The Seven Habits of Highly Effective Security Teams

Introduction

Stephen Covey's bestseller, "The 7 Habits of Highly Effective People," has sold over 25 million copies translated into 40-plus languages. Many people will swear on it as a self-help bible that has changed their lives, made them more efficient, helped them achieve a work-life balance, and so on. If you are not one of the 25 million who either bought the book or one of the countless other millions who have borrowed someone else's copy, the sidebar has a quick recap of the seven habits—thanks to Wikipedia[1].

The Need for Effective People, Process, and Technology

Before we dive into how these seven habits apply to security, it might be worth considering why they are even necessary. It is often tempting to think that buying into the latest technology trends (which currently there is no shortage of, with machine learning, artificial intelligence, blockchain, and more!) will offer protection. However, one only has to look at some of the recent, large-scale data breaches[2] to understand that even companies that spend millions of dollars on the latest technologies still get compromised.

A significant contributing factor to this trend is that the job of defending the organization has evolved. The skills crisis and the lack of security expertise have been discussed ad nauseam, but the elephant in the room is that the pace of technological change and the associated increase in the complexity of the environment continues to accelerate. Here are three macro trends that are contributing to this security complexity:

1. What needs to be protected changes every day, if not multiple times a day. The sprawl of devices, including IoT, BYOD, VDI, shadow IT, etc., has resulted in many more devices in the organization than most security teams are aware of, making security updates difficult to manage.
2. Moving beyond devices, consider the volume of applications that house or process sensitive data. More and more business applications are being deployed in SaaS environments, including Dropbox and other services, which correlates with an increase in the number of S3 bucket breaches[3] you have probably read about.
3. The attacks themselves have evolved from the traditionally malware-heavy to "malware-free" living off the land attacks. The latter is the result of abuse of existing system tools used by administrators or powerful application capabilities (e.g., Microsoft Office macros) to further the malicious intent of a threat actor. This evolution means the traditional approach of using malware signatures or "indicators of compromise" is no longer effective at catching a determined adversary.

The 7 Habits of Highly Effective People

First Independence

The first three habits surround moving from dependence to independence (i.e., self-mastery):

1. **Be Proactive**
   Anticipate the problems rather than wait for them to happen before deciding what to do.
2. **Begin with the End in Mind**
   Focus on the destination while constantly evaluating where you are in the journey towards the destination.
3. **Put First Things First**
   Distinguish between what is important and what is urgent and prioritize accordingly.

Interdependence

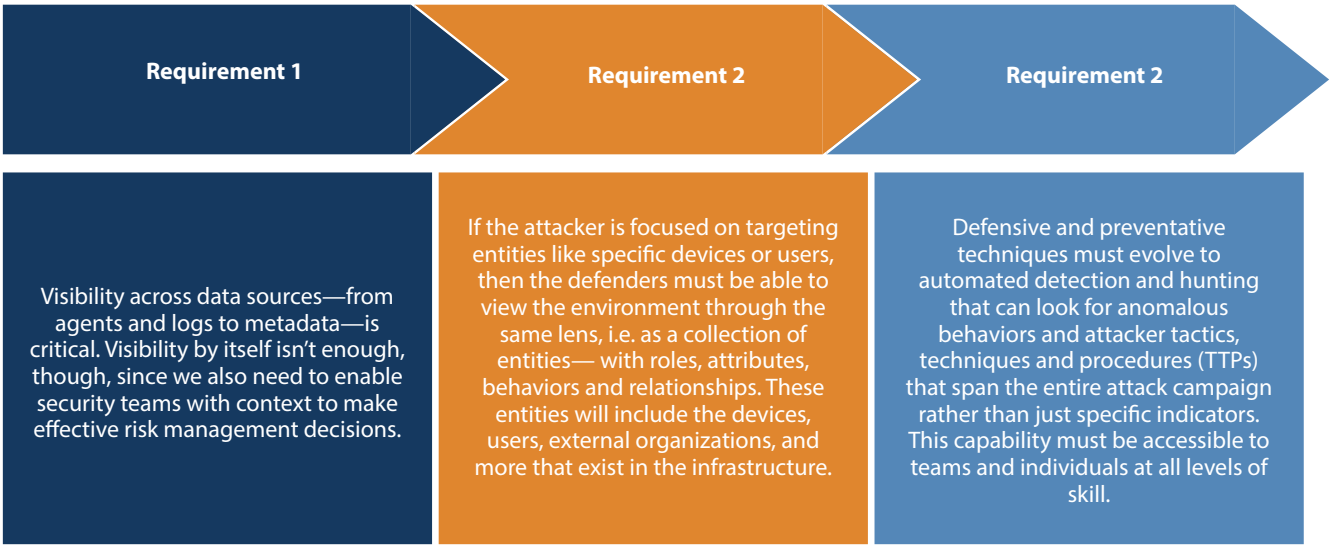
The next three habits talk about interdependence (working with others):

4. **Think Win-Win**
   Effectively collaborating so everyone is successful ultimately drives long-term positive results.
5. **Seek First to Understand, Then to be Understood**
   Said differently, listening begets listening which ultimately improves problem-solving.
6. **Synergize**
   It takes a village; most tasks these days need multiple people working in lockstep to achieve goals.

Continuous Improvements

7. **Sharpen the Saw**
   Learning from your mistakes and those of others ultimately makes you less likely to make the same mistakes again.

So, what do these trends mean for security teams? For starters, they force security teams to address new requirements as they plan for the future, including:



Applying the 7 Habits to Security Teams

With these new dynamics at play, teams continuing the same security practices of recent years are not likely to produce different results. The best security teams realize this and adapt. In conversations with hundreds of security teams, several recurring themes have emerged that map back to Stephen Covey's original seven habits.

As mentioned in the sidebar, the first three of Covey's habits focus on the foundation of "Self." In ours, we map these to the ability of the security team to adopt the automation techniques and tools to maximize the individual effectiveness of each member of the security team.

1. Manage your four data sources

Clearly, if you don't find out about something until after it gets hacked, it's too late. Being proactive means continuously collecting and managing available data from all three primary security data sources: the network, endpoints, and log/event data. Even more important is understanding what exists in that data that might be a threat. This is where a fourth critical data source comes into play: human procedural, institutional and tribal knowledge. Unless managed at least as well as the other three, this will leave the building when the SOC shift is over, or worse, when the person leaves the organization. Balanced investment in managing all four data sources prepares the organization to respond quickly and accurately.

2. Protect what really matters

An attacker clearly has an end in mind; do you know what that end is? This is an asymmetric fight with attackers needing to find the one weak link. It is vital; therefore, that security teams always operate with a threat model in mind. As someone once said, if you try to protect everything all the time, you protect nothing all the time. In most cases, the "things" being protected are "entities"—think users, devices, data, etc. But in most cases today, the currency for security teams are primitive and ephemeral attributes, like IP addresses and log sources. Using context data from locations such as directory services, HR systems, vulnerability and threat data, the analyst is then left with the task of correlating those entities with their attributes, behaviors, relationships and activity records. Fortunately, modern AI-driven security solutions do a better job of supporting security teams with technology that can extract signals from the individual data sources and automate this context gathering.

3. Put first things first

As one CISO put it recently, they almost never "respond to alerts"; instead alerts are just another data source in a comprehensive, risk-scoring scheme that defines priorities for their security team. The good news is once you have mastered habit 2 and have the entity

view of your enterprise (organization), you can start to look at them in the aggregate, viewing summaries of the behavior of those entities over time. Analytics on the entities can then identify anomalous behaviors, highlight what makes them unique and different in the environment, reveal how entities are similar to other entities, confirm which have access to the crown jewels, etc. Human knowledge (see Habit 1) might be able to add to the risk equation by annotating that entity as a VIP employee or someone who has just resigned etc. Compare that to today, where you see each alert in isolation, then guess what to prioritize.

In Covey's work, the next three habits focus on working well in the real world with a team. We apply that same principle to our next three habits for security teams:

4. Invest in technology that promises to enhance your people, not replace them

A lot has been made about the power of artificial intelligence and machine learning and its application to security[4]. Truth be told, these are not silver bullets that will eliminate your need for people, no matter how much vendor marketing teams might want you to believe that is the case. Instead, the best organizations have used these technologies to enable their teams to be more productive by eliminating duties like cumbersome context gathering (see Habit 2). It also brings a sense of consistency that is lacking when deliverables depend on tribal knowledge. When not executed correctly, though, these technologies can exacerbate your need for people[4].

5. Understand thy attacker

Unfortunately, many security teams and technologies are focused on defending against known attacker tactics. This approach is good at protecting known threats, but what about new ones? The most effective security teams go beyond detection solely based on IOCs to detection based on TTPs and behaviors. Specific malware or command and control (C2) domains are easy for an attacker to change, but any organization or individual attackers are harder pressed to change the underlying tactics, such as how they set up their C2 infrastructure or the non-malware tools they use once they are inside your environment. Successful security teams can detect and hunt based on attacker behavior or even behaviors that just don't fit in their environment—which emphasizes the need to understand what does fit your environment (see Habit 2).

6. Security is a team sport

A tiered model for the SOC, where most things get pushed to higher levels, simply isn't sustainable. Research shows that the difference between junior and senior analysts typically isn't the quality of their conclusions but rather their ability to support those conclusions with compelling evidence on which to base decisions. So, how do you bring the capabilities of those senior analysts to the junior ones? The win-win here is enabled by technology that eliminates the requirement of expertise to simply organize the data so someone can ask the questions that need to be answered. If junior analysts can take on tasks like triage, forensic investigations and timelining, which today not only take time but require deep expertise, those with deeper expertise can focus on continually evolving the organizations' capabilities to find threats, then codify that knowledge so that this virtuous cycle continues.

Finally, Stephen Covey focused on the notion of continuous improvement—making the collective better.

7. Don't make the same mistake twice

They say the definition of insanity is doing the same thing over and over while expecting different results. If that is true, many security practices are truly nuts! Often, lessons learned are not fed back into the process. As one CISO said, "the red team isn't allowed to mic-drop and walk away just because they successfully evaded security controls." Instead, every investigation and red teaming activity is not complete until it results in improvements to the system—even if it is as simple as documenting tribal knowledge, such as "Alice from Legal works from her home in Iowa." When the analyst on the next shift sees an alert about access to the data center from a DSL line in Iowa, at least they are not wasting time only to eventually find out what someone already knew.

Wrap Up

As the job of defending the organization continues to evolve, security teams must evolve as well. As of 2021, research shows that there are more than three million unfilled security jobs[5]. It is crucial now more than ever that security teams establish a repeatable process rhythm that drives consistency and gives them the best shot at protecting their organizations successfully. In our research, we spent thousands of hours talking to hundreds of security teams and the analysts within. What we learned is that the most successful teams adopt habits like the ones above to ensure all members are as effective at doing their job as possible. Our thanks to all of those teams that have helped shape this paper.

References

1. https://en.wikipedia.org/wiki/The_Seven_Habits_of_Highly_Effective_People
2. https://awakesecurity.com/mega-breach-lessons/
3. https://www.google.com/search?q=s3+bucket+breaches
4. https://awakesecurity.com/infosec-artificial-intelligence/
5. https://www.cnn.com/2021/05/28/tech/cybersecurity-labor-shortage/index.html

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor

Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard

#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062

Copyright © 2021 Arista Networks, Inc. All rights reserved. CloudVision, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. 12/21