WHITE PAPER

A New Approach To Security Operations: Inverting The Investigation Workflow

By Joshua Goldfarb, Chief Product Officer – IDRRA
& Matt Cauthorn, VP Security – ExtraHop Networks

Flipping The Alert Funnel and Inverting The Investigation Workflow

To gain greater visibility, eliminate alert fatigue, and reduce dwell time of threats in the network, security programs need a new approach to gathering data and conducting investigations.

In this white paper, we propose a new, inverted workflow that focuses on monitoring and protecting critical assets first, and conducting analytics much sooner in the process to drive down dwell time and prevent attackers from harming the business.

TABLE OF CONTENTS

Introduction

In many aspects of life, people introduce efficiencies by prioritizing from the beginning. Let's take a look at two different approaches to car buying as an illustrative example.

In the first approach, we narrow the field of possible cars before we visit a single showroom. We look at factors like price, fuel efficiency, size, reliability, and many others that allow us to home in on a few potential models that suit our needs. After that, we invest time in vetting and qualifying the research we've done and explore which of the remaining candidates best meets our needs.

In the second approach, we begin by test driving 500 cars. Only afterwards do we consider which of those 500 best suit our needs and set out to research which would be the best choice for us. Of course, as you have realized, this second approach is not very efficient and does not make very good use of time at all.

While it is easy for most of us to see how up front prioritization aids in the car buying process, it is more difficult for many organizations to understand how it can help them optimize how they use their security resources and greatly improve their security postures. For security, the ability to see all the necessary data and conduct analysis sooner rather than later is a prerequisite for taking a more effective approach.

State of Affairs

For anyone who has worked in security for any length of time, they would likely agree that the current state of affairs is far from optimal.

The field of information security has evolved and matured quite a bit over the years. This, together with other historical reasons, has led to the less than strategic acquisition and deployment of security technologies. Often, specific technologies were acquired to fill certain tactical gaps without giving thought to how they fit into the bigger, strategic picture. Over time, this has resulted in a maze of different technological silos that struggle to share information and integrate with one another. Security professionals are left with no choice but to spend valuable time fighting their tools, rather than working together with them.

In parallel, alerting content and logic have typically been developed in a tactical manner as well. New technologies that were deployed often came with specific signature sets or alert logic of their own. Major vulnerabilities, malware epidemics, or other notable industry events often came with and left behind specific detection techniques. With time, additional signature sets or alert logic were developed internally or leveraged from external sources as well. The end result of all of this is a cannon of alerts that relentlessly unleashes its noisy, low fidelity wrath on organizations day in and day out.

As you can imagine, adding a shortage of skilled security professionals to the less than ideal scenario described above doesn't help matters. In the best of scenarios, with appropriate staffing and with technology and workflow optimized and efficient, it would still be difficult for organizations to stay on top of things. But with siloed technology, alert fatigue, and a skill shortage? It's hard to be an optimist.

The Problem of Dwell Time

Thus we can understand why so many intrusions fly under the radar and remain undetected for so long. This dwell time, as it's known, provides cover for attackers as they discover and pilfer sensitive, confidential, and proprietary data from organizations. Attackers take advantage of the current noise level and difficulty with prioritization that organizations experience. They leverage this confusion to hide in the noise and move around through the organization as necessary to capture the data they're after.

Discussing dwell time is uncomfortable because it casts light on the failings of current security approaches. Now, more than ever, this discussion is absolutely necessary. Given this state of affairs, what can organizations do to regain control of their security operations, reduce risk, and improve their security postures? They need to flip the funnel.

What Does It Mean To Flip The Funnel?

Returning briefly to the car buying thought exercise above, it is quite easy to see that the first approach is far more efficient and effective than the second approach. The concept holds true in the security realm as well. Let's take a closer look at what it takes for organizations to flip the funnel.

The first step involved in flipping the funnel is to prioritize risks and threats to the organization. First and foremost, this step necessitates a thorough understanding of the business, what is important to it, and what would cause grave damage to it. Prioritizing risks and threats typically involves understanding the concerns of executives, the board, leaders on the business side, customers, partners, and other key stakeholders.

This step presents the security team with a number of unique opportunities. If relationships with key stakeholders aren't yet in place or could stand to be improved, this provides a great opportunity to begin that important work. The inputs from these stakeholders, together with internal team and external industry knowledge, expertise, and intelligence form the basis for enumerating the risks and threats to the organization. Once these have been enumerated, the security team can work together with stakeholders to determine the potential for damage or loss to the business that each one presents. Based on these calculations, the list of risks and threats can be prioritized.

As a next step, critical assets will need to be identified, inventoried, and prioritized as well. Each risk and threat will map to a certain number of associated assets. If the priority of the risk is high enough and has the potential to cause enough damage to the business, the assets associated with it become critical assets. Where this line is, exactly, will vary from organization to organization, depending on their particular business and appetite for risk. It is important, however, to make these calculations based on data and knowledge, rather than assumptions and guesswork.

> "We want to make sure that we don't get distracted by tools or approaches that don't serve our strategic goals and cause us to wander."
>
> ***Joshua Goldfarb***
> ***Chief Product Officer, IDRRA***

Beyond just prioritizing critical assets, the organization will next need to prioritize where critical data resides. It's easy to understand why this is an important step in the process. Because hackers most often target the sensitive, confidential, and priority data that organizations possess, many information security risks and threats translate directly to the loss of that data. The means by which attackers get to this data varies, which affects the way we write alert logic. This will be discussed in a bit. But we need to complete these important steps before we can even think about generating a single alert.

Once we have prioritized risks and threats, critical assets, and critical data, there is another important step in the process that we must focus on before we can turn our attention to alerting and the work queue. All the prioritization in the world will do us no good if we don't have concrete data to apply it to. Or to put it another way, visibility is king. I can only monitor that which I can see.

In most organizations, visibility typically involves collecting telemetry data and alert data from network, applications, databases, endpoint, mobile, cloud, and other sources. As you can imagine, if an attacker is performing an attack in an area of the network, within a particular application, or inside a database that I am blind to, I'll miss it entirely. No matter how well I've prioritized or how good my alert logic is.

If I've completed the above steps, only now has the time come to think about alerts. Conceptually, what we want to do here is fairly straightforward. We want to write targeted, precise, incisive alert logic to identify activity inside our organization matching activity indicative of the risks and threats we've prioritized. What we don't want to do is stray from this focused approach. Of course, we want to make sure we leverage all of the tools and approaches at our disposal, whether they be hardware, software, signature sets, detection techniques, intelligence, or otherwise, to accomplish our goals. We want to make sure, however, that we don't get distracted by tools or approaches that don't serve our strategic goals and cause us to wander. This has the potential to re-introduce a tremendous amount of noise and inefficiency into our workflow, which can quickly negate the gains we've made by flipping the funnel.

In practice, this content development process typically involves quite a bit of research, experimenting, and tuning. The right logic needs to be developed, applied to the correct telemetry data, and within the right tools that allow for the necessary flexibility and granularity in logic. The investment in time is well worth it, precisely because of the previous steps we've taken. Content we successfully develop generates reliable, high fidelity alerts that map directly to mitigating risks and threats to critical assets and data we've already determined we're concerned about.

If that all sounds pretty refreshing, we're not done just yet. Before we send these alerts to the work queue, we need to build the narrative around them and prioritize them. Building the narrative involves filling in essential contextual information around the raw alert. Think of it like a 500 piece puzzle. Looking at just one piece of the puzzle (a raw alert) makes it difficult to see the big picture - what is really going on. Looking at even 200 of the 500 pieces, however, provides a completely different experience. So it goes with alerts as well. The more puzzle pieces that can be assembled around the raw alert before the analyst sets eyes upon it, the more quickly that analyst can vet, qualify, and investigate the alert. This leads to reaching an educated, informed decision on what, if any, action is required in far less time, freeing up resources for the endless list of tasks that awaits most security organizations.

Once the raw alert has been enriched with important, contextual information, the prioritization happens. Each organization will calculate priority based on its particularly sensitivity to risk and business needs. But at a high level, this process involves a calculation based on the intersection of the risk priority based on potential damage to the business, the criticality of the asset, and the criticality of the data. Executing these calculations and prioritizations at scale may require the assistance of machine-learning systems, which are rapidly growing more effective and ubiquitous, but have not reached full adoption yet.

Only now do we send alerts to the work queue. This is the last step in the process, rather than the first as we are accustomed to. The content we do send to the work queue has been strategically designed, enriched with important contextual information, and prioritized for us ahead of time before we ever set eyes on it. This is quite a change from the tactically-driven process that dominates the current state of affairs and results in the alert fatigue most organizations deal with on a day-to-day basis. The end result is that will we have far fewer alerts, and those alerts that we do send to the alert queue will tell a far more detailed version of the story than the standard-issue, context-less alerts we're used to working with.

As an added benefit, by flipping the funnel, we gain a tremendous advantage in communicating the value we provide to our stakeholders. Since all of our efforts tie back to our stakeholders' business priorities, it is much more straightforward for us to generate metrics around how we are progressing against our goals and how we are protecting their business assets. This may sound like something that is trivial or obvious, but in the current security state of affairs, it is, unfortunately, something that cannot be taken for granted.

Living Inside the Flipped Funnel

So now that you know all about flipping the funnel, what does it take to live it? First and foremost, flipping the funnel is a state of mind. The value and success of any security organization is directly correlated with the quality of its security operations function. And that quality is directly correlated to the efficiency and value of the security operations workflow. To flip the funnel, we need to go through the process enumerated above and get our security workflow working for us, rather than the other way around. Once that is done, we need to ensure that we keep abreast of changing risks and threats and critical assets and data so we can improve and evolve our workflow continually.

Inside the flipped funnel, we forego the need to open and close a certain number of tickets each day, to generate hundreds of thousands of alerts that no one will ever look at, and to blindly implement signature sets and detection techniques someone told us were worth implementing. We turn our focus from quality to quantity. We move from thinking tactically and playing whack-a-mole to thinking strategically and mitigating risk. We seek visibility across the enterprise. We evolve from siloed technologies fighting each other to integrated technologies working together to help us achieve our goals.

Technology Required to Flip The Funnel

We've dedicated much of this paper to the process of flipping the funnel. But as we know, solving any problem in security requires a mix of people, process, and technology. So what technology is required to flip the funnel?

Any discussion of technology around flipping the funnel generally begins with visibility. The discussion of the process above highlights the centrality within it that visibility plays. While visibility across the network, applications, databases, endpoint, mobile, cloud, and other sources is important, it can be difficult for organizations to cover so many bases all at one time. Further, data sources that reside on assets (e.g., endpoint protection platforms) are subject to tampering by attackers that manage to gain control of those assets.

It is for these reasons that organizations typically begin by looking to gain network visibility around the enterprise. Network telemetry products have come a long way in recent years and in addition to their traditional capabilities, can now discover and prioritize assets, identify and parse database and application transactions, and monitor traffic to and from Internet of Things (IoT) devices, among other things. Thus, by strategically planting a few network security appliances around the enterprise, an organization can cover many of its needs around flipping the funnel with a relatively small amount of technology. In addition to providing much needed visibility, this approach reduces both complexity and cost.

During the daily security operations rhythm, a whole host of questions need to be asked continually, among them: What traffic is transiting the network? What is entering and leaving my enterprise? How can I identify malicious activity? Where are my gateways? What assets are on the network? Which are the most critical? Where does data reside around my enterprise? What data are the most critical? What applications do those data reside in? How can I monitor those applications for misuse?

In addition to enabling organizations to flip the funnel, any technology also needs to integrate with the rest of the security ecosystem. As discussed above, organizations don't have time to fight their security technology - they need it to work collaboratively with them. Therefore, any technology that is going to enable and facilitate flipping the funnel needs to drop seamlessly into the security architecture.

Conclusion

Security operations doesn't have to be a constant struggle. Security organizations needn't find themselves suffering from lack of visibility, alert fatigue, and without the ability to properly prioritize their security workflow. Although flipping the funnel requires moving out of our comfort zone, changing the way we think, approaching security operations differently, and a bit of an up front investment in time, it pays huge dividends. It's hard to imagine another way in which organizations can truly come to terms with the volume of data and evolving threat landscape we currently find ourselves inundated with.

ABOUT EXTRAHOP

ExtraHop makes real-time data-driven IT operations possible. By harnessing the power of wire data in real time, network, application, security, and business teams make faster, more accurate decisions that optimize performance and minimize risk. Hundreds of organizations, including Fortune 500 companies such as Sony, Lockheed Martin, Microsoft, Adobe, and Google, start with ExtraHop to discover, observe, analyze, and intelligently act on all data in flight on-premises and in the cloud.

ExtraHop Networks, Inc.
520 Pike Street, Suite 1700
Seattle, WA 98101 USA

www.extrahop.com
info@extrahop.com
T 877-333-9872
F 206-274-6393

Customer Support support@extrahop.com
877-333-9872 (US)
+44 (0)845 5199150 (EMEA)