The Next Board Problem:

Automatic Enterprise Security Orchestration — a Radical Change in Direction

By Rick Howard

Palo Alto Networks Chief Security Officer

Commercial boards and senior government officials may be the only groups capable of kick-starting this new and absolutely necessary direction in the evolution of cybersecurity. The network defenders that you have hired to defend your electronic assets are locked into a set of best practices developed over 20 years that make it almost impossible to veer away on a radically new path, a sound and exceptional path, but a path that goes against everything they have learned in their careers. In order to understand why this is a board issue, it is important to understand why commercial industry and government operations are at this critical intersection between best practices and new ideas.

This paper describes Defense-in-Depth and why it is a failed model. It also describes how network defenders adopted the Cyber Kill Chain model as a replacement but have not implemented it well. Finally, it describes a much better way to implement the Cyber Kill Chain model: the security platform. The security platform automates enterprise security orchestration from a single vendor with some key and essential trusted vendor partners. It effectively reduces complexity in extremely entangled environments, reduces vendor assessments that are consuming your network defender staff, and changes a tedious and manual process of converting indicators of compromise into prevention and detection controls into an efficient and automatic process.

Because of these things, the single vendor model significantly reduces the total cost of ownership (TCO) in your material risk mitigation efforts. The reason board influence is needed is that the idea of using a single vendor to do most of your security is anathema to many network defenders. In order for the idea not to be rejected at inception, board members and senior government leaders can facilitate a serious conversation with their CSO/CIO/CTO about the pros and cons of this radical idea.

THE STATE OF ENTERPRISE CYBER DEFENSE

In order to understand the current state of cyber defense, it is useful to first understand how commercial and government organizations got here. When companies began to leverage the internet for business purposes back in the 1990s, it quickly became apparent that cyber criminals and cyber spies could also use these new electronic marketplaces for their own illicit activities. Business leaders started hiring network defenders to protect their digital assets. The cybersecurity best practice that emerged was something called *Defense-in-Depth*. [1] [2] The idea was that network defenders would deploy multiple prevention and detection controls within their networks and hope that one or more of them would prevent successful cyberattacks. Typically, organizations would at least deploy a firewall, an intrusion prevention system and an antivirus system. Some organizations would deploy many more controls.

With Defense-in-Depth, network defenders hoped that the firewall would stop most attacks. If it didn't, then they hoped that the intrusion prevention system would. If that failed, they hoped that the antivirus system would. Some organizations would deploy multiple versions of the same control from multiple security vendors. In other words, they might deploy an intrusion prevention system from vendor A and another intrusion prevention system right behind it from vendor B; something the network defender community jokingly refers to as "Vendor-in-Depth."

Historical Note:

Who Coined the "Defense-in-Depth" phrase for Cybersecurity?

In 1976, Edward Luttwak published his book, "The Grand Strategy of the Roman Empire from the First Century AD to the Third," in which he coined the phrase "Defense-in-Depth" to describe his controversial theory about the Roman Army's defensive posture from the first to third century A.D. In 1980, leaders from the U.S. Nuclear Regulatory Commission published their guidance on protecting nuclear power plants built before 1979. They advocated for a Defense-in-Depth model. Dr. Fred Cohen published the first papers in 1991 and 1992 that used Defense-in-Depth to describe a common cybersecurity model in the network defender industry, but he did not claim that he was the first to use the phrase in that context. [1][2] So, I called him and asked. Dr. Cohen said that he was not the first to use it, but he was probably the first to describe it in a paper. [6]

Initially, the Defense-in-Depth philosophy worked fine, but as the cyber adversary began to mature, Defense-in-Depth became less and less effective. Network defenders learned that the philosophy was too general. It did not have enough precision to be effective. Cyber adversaries routinely found ways to bypass those controls. But the network defender community had no alternatives, and Defense-in-Depth remained the dominant security philosophy for 20 years.

During the first Gulf War in 1991, Iraq's SCUD missiles gave the United States Air Force and Navy pilots trouble. The Iraqi soldiers were able to fire many of them before the U.S. planes could find them and blow them up. [3] After the war, General John Jumper changed air combat doctrine by formalizing the techniques necessary to compress the time it takes to find and kill the enemy. He called it "compressing the kill chain." Instead of hours or days to complete the kill chain, he wanted to do it in under 10 minutes. [3] In 2010, researchers at Lockheed Martin revolutionized the network defender community by adopting the military kill chain model to network defense. They called it the Cyber Kill Chain™. [4]

The Lockheed Martin Cyber Kill Chain [4]

1. Recon their target for potential weaknesses.
2. Build a tool that will leverage those newfound weaknesses.
3. Deliver that tool to some endpoint on the target's network.
4. Use that now-delivered tool to compromise the endpoint and establish a beachhead for future operations.
5. Install a back door on the beachhead that will allow the cyber adversaries to return whenever they like to maintain persistence within the victim's network.
6. Establish a command-and-control channel that will allow the adversaries to fully control the beachhead and deliver more tools that will help complete the mission.
7. Take the actions to complete their mission. Since they are inside the victim's network now, the cyber adversaries can search for the information they came to steal, collect it, and exfiltrate it using the already established command-and-control channel.

In order for network defenders to defeat the cyber adversary – to compress the kill chain – they have to: Find them in their networks; Fix them in place; Track their behavior; Target them with the right prevention control; Engage them with that control; and then Assess the control's effects. The military uses the acronym F2T2EA as shorthand for this concept. [4] Lockheed Martin described it as a linked chain because the network defender has to accomplish every step in the F2T2EA system, or it completely falls apart. In order to do that, network defenders had to exactly understand how cyber adversaries moved through their victims' networks. It turns out, according to the Lockheed Martin research team, regardless of what hacker tools the cyber adversaries use or what motivates them to attack their victims in the first place, the hackers have to successfully complete the same seven tasks to accomplish their mission.

The Lockheed Martin research suggested that, now that the network defenders understood how cyber adversaries move through a victim's network, they could apply the principles of F2T2EA at each phase. In other words, network defenders needed to deploy prevention and detection controls at each link in the Cyber Kill Chain. This was a radical and disruptive idea presented at exactly the right time. Defense-in-Depth hadn't really worked in over a decade anyway, and this was calling for network defenders to be much more precise and complete with how they should deploy their security controls. They could no longer rely on the generic layers of defense they got with the Defense-in-Depth model. What they needed was the precision they got with the Cyber Kill Chain model.

The security vendor community responded in kind. They came out of the woodwork to build a cornucopia of innovative tools and controls designed specifically for every link in the Cyber Kill Chain. Pundits in industry call them "point products." Network defenders bought a ton of them. The result is that most medium- to large-scale organizations routinely deploy 10-15 point products in their environments from different vendors to cover the entire Cyber Kill Chain. Other smaller organizations usually do not have the resources to deploy that many tools. They typically fall back on the Defense-in-Depth model, if they pursue a model at all. Still, six years after Lockheed Martin researchers published their paper, the network defender community has adopted the Cyber Kill Chain model as the best practice even if they do not have the resources to fully implement it in their own networks. But there are problems.

Historical Note:
Limitations to the "Lockheed Martin Cyber Kill Chain" Name
The researchers at Lockheed Martin invented the phrase "Cyber Kill Chain" when they published their paper called "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." [4] Sometime after, the company leadership decided to copyright the phrase. [9] The impact of that copyright decision made it impossible for security vendors to use the phrase in any of their marketing materials. Consequently, every security vendor has a different name for the same concept, thus causing massive confusion in the security.

PROBLEMS WITH ORCHESTRATION OF THE CYBER KILL CHAIN

The Cyber Kill Chain has revolutionized the way network defenders think about securing the enterprise. The model is sound, but many struggle with the management of the system.

Too Many Tools to Manage

At least in the Defense-in-Depth model, network defenders only had to manage three or four controls. That was doable. With the Cyber Kill Chain model, they now had to manage three times that many tools. And the dirty secret in the security vendor space is that the vendors have pushed the responsibility to maintain that set of deployed point products, and the responsibility to orchestrate the data coming off those point products, to the network defender. What the network defenders did not realize back in 2010 was that they would end up buying point products four times. They have to buy the point product. Next they have to buy a person who can maintain the point product. Then they have to buy a person who understands the data coming out of the point product. Finally, they need to buy somebody who can stitch the data from all of their point products into something coherent in order to complete the F2T2EA system. This is hard to do, time-consuming and expensive. The result is that many of the deployed tools are poorly maintained, never fully up to date on the latest security intelligence, and the coherent adversary picture that was supposed to materialize with the F2T2EA system is rarely accomplished.

Too Much Complexity for Security

Besides the Cyber Kill Chain and Defense-in-Depth models, there is another network defender best practice. It is the idea that complexity is the worst enemy of security. [5] Unfortunately, with the explosion of point products deployed across the enterprise in the Cyber Kill Chain model, the security architecture for the enterprise exponentially got more complicated. If deployed correctly, the Cyber Kill Chain model gives network defenders more visibility into what is going on within their networks and multiple chances to prevent the success of the cyber adversary. But it also introduces a high degree of complexity within the environment, and hackers love complexity. The more complex it is, the easier it is for network defenders to make a mistake in the deployment. Leveraging those mistakes is what hackers do.

Too Much Wasted Time

Followers of the Cyber Kill Chain model have found themselves within an infinite loop of security vendor assessment. Many believe that they not only need to deploy security controls at every link in the Cyber Kill Chain but also the best-of-breed for that class of controls. To accomplish this, they arrange head-to-head competitions for every point product class that they own or plan to add to their Cyber Kill Chain architecture. These can take months to orchestrate. Buy decisions are usually made on the technical merits, regarding the speed of the point product on the network or whether or not the point product has the latest innovation. This was fine when they only had three or four tools deployed in their networks with the Defense-in-Depth model. Lifecycles of security products typically range between two and five years. This works out to be roughly one vendor assessment per year. But with the Cyber Kill Chain model, network defenders now have 10-15 controls deployed in their networks. Instead of maintaining and orchestrating what they already have deployed, they are continuously spending resources evaluating up to four security point products a year. This puts them on a continuous cycle of assessing vendor point products, forklifting the losing vendors out of their environments and the winning point products in to replace them. Instead of managing their existing security infrastructure, they are spending a lot of time managing the churn. This is wasted time.

Too Inefficient Crossing the Last Mile

Even with 10-15 point products deployed across the enterprise, that is still not enough for network defenders to prevent cyber adversaries from being successful in their attack campaigns. The thing that drives these security controls is intelligence. As cyber adversaries crawl through victims' networks, they leave clues in their wake. The industry calls these clues indicators of compromise. Security vendors and white hat researchers are in a continuous state of seeking new indicators of compromise. Once found, security vendors convert them into prevention and detection controls that they deploy to their customers in the field. The trick then for network defenders is to get these new controls installed in their deployed toolset down the Cyber Kill Chain as quickly as possible. This is called *crossing the last mile*. In other words, crossing the last mile is the process of finding new indicators of compromise, converting them to prevention and detection controls, and then deploying those controls to an already installed system in the environment. Security vendors do this for their products fairly well, but when a new indicator of compromise indicates that controls should be deployed across multiple products not owned by a single vendor, or when independent white hat researchers discover new indicators of compromise on their own, that is when things slow down. In certain situations, it may take days, weeks or even months to get the right security controls deployed into the F2T2EA environment. And if the network defender has more than a handful of tools deployed across the enterprise, keeping track of the status of each tool, and whether or not that tool has the most updated controls deployed for the latest intelligence, is a nightmare.

THE SOLUTION – AUTOMATIC ORCHESTRATION THROUGH A SECURITY PLATFORM

In the last three years, an innovation has emerged from the security vendor community that addresses these problems. The security vendor community calls it the "security plat-

form." It is an end-to-end system-of-systems where the deployment of security controls down the Cyber Kill Chain to establish the F2T2EA framework is accomplished from one security product built by one vendor. The platform contains most of the tools that network defenders have previously deployed separately from multiple vendors and manages the deployment of prevention and detection controls to every possible link in the Cyber Kill Chain automatically. Advanced platforms even automatically orchestrate the last mile by discovering new indicators of compromise on their own and deploying new prevention controls to counter them. Some innovative security platform vendors have even banded together to share threat intelligence to accommodate the discoveries of independent white hat researchers.

It is true that most of these new vendor platforms do not contain all of the tools that network defenders might need. To accommodate that, the vendors themselves have reached out to each other to establish unified partnership agreements to fill the holes in their proprietary systems. These partnership agreements tightly integrate by exchanging intelligence and making it easier for the network defender to orchestrate both products in tandem into their F2T2EA framework.

All of these innovations add up to mutual benefits for the network defender.

Complexity Reduction

The simple solution that has emerged for the math problem is that adopting a platform approach reduces the number of deployed products that network defenders have to manage from 10-15 down to a handful: the platform itself and the partners associated with the platform. But even with the partner products, they are so tightly integrated that they are much more easily managed compared to the old way of managing them separately as deployed best-of-breed solutions. This reduction in the number of independently deployed systems greatly simplifies the design, deployment and operation of the F2T2EA framework and greatly reduces the attack surface that cyber adversaries can leverage. For buy decisions in the cybersecurity world, always pick simplicity over complexity.

The simplicity that the security platform offers also has another benefit: more efficient utilization. Because the independently deployed point products are so hard to manage, it is likely that network defenders rarely get them fully configured to their maximum potential. With a single vendor solution, network defenders will be able to get closer to that maximum potential.

Completing the Last Mile Is More Efficient

Simplifying the orchestration of the last mile problem is no minor feature. It is the thing that drives the entire F2T2EA framework. Converting indicators of compromise into prevention controls is important, but deploying those new controls to existing systems is the gas that fuels the entire operation. Without an efficient way to do that, cyber adversaries will continue to run circles around their victim networks because the responsible network defenders will be unable to move fast enough to counter them. Automatic orchestration is the key to crossing the last mile with any speed.

Potential Buying Leverage for a Single Vendor Solution

Choosing a single vendor with strong partner ties is counter to everything the network defender has been doing for the past 20 years. But once that decision is made, organizations can leverage that decision to simplify the buying process. Organizations can now get their security staff off of the security vendor assessment treadmill. They no longer have to assess a class of security products every two or three years. Since they have decided on a one-vendor approach, they have, by default, chosen that vendor as a trusted partner. Instead of buying new point products every three years, network defenders can look for longer contract times and get better deals. For example, if an organization commits to a specific platform vendor for five years, instead of three, sales people are willing to give substantial discounts for a guarantee of a long-term relationship. Further, since the relationship is now trusted, partners and resellers are willing to bend over backward to accommodate specific asks.

For example, a CISO of a very large American insurance company was able to negotiate a lease for the security platform's hardware. He did not want to own any of it because, in his company, capex was a drain on the financial statement. By leveraging his trusted partner status to get a lease of the equipment, his entire purchase became opex, which was much more acceptable. [6]

CONCLUSION

The cybersecurity community has gone through a massive evolution of best practices in a short amount of time. From the beginnings of internet business to today, we have moved quickly through the Defense-in-Depth model, the Cyber Kill Chain model, and manual orchestration of every security control down the Cyber Kill Chain. The community believes that the Cyber Kill Chain model is the right approach, but the current implementations of it leave a lot to be desired. It is not that the model is wrong. It is the way we have deployed it that causes the issues. Current implementations add complexity to an already complex environment, waste our network defender assets by having them on a continuous vendor assessment treadmill, and exponentially add difficulty to the task of crossing the last mile. The innovative solution that has emerged to solve these issues is the security platform. It effectively reduces complexity, reduces vendor assessments, and automatically crosses the last mile for the network defender. Essentially, it automates the orchestration of the Find, Fix, Track, Target, Engage and Assess (F2T2EA) framework that network defenders have adopted for their electronic environments. Change is required, but because

it is hard to veer away from standard best practices that have defined the network defender's career for the past 20 years, it may be prudent for the board to get involved in the conversation. The security platform from one vendor and associated, tightly integrated partners is a radically different approach from the common vendor-in-depth approach. Network defenders may eventually come around to it, but if board leadership would like to get there sooner, then it may want to get involved in the discussion.

THIS IS WHAT THE BOARD CAN DO

Change is hard. Even when almost everybody in the room agrees that a change is required, people resist it. It is tough for network defenders to go against best practices that have been defining their career for over 20 years, such as Defense-in-Depth or deploying best-of-breed point products down the Cyber Kill Chain. But a change in thinking is required here. The F2T2EA framework and the Cyber Kill Chain model provide absolutely the right theory for how organizations could regularly defeat cyber adversaries attacking their networks. But our first attempts at orchestrating those concepts in the real world have not really worked that well for most network defenders. In order to reduce the number of security tools deployed in your organization's networks, and to reduce the architectural complexity that makes it easier for hackers to leverage your organization's security weaknesses, as well as to redirect company resources away from an endless cycle of security vendor assessments, board members should have a serious conversation with their CIO/CSO/CTO about the benefits of adopting a security vendor platform in order to accomplish efficient orchestration. The network defenders in the organization may eventually come around to the idea, but if the board would like to expedite the process, its members may want to influence the decision from the top down.

SOURCES

[1] "Trends In Computer Virus Research," by Fred Cohen, VXHeaven, sponsored by ASP, 1991, Last Visited 26 August 2016.

http://vxheaven.org/lib/afc06.html

[2] "Defense-In-Depth Against Computer Viruses," by Fred Cohen, Computers and Security, Volume 11, Issue 6, pp. 563-579, ISSN 0167-4048, October 1992, Last Visited 26 August 2016.

http://vxheaven.org/lib/afc12.html

[3] "Find, Fix, Track, Target, Engage – Compressing the Kill Chain," by MILITARY TECHNOLOGY, 28 August 2013, Last Visited 26 August 2016.

[4] E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113–125; URL

[5] "Complexity the Worst Enemy of Security," Bruce Schneier interview by Chee-Sing Chan, Computerworld Hong Kong, 17 December 2012, Last Visited 28 August 2016.

https://www.schneier.com/news/archives/2012/12/complexity_the_worst.html

[6] Phone conversation between the CISO of a large American insurance company and Rick Howard, 29 August 2016.

[7] "The Grand Strategy of the Roman Empire from the First Century AD to the Third," by Edward N. Luttwak, published by Johns Hopkins University Press, 1976.

https://www.goodreads.com/book/show/1726901.The_Grand_Strategy_of_the_Roman_Empire

[8] "NRC: Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979."

https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appr.html

[9] "Cyber Kill Chain," by Lockheed Martin, Last Visited 17 March 2017.

http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

REFERENCES

"A Military Guide to Terrorism in the Twenty-First Century," by United States Army Training and Doctrine Command, August 2007, Last Visited 26 August 2016.

"Building A System For Insider Security" by F. Duran, S. H. Conrad, G. N. Conrad, D. P. Duggan, and E. B. Held, IEEE Security & Privacy, 7(6):30–38, 2009, Last Visited 26 August 2016.

http://ieeexplore.ieee.org/document/5235135/authors

"Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities (Abbreviated Version)," by the National Research Council, 2007, Last Visited 26 August 2016.

"Defending Against the Unknown: Antiterrorism and the Terrorist Planning Cycle." by "LTC Ashton Hayes, The Guardian, 10(1):32–36, 2008, Last Visited 26 August 2016.

"Defense-In-Depth Against Computer Viruses," by Fred Cohen, Computers and Security, Volume 11, Issue 6, pp. 563-579, ISSN 0167-4048, October 1992, Last Visited 26 August 2016.

http://vxheaven.org/lib/afc12.html

"Exploring Security Countermeasures along the Attack Sequence," by "T. Sakuraba, S. Domyo, Bin-Hui Chou, and K. Sakurai, Proc. Int. Conf. Information Security and Assurance ISA, pages 427–432, 2008, Last Visited 26 August 2016.

http://ieeexplore.ieee.org/document/4511605/

"Find, Fix, Track, Target, Engage, Assess," by John A. Tirpak. Air Force Magazine, 83:24–29, 2000., Last Visited 26 August 2016.

"Joint Targeting," Joint Publication 3-60, U.S. Department of Defense, April 2007, Last Visited 26 August 2016.

"Overcoming the insider: reducing employee computer crime through Situational Crime Prevention," by Robert Willison and Mikko Siponen, Communications of the ACM, 52(9):133–137,. 2009, Last Visited 26.

http://doi.acm.org/10.1145/1562164.1562198

"The Advanced Persistent Threat," M-Trends, Mandiant, January 2010, Last Visited 26 August 2016.

"Trends In Computer Virus Research," by Fred Cohen, VXHeaven, sponsored by ASP, 1991, Last Visited 2 6 August 2016.

http://vxheaven.org/lib/afc06.html

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com