization data and its flow, as well as seamlessly apply security and privacy policies across it. This need specifically relates to recurrent concerns like data tokenization, data anonymization, and both direct and indirect data sharing between companies. Further, Identity and Access Management (IAM) has been projected to remain a concern. Many experts see ample opportunity in the challenges surrounding online credentials for sectors like finance and retail. Companies have yet to provision and de-provision access at an optimal speed, if they do at all. Those that do grant such access still struggle to carry it out in a cloud-friendly manner.

Regulatory Environments

Many of our experts specifically shared concerns about regulatory environments within the context of privacy, as regulatory pressure, such as for GDPR compliance, continues to increase in this sphere. Companies, especially in highly regulated domains, will have to continue to expand their teams to keep up with this pressure. Many organizations are beginning to turn to third-party security vendors to implement these functions. Those same companies are also looking for the right technologies and tools to handle these new demands, and have had to increase their cooperation with the legal arms of their organizations. Larger firms have shifted focus to pre-empting future legislation to anticipate any significant restructuring ahead of time.

^^^According to Gartner, over 20 billion devices will be connected to the Internet worldwide. (Gartner, *Leading the IoT*. Introduction, 2017.)

AUTOMATING MANUAL PROCESSES

We asked our participating experts to share which currently manual processes they would like to automate.

Incident Response

Incident response was highlighted as the top operational activity that our network is looking to automate. Most experts agree that the majority of detection and response mechanisms can be automated. In fact, a number of interview participants are already implementing various stages of automation in this field, including ticketing, alerts, and even next-level remediation.

The drive to automate incident response relates to how personnel-intensive operations are within an organization. Automation is needed for log collections in transactions, data analysis, Tier 1 and 2 filtering, and repairing common incidents. Our respondents predict that machine learning (ML) and artificial intelligence (AI) will be key enablers in helping them navigate this field. Respondents also articulated a need for "next generation" SOAR to automate the workflow among different tools. Interviewees anticipate challenges in setting best practices for handling this automation as well as ensuring that conflicting technologies do not present barriers to deployment. Vulnerability management, such as remediation and patch management, has specifically been earmarked as an important point of automation.

Repetitive Processes

Repetitive processes as a whole were also cited as "low hanging fruit" for automation. Analysts are currently encumbered by the responsibility of carrying out many repetitive tasks manually. Many of our experts voiced an interest in finding a niche of heavy operational repetition that does not require any human skill set as an opportunity for automation, such as phishing email triage.

PROMISING VENTURES FOR EARLY ADOPTION

However, automatic detection and response solutions, specifically autonomous threat hunting, earned a number of notable mentions. These solutions include monitoring and detection tools that automatically aggregate logs, use ML, and consolidate all security data in a single location. The end goal of these solutions would be to reduce the workload before it even reaches humans. Solutions that automate the threat hunting process were voiced as particularly desirable, although they face a significant adoption barrier due to the deficit in human talent and skill to support threat hunting operations.

Respondents also revealed their needs in the domain of vulnerability management. They are searching for solutions that can automatically and continuously report, prioritize, remediate and correlate results of vulnerability management solutions with other platforms.

BIG BUDGET ALLOCATIONS THAT HAVE YET TO BE SPENT

Our research moreover explored areas in which CISOs are already prepared to invest:

Data governance and compliance

Several of our experts conveyed that existing data governance solutions are either robust and scalable, but not cost effective, or conversely cost effective, but unstable and difficult to scale. An affordable, robust, and scalable solution in this space is needed. Respondents are looking for GRC (Governance, Risk management, and Compliance) management tools as a whole to overcome the fact that many GRC tools are either antiquated or require multiple staffers to make them work at all. Our respondents also voiced interest in solutions that can address

compliance gaps for multiple regulations across different regions.

IAM

Respondents expressed their desire for access control and IAM solutions for unknown and unsanctioned SaaS applications. Many CISOs are concerned with unsanctioned tools and the need to understand what they are and where they are deployed. CISOs also require greater access control within customer account management systems and the ability to carry out robust and dynamic security actions within those environments, such as granting access permissions on a timely basis.

OVER-HYPED TRENDS IN CYBERSECURITY

We detected a common thread of criticism from our experts about industry trends that are overpromoted. We distilled them into the following two categories:

Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) were the most overwhelmingly common responses. Our experts insist that the hype surrounding both of these emerging technologies does not match their real-life usage and application. They specifically point to promotional trends surrounding AI-based threat detection as tired and overestimated. Today, nearly every vendor claims to offer AI-oriented solutions in broad, sweeping terms that leave many of our experts feeling that their AI use is more focused on form than substance.

Blockchain

Blockchain is another buzzword our experts suggest is overused and under-realized, both for cybersecurity solutions targeting blockchain and blockchain-based solutions for cybersecurity. Many respondents expressed that, because the underlying technology is still under development, blockchain is not ready for mainstream cybersecurity deployment. Interviewees went on to share that a problem has yet to arise for which blockchain is the appropriate solution.

CYBERSECURITY RISKS IN CLOUD ADOPTION

We asked our executives about the most pertinent cybersecurity risks that most concern them in their migration to cloud environments.

We were unable to extract a definitive trend from respondents' answers to this question. However, a comparatively recurrent concern was the ability to secure hybrid environments through "one plane of glass" – a single solution for cloud security issues across on-premises, private, and various public cloud infrastructures. Our expert network also voiced concerns over multi-cloud security, given that most enterprises consume cloud infrastructure from different vendors.

Moreover, as cloud migration continues to dominate the industry, many companies are migrating legacy apps to the cloud. These migrations are particularly risky endeavors, given that security in legacy applications is often omitted when transitioning those apps to the cloud. As such, when "lifting and shifting" legacy applications into the cloud, security around new environments is often overlooked. Many of the inherent risks of these moves lie in companies cutting corners and refusing to restructure application architecture.

Finally, asset visibility, already proven to be an issue in on-premises environments, is re-emerging as a challenge in cloud environments, which are ephemeral and distributed.

FINAL OBSERVATIONS

It is paramount for startups to understand the needs and concerns of CISOs in order to successfully break into the market. Our compiled insights this quarter most notably reveal how CISOs are prioritizing their operational concerns over the acquisition of “blue ocean” technology. CISOs have become wary of buzzwords and are instead focusing on how to optimize basic security functions in complex, large-scale environments. They are searching for management solutions that can assist with siloed products and quantifiably extracting the most value out of their existing security stack.

APPENDIX

Interview prompts:

- What are the three biggest problems you face in your daily cybersecurity operations?
- Can you share 2-3 fields that you anticipate are going to be major pain points in the future?
- Are there any manual processes run today that could ideally be automated?
- What technologies/solutions/value propositions are you likely to adopt early or engage with as a design partner?

OUTREACH AND CONTACT INFORMATION

This report was compiled with Israeli cybersecurity entrepreneurs in mind. If you are an Israeli-based start-up looking for guidance for seed-stage funding, we invite you to contact YL Ventures Partner & Head of Israel Office, ***Ofer Schreiber****, at ofer@ylventures.com.*

We would like to sincerely thank all of the CISOs that participated in this report. If you are an industry insider and would like to be interviewed for the next edition of the CISO current, please contact YL Ventures Partner, ***John Brennan****, at john@ylventures.com.*

We also invite any questions relating to this report to be directed to YL Ventures Analyst, ***Naama Ben Dov*** *at naama@ylventures.com.*