Smarter Security: Cybersecurity must Learn and Evolve to Match the Environment

Published 23 March 2021

Team8
Global venture group

The pace of change in technology brings immense complexity to security causing organizations to integrate dozens of products. Orchestrating this is a growing challenge and contributes to technology debt and overhead. Further, an expanding enterprise network and shortage of cyber talent, combined with an adversary leveraging increasingly sophisticated capabilities, is stretching response capacity to its limits. Smarter security solutions can incorporate automation, data, and AI to plug the gaps and provide teams with greater leverage on their human capital.

Organizations are deploying and managing an increasing number of security tools to manage ever-expanding networks. In fact, larger organizations deploy 130 cyber tools on average.1 Chief Information Security Officers (CISOs) are being bombarded by vendors with tools that solve specific problems but don't interoperate. Beyond the initial purchase price, the hidden costs of managing these tools, making sense of the data generated, and the time it takes for the security operations center (SOC) to tie it all together for actionable information are overwhelming. The global shortage of skilled cyber talent exacerbates the problem. The United States faced a shortfall of almost 314,000 cybersecurity professionals as of January 2019. By 2022, the global cybersecurity workforce shortage has been projected to reach upwards of 1.8 million unfilled positions.2 Employers today are desperate for people with real technical skills who can design secure systems, create new tools for defense, and hunt down hidden vulnerabilities in software and networks. At a time when attackers are accelerating attacks by employing AI tools, the talent shortage is more pronounced. Smarter security can alleviate the deficit facing defenders by using automation not purely to eliminate human error or save money, but also to empower security teams to be able to defend against attacks at the same rate at which they're happening.

Impact - Enterprises need software engineers and systems that are focused on APIs and more useful interfaces to enhance security analyst productivity. They need tools that facilitate comprehensive security orchestration. And they need smarter security that leverages automation, data, and AI so that humans can focus on decision making around exceptions, while security solutions analyze data, automate processes, learn over time, and automatically enforce policies.

Solutions - Security Orchestration, Automation, and Response (SOAR), Security Information and Event Management (SIEM), Robotic Process Automation (RPA), Logging & Analytics, Security Policy Automation

Perspectives:

- **Defender's Perspective** - "*In a post SolarWinds environment, there will be a renewed focus on integrity of the code base, digital supply chain and APIs to monitor and distinguish between purposeful changes and malicious ones. Even the most robust security teams will need creative solutions to handle the growing number of alerts and identify tamper evidence with enough fidelity to subvert a sophisticated attack. Smarter security can not only aid security professionals in executing on their mission, but will enable human capital to run more investigations and prevention activities in parallel*." - Admiral (Ret.) Michael Rogers, Former NSA Director, Team8 Operating Partner.
- **Team8's Attacker Perspective** - "Security automation allows the defender to react faster and augment the human element. In some cases taking it out of the loop entirely. In the future, attackers might do the same. Attacker automation will shorten the time from initial breach to crown jewels access and might threaten the concept of a manned SOC reacting to attacks. Attacker automation will try to "outpace" the defense in a bot-to-bot war."
We hope you have found our series of eight blogs on key cybersecurity themes both helpful and informative.

We hope you have found our series of eight blogs on key cybersecurity themes both helpful and informative.

The views expressed in this blog are those of Team8, any reference to "we" should be considered the view of Team8 and not necessarily those of WisdomTree Europe.

Team8 is a global venture group with deep domain expertise that creates companies and invests in companies specializing in enterprise technology, cybersecurity, and fintech. Leveraging an in-house, multi-disciplinary team of company-builders integrated with a dedicated community of C-level executives and thought leaders, Team8's model is designed to outline big problems, ideate solutions, and help accelerate success through technology, market fit and talent acquisition. For further information, visit ***www.team8.vc****.*

1 https://biztechmagazine.com/article/2019/03/rsa-2019-most-organizations-use-too-many-cybersecurity-tools

2 https://www.csis.org/analysis/cybersecurity-workforce-gap

Related blogs

+ Introducing cybersecurity, the megatrend of the 2020s

+ Cloud security: A necessary component in digital transition planning

+ Security of Things: Dealing properly with the explosion of connected devices

+ Perimeterless world: Networks are becoming less tied to physical locations

+ Privacy & Digital Trust: 2010' s were about Data Collection, 2020' s will be about Data Protection

+ Shift-Left: Security is a Part of all Phases in Software Development

Related products

+ WisdomTree Cybersecurity UCITS ETF – USD Acc (WCBR)

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an oer for sale nor a solicitation of an oer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can oen lead to a number of dierent interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public oering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any ailiate, nor any of their respective oicers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.