CISO MindMap 2020: Summary of Recommendations for Updating Security Programs

Rafeeq Rehman
rr AT rafeeqrehman.com[*]

June 28, 2020

Abstract

Cybersecurity is a complicated business. Many people outside this profession don't fully realize and appreciate the complexities of the job. CISO MindMap [4] is an effort to educate public about Cybersecurity professionals' job responsibilities. The MindMap also enables Cybersecurity professionals design and refine their security programs. Each year, I also publish recommendations along with the updated MindMap to cover changes in threat landscape and impact of new technologies. The latest version of CISO MindMap includes eight recommendations to consider for updating your security program and roadmap. This paper provides a rationale behind these recommendations, why one should care about these and steps you can take to make a progress.

Keywords : SASE, Cloud, SOAR, Zero Trust Architecture, Secure Enclave, Edge Computing, Deception

The eight recommendations included in CISO MindMap 2020 are listed below. The main objective of providing these recommendations is to help you consider specific *focus areas* that can bring significant value to your program, reduce risk, and enable business. These recommendations are based upon research reports from different security organizations, research, and my interactions with Cybersecurity leaders.

1. Improve SOC analyst productivity with SOAR
2. Reduction/consolidation of tools/technologies
3. Better protection & monitoring of Cloud
4. Explore new architecture models like SASE
5. Consider zero trust and secure enclaves
6. Edge computing security
7. Include deception technologies as part of security tools
8. COVID19 and Work from Home

The following sections provide a brief description of each of the above recommendation. Depending upon the current maturity level of your program, you may already be on a journey to explore or implement some of these recommendations. If you have not started yet, please note that these recommendations are provided to further improve and not necessarily as a replacement of any other parts of your overall security program. This list does not reduce importance of any other activities to manage risk to your organization. Phishing is still there, ransomware attacks are still happening and you still need to manage compliance needs!

1 Improve SOC analyst productivity with SOAR

What is it? Security Orchestration Automation and Response (SOAR) refers to technologies for collecting threat intelligence and other information to help automate triage, create digital workflows, and automate incident response tasks. SOAR technologies help reduce time to respond to events and enhance efficiency of SOC staff significantly.

Why should I care? We know that Security Operations Center (SOC) staff is over burdened with number of security events and incidents they have to deal with on a daily basis. The main objective of SOAR is to reduce cost of responding to average incidents and use automation for many routine tasks as part of incident response process. In addition, SOAR can also help improve morale and job satisfaction for the SOC staff by eliminating need for manually carrying out low level routine tasks.

What steps can I take? SOAR tools are becoming

[*] Rafeeq Rehman is an author, entrepreneur, and information security advisor based in Columbus OH. He blogs at rafeeqrehman.com and can be reached via email, LinkedIn, or twitter handle @rafeeq_rehman

mature and there are a number of options available from many vendors. While selecting a SOAR tool, consider your SIEM implementation, threat intelligence sources, your existing security technologies, and SOC processes. SOAR is a complimentary technology and usually is not considered a replacement of any other tools (unless you have existing, home-grown tools that you want to replace with a commercial technology).

2 Reduction and consolidation of tools and technologies

What is it? All CISOs are dealing with complexity of effectively integrating a large number of security tools and technologies. The consolidation is taking place and majority of the organizations are now using less than 20 security technologies[6] which is an improvement compared to just few years back.

Why should I care? When it comes to number of technologies used for security, more is not necessarily a good thing. As a principle, *complexity is enemy of security.* More and more vendors and technologies also strains resources to effectively implement and integrate, creating less-than-optimal configuration and wastage of money.

What steps can I take? First of all, resist the urge to purchase new tools. Evaluate existing technologies to identify overlaps in functionality. Map usefulness of each tool in achieving your risk management objectives. Build a roadmap to consolidate technologies and vendors. This will reduce overall cost and ensure that your investment in tools don't end up to be shelfware.

3 Better protection and monitoring of Cloud

What is it? As more and more organizations move to Cloud, data breaches in the Cloud are increasing. Major reasons for this increase include misconfiguration and errors as shown in the Verizon Data Breach Investigations Report[7].

Why should I care? CISOs are responsible to enable migration to Cloud and at the same time protect assets in public or private Cloud environments. Managing Cloud technologies is different than traditional corporate data centers in many ways. IT staff is still not well trained in properly understanding Cloud services and securely configuring Cloud environment.

What steps can I take? Start with training security staff in Cloud security and use of Cloud-native options to manage security. Implement solutions to continuously monitor Cloud configuration. Implement a CASB[3] solution to enhance visibility into Cloud. Some specific areas to consider are:

- Better understand Cloud native options provided by your Cloud Service Provider.
- Take into account options from other security vendors.
- Enhance visibility into Cloud.
- Prepare for incident response in the Cloud which is different than incident response in corporate data centers. For example, proactively establish network segments in the Cloud where you will move your workloads in case you have to take images of a running system.
- Consider using deception technologies for breach detection.
- Continuously monitor for errors and configuration flaws of your Cloud environment.

4 Explore new architecture models like SASE

What is it? Gartner published a report in 2019 "The Future of Network Security Is in the Cloud" that introduced Secure Access Service Edge or SASE[2]. This concept is getting industry backing and provides some good ideas to improve security programs.

Why should I care? SASE architecture is interesting for CISOs to enable delivery of security services from the Cloud and convergence of network and security services. Reducing complexity is another area that makes SASE interesting.

What steps can I take? Most organizations have just started to get acquainted with the concepts and are in very early phases of defining a SASE strategy. However, security vendors are creating a hype about SASE and using it as a new buzz word coupled with *"me too"* messaging. CISOs need to carefully educate themselves and their teams, understand different offerings, and strategies that different vendors are pursuing. Implementing SASE architecture will be a multi-year project, but start with spending time in evaluating your options.

5 Consider zero trust architecture and secure enclaves

What is it? A zero trust architecture (ZTA) is a key concept for any modern network. According to NIST, in a zero trust architecture, *"there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet). Authentication and authorization (both user and device) are discrete functions performed before a session to an enterprise resource is established."*[1].

If fully implemented according to NIST guidelines[1], ZTA will help:

- Shift focus from protecting network segments to protecting assets and applications.
- Remove any notion of implicit trust based upon location or being on a particular network segments.
- Authentication and authorization *before* a establishing a session with a resource.
- Access to resource is granted on per session basis and through a policy.

NIST publication 800-207 is an excellent resource to get familiar with the ZTA model[1].

Why should I care? With migration to Cloud, mobile workforce, and work from home, people need access to applications and other assets/resources from anywhere. The old notion of *trusted network segments* and implicit trust based upon network location is no longer as relevant as it used to be. ZTA provides new paradigm where you turn focus on protecting applications, resources, and other assets instead of protecting networks.

What steps can I take? Start with educating technology people in your organization about this new paradigm, including everyone who is involved in designing and supporting information technology infrastructure. Create a ZTA strategy in collaboration with stakeholders before choosing products and vendors. You may already have technologies to implement some features of ZTA.

What about secure enclaves?

A growing number of use cases in healthcare, manufacturing, finance and other sectors require IoT devices and machines to be on public Internet or on third party networks (outside private corporate networks) with a need to securely communicate to backend systems. Examples include medical diagnostic machines sitting on hospital networks, ATM machines connected to public Internet, IoT devices and many others. Secure enclaves enable creating a policy-based overlay network to ensure these devices communicate to systems on the same enclave. The enclaves can also address privacy concerns for mobile users. Some enclaves technologies can enable one-to-one or one-to-many communication based upon policy. This is a specialized area and applicable to specific use cases.

6 Edge computing security

What is it? The main concept of Edge Computing is to reduce latency by bring decision making, computing, and data storage close to physical location where the action takes place[8]. Multiaccess Edge Compute (MEC) and 5G technologies are accelerating this trend.

Why should I care? Edge computing is essential to enable business of the future. Like Cloud, Edge computing brings new items to security paradigm requiring CISOs to ensure they enable their businesses by taking proactive actions. All major Cloud service providers, as well as telecom service companies, have edge compute initiative to cater for applications requiring low latency and high bandwidth needs. Essentially, Cloud service providers are bring Cloud to you instead of you taking your data and compute to the Cloud!

What steps can I take? Like other emerging technologies, understanding the evolution of edge computing is the immediate action for security professionals otherwise they will end up playing a catch-up game. It is important to understand the use cases of edge computing in your particular business and proactively define policies, understand compliance needs, and research technologies to secure edge computing.

7 Include deception technologies as part of security tools

What is it? Concept of deception is centuries old, almost as old as the recorded history of humankind. In computer networks, people have used honeypots for decades. New deception technologies combine older concepts with Cloud computing to catch bad actors on your network quickly and detect breaches early.

Why should I care? Delta between time to compromise and time to detect has been a reason of concern for a long time[7]. In many cases it takes weeks and months to detect a breach after the initial compromise. Deception technologies can bridge this gap and make detection very effective with a low rate of false positives.

What steps can I take? Multiple vendors have deception technologies commercialized. A *proof of concept* is a good starting point to test how these technologies work. Implementation will be much simpler than you think as most of the infrastructure stays in the Cloud.

8 COVID19 and Work from Home (WFH)

What is it? Work from home is not a new phenomenon[5]. However, COVID19 is giving it a completely new dimension and scale. Conceivably, COVID19 impact on WFH will be long lasting. Even if it does not, businesses will plan for any future pandemic or other emergency situation and make it part of their business continuity plans.

Why should I care? WFH brings new areas of risk management for CISO where employees need secure access to business applications on a mass scale, may be permanently working from locations with unknown physical security, access to confidential data from homes, printing confidential documents on their home printers, onboarding new employees without face-to-face meetings and so on. A CISO needs to make WFH a permanent part of their security programs, at least for now.

What steps can I take? Updating data security policies, awareness campaigns to avoid phishing attacks related to COVID19, and protection of confidential data while enabling business processes are top actions for security leaders.

Final thoughts

Revising and improving an information security program is a continuous process. Ideas presented in the CISO MindMap 2020 and in this paper are an effort to help security leaders evaluate and update their program. Implementing all recommendations provided in this paper will not be an easy task. Some of these recommendations are actually multi-year long projects. The recommendation about these recommendations is to prioritize and pick the ones that make more sense for your particular organization.[1]

If you are a CISO and need some advice or want to share your thoughts, feel free to contact me for a brief conversation. We can learn a thing or two from each other!

References

[1] S Scott Rose (NIST) et al. *Zero Trust Architecture (2nd draft)*. 2020. URL: `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf`.

[2] Neil MacDonald, Lawrence Orans, and Joe Skorupa. *The Future of Network Security Is in the Cloud*. Analyst Report. Gartner, 2019.

[3] Netskope. *What is a cloud access security broker (CASB)?* 2020. URL: `https://www.netskope.com/about-casb`.

[4] Rafeeq Rehman. *CISO MindMap 2020: What do InfoSec professionals really do?* 2020. URL: `http://rafeeqrehman.com/2020/06/12/ciso-mindmap-2020-what-do-infosec-professionals-really-do/`.

[5] Sampath Sowmyanarayan and Val Elbert. *Return to business as unusual: Workplace of the future*. 2020. URL: `https://www.verizon.com/about/sites/default/files/Return_To_Business_As_Unusua-2020-White-Paper.pdf`.

[6] CISCO Systems. *CISO Benchmark Study: Securing What's Now and What's Next*. 2020.

[7] Verizon. *2020 Data Breach Investigations Report*. 2020. URL: `https://enterprise.verizon.com/resources/reports/dbir/`.

[8] Wikipedia. *Edge computing*. URL: `https://en.wikipedia.org/wiki/Edge_computing`.

[1] Recommendations in this paper should not be considered as professional advice. Opinions expresses in this paper are author's own and not of any of his employer or the organizations he works for. Mention of any vendor is not equal to endorsement. All trademarks and service marks in this paper are the property of their respective owners.