WHITEPAPER

Cybersecurity Intelligence in Today's Advanced Environment

SECURITY ON-DEMAND

Security Use Case: When Normal is Dangerous

It is generally accepted in the information security community that a good way to identify threats is to look for "anomalous behavior". That's all well and good, but we have recently discovered that seemingly normal behavior has led to successful security breaches and massive data loss for many companies out there. How do you know what to look for? How does one actually pinpoint potentially dangerous activity in your systems, even if it appears normal? I'd like to share some interesting findings from a recent beta testing scenario while preparing for the next release of our security monitoring solution.

What We Found

During recent beta testing of our Advanced Threat & Log Analysis Service (ATLAS), we discovered several of our customers who had VoIP systems manufactured by the same company in China were at particularly vulnerable and subject to significant attack risk. Our new technology allows us to monitor and detect outbound anomalous traffic across well-known ports. In this case we were monitoring outbound connections over port 21 or 22 that were assumed "safe". While engaged, we observed Port 22 (SSH) traffic going out to China. This immediately go our attention because we identified several different companies communicating to the same IP address. Upon further investigation, we also noted that these companies all had the same VOIP-based phone systems that were built by the same manufacturer in China. The phone manufacturer had installed a secret "back door" into the computer system, which allowed unauthorized remote entry into the system.

Impact

If this customer had been set up to allow all traffic outbound (which is quite prevalent in many customer environments), the backdoor would have allowed this unauthorized access and potential for being a "landing pad" for further surveillance, and data breach. To make matters worse, the phone system manufacturer required the phone system have domain admin account credentials in order to function, so essentially, the Chinese company had full domain admin rights to the network.

With the powerful new features of our service, we are able to define baselines for normal traffic that are behavior based. We knew it was not normal for this customer to be sending traffic to China. Because of our service, this potentially major vulnerability was identified and corrected before critical data was compromised.

It has long been known that certain manufacturers have been building in backdoors on their products. This presents a challenge to any company using these products because the traffic patterns will not be easily detected by conventional SEIM technology. Using current approaches, the customer would see this phone system communications as "normal" and was assume that this was trusted communications. These types of security incidents and many other newer kinds of attacks (APT's, and Zero-Day threats) can more easily be detected through a new class of technology capabilities, known as Security Analytics.

###

Understanding The 8 Keys To Security Success

We work every day to manage risk and ensure the security of our organizations. We strive to create an environment where business can be transacted seamlessly, conveniently and securely. We are charged with enabling business to continue while accomplishing our ultimate responsibility of protecting the business. The threats coming at us are complex, advanced and hard to detect. We know that we can do everything the right and still fall victim. This is why the keys to security success are focused on not only doing the right things to protect our organizations, but also being ready for the worst. Security success no longer means preventing a breach. It now means achieving a balance between prevention, compliance, threat management and preparation.

As Steven Covey said, "Begin with the end in mind." Starting this journey with a clear picture of what you want to accomplish helps pave the way for a smooth journey. From decades of helping organizations achieve security success, we have come up with this list of eight things organizations should be doing in order to achieve security success.

1. **Have a coordinated operational and technical capability approach to prevention, detection and remediation of events and incidents.** This sounds easy, but it requires buy-in and participation across the organization. Business and data owners must take ownership and responsibility for the security of data under their purview. This often means getting non-security personnel involved in security conversations. End users must be educated in the company's security practices and policies. The security and network teams must work together to ensure a robust and well-protected infrastructure. The security team must have the proper tools to enable detection of events and incidents and there must be a documented and tested incident response plan ready to go. The executive suite must be continually informed and ready to uphold the incident response policy; and to address shareholders, customers and the media in the event of a breach. The key here is planning, preparation and practice.

2. **Have a centralized, systematic (technological or otherwise) way of sharing knowledge related to threats and incidents.** Information regarding current and imminent threats and incidents is extremely valuable. This information could be used to help prevent attacks from spreading across an enterprise. Unfortunately, many organizations struggle to find ways to efficiently share information across disparate business units. Information silos prevent effective notification of emerging threats and attackers use this to their advantage. Leveraging a managed security services provider that delivers a master portal with a roll up view of the entire enterprise, along with business-unit sub-portals can help organizations ensure that everyone has the information they need as quickly as possible.

3. **Stay ahead of threats with continuous configuration management and analysis.** Your technology is only as good as its

Understanding The 8 Keys To Security Success

configuration. This also requires highly trained specialists who are skilled in the use of a particular technology.

4. **Deploy the right security technology.** Technology is the tools used by your people to enable your processes. Without the people and the process in place, the technology will never be fully utilized. Take the time to evaluate what you have. Are you using every tool in your arsenal to its fullest potential? Are you taking advantage of all the features? If you determine that you do need new technology, take great care in selecting it. What solutions are available to you? Are there alternative solutions that don't require technology? What skills and training would your team need? How does this new technology fit with your organization's plan and capabilities? Do you need another point solution? With traditional approaches becoming less effective, the addition of behavioral analytics greatly improves an organization's detection capability and compliments the security technology investments already made.

5. **Keep Systems Running Efficiently and Beat Alert Fatigue with a Managed Solution.** You can't solve security problems with technology alone. You must have someone keeping up with patches and updates to ensure it is functioning as required. Organizations struggle to keep up with the vast quantities of alarms and alerts that most technologies generate.. According to a recent Ponemon study, it costs organizations an average of $1.27 million annually to investigate and respond to erroneous malware alerts alone. Managed security services are a great option to help one operationalize the maintenance of systems and streamline alert triage. As threats have become more targeted and sophisticated, so have the technology solutions. These new technologies can be complicated and confusing. In order to ensure they are doing the job they are intended to do, they must be constantly monitored and maintained by trained specialists.

6. **Respond to threats in a timely, and consistent manner.** They key here is to be able to identify those threats quickly and be prepared with a response plan. Leveraging advanced tools such as behavioral analytics is one way to get ahead of the curve. Having the ability to constantly monitor network, user and application behavior and quickly identify behavior that falls outside of the norm is the advantage organizations need. Finding these compromises early and being able to respond and minimize impact is truly what security success is all about.

7. **Employ a consistent approach to the handling of incidents and threats from identification through closure.** With the huge volume of attacks against an organization, it would be easy to get bogged down in dealing with these incidents. Organizations who have a well-developed and thoughtful approach to working through these incidents have an advantage. Having a trusted partner that can provide you with actionable intelligence to

Understanding The 8 Keys To Security Success

go along with each incident requiring your attention helps maximize the efficacy of your team and dramatically improves your ability to respond and contain incidents.

8. **Apply metrics around the efficiency of information security technologies, processes and people.**

By starting off with a goal in mind, you can identify the key metrics you will track to ensure your journey to success is on the right path. Having access to the reporting and data needed to understand what is working and what needs improvement will help you make educated decisions on what to change, improve or do more of. Organizations that continually track key metrics are far more likely to achieve security success.

###

What Exactly are Behavioral Analytics?

Behavioral analytics is a term being tossed around the cybersecurity world in the last couple of years. So what are they? Well, traditionally, behavioral analytics are analytics that businesses use that focus on consumer trends, patterns, and activities. Humans are typically creatures of habit and our use of the Internet is no different. Through developing and deploying analytics that baseline an individual's behaviors and trends, companies are able to personalize marketing efforts, improve the customer experience, and even alter product offerings to suit a customer's particular tastes. However, behavioral analytics don't need to be limited to just analyzing customer behaviors. In fact applying them to cybersecurity can determine the difference between a major breach and warding off an attack.

A big mistake organizations tend to make is limiting cybersecurity behavioral analytics use to only focusing on their employees. Because behavior is often associated with human activity, it is easy for companies to simply focus on user actions to identify insider threats or compromised credentials by establishing a baseline of user activity and looking for anomalies. However, behavioral analytics have so much more potential in the cybersecurity space.

The fix? Applying Behavioral Analytics to Not One, But Three Areas

In a corporate enterprise, we typically have three domains that need to be monitored: the network, the users, and the assets. Applying behavioral analytics to each of these individually is valuable to help us understand and baseline normal behaviors. For example, a typical asset on the network is designed and structured to carry out particular functions. Through behavioral analytics we can develop an understanding of how frequently certain processes and applications on a device are used, who accesses the asset and how often, what other devices the asset communicates with, and so on. Once the baseline is established, we can now alert on statistical anomalies and investigate why such events may happen. As these events are investigated such learning can be turned around back into the system and our monitoring gets smarter. In many instances, we are able to identify malicious activity on the asset and remediate the event.

More Data Leads to More Questions

However, even that example alone leaves us with a lot of questions. How did the anomalous event occur in the first place? Was there a user who initiated it? Were other devices also infected or accessed? And so on. Not only that, but there is still a chance that we have a false positive. Perhaps the anomalous behavior on the asset looked malicious but was really benign (or vice versa). Focusing only on asset activity or monitoring and analyzing events in a silo limits the context and prevents event correlation.

The Solution: Data Correlation

To maximize the use of behavioral analytics in security operations, we have to look at behaviors of all three domains AND marry them together. Correlating behaviors enable us to get the whole picture of what is occurring in the enterprise and to identify truly anomalous activity. In a data breach scenario, it allows us to understand how many and

What Exactly are Behavioral Analytics?

which specific devices were compromised, how the attacker got in, what data may have been taken from the network, how long the hacker was on the network, and what exactly needs to be cleaned.

Sifting Data: Finding Threats in Piles

To further automate and optimize our analytics it is important to employ both supervised and unsupervised learning. Supervised learning is generally how behavioral analytics work. In these cases, the analytic is coded to look at specific types of data, baseline that data, and look for anomalies outside of the norm. Going back to our asset example, if we want an asset to identify behavioral anomalies on how much data is normally transferred to and from the system in a given day, the analytic is coded to read that specific data. It baselines the normal range and then alerts when that norm range is exceeded.

However, more valuable, yet more complicated, is unsupervised learning. According to "Machine Learning Mastery": "The goal for unsupervised learning is to model the underlying structure or distribution in the data in order to learn more about the data. These [models] are called unsupervised learning because unlike supervised learning above there are no correct answers and there is no teacher. Algorithms are left to their own devices to discover and present the interesting structure in the data."

Algorithms: The Parent of Unsupervised Learning and Advanced Behavioral Analytics

Simply stated, an algorithm is released among the data and it learns. It looks at all the data, establishes baselines, and then looks for anomalies. To paraphrase Forrest Gump, "it's like a box of chocolates, you never know what you are going to get." Unsupervised analytics add considerable to value to security operations because it largely automates the hunting process and helps us discover those "unknown unknowns". However, they also require patience and understanding and, like anything worthwhile, they take some time to learn. Many of the anomalies discovered may be innocuous and outside the scope of security operations. That's ok. The intent is to find anomalies, with the expectation being that among those anomalies will be malicious activity that we would otherwise miss without them (the proverbial needle in the haystack). Once those malicious anomalies are discovered, we turn those into supervised behavioral analytics. Essentially, the unsupervised analytic becomes our discovery tool.

Simply applying one facet of behavioral analytics isn't enough. There are too many variables and too many threats. The true definition of behavioral analytics must be the application of it to the three levels – asset, user, and network – to find threats quickly, thoroughly, and before they have the chance to do any damage.

###

3 Reasons Why Hackers Love Universities and State Governments

If you've followed data breaches over the years you will notice that no industry is safe – which is no secret to anyone. But what may be surprising is the amount of Universities and local governments (including States) are targeted by hackers.

Perceived of Lack of Security

Being either government or non-profit (in the case of private universities), funding and spending can be a trial. There is a common belief – whether true or not – that security teams in state and local governments and universities are underfunded and therefore the organization is unsecure. So hackers, as opportunists, often view these organizations as low hanging fruit. However, this alone is not reason enough for hackers to go after it, there needs to be something of value.

Useful as Attack Launch Point and Command and Control

Hackers often take advantage of "low hanging fruit" in order to set up an attack infrastructure that can be used to obfuscate where the attack is coming from. It is not in the hackers' interest to launch attacks against a particular organization directly from one's own computer and terminal as the attack can be easily traced back.

Universities, in particular, are very popular locations to use as the attack hop points, as well as command and control (C2) nodes and data exfiltration points. This is because there are often wide-open segments on the network that generate a large amount of traffic. For example, a DNS server at a University library on the student network typically produce very large amounts of data during a normal day. Installing command and control tools and gaining remote access on such devices are less likely to be noticed than if they were installed and operating on a quieter device.

On top of that, many networks at colleges such as those that serve the student dorms have decreased security restrictions for ease of use by the students. On such networks it is not uncommon to see large amounts of torrent, file sharing, and TOR activity, for example. Thus hackers can also use such services for their purposes and the security administrators may be none-the-wiser.

We also see similar activity in state and local governments, though perhaps to a bit lesser extent. However, any network that processes a large amount of internet traffic, such as the DMV, are often targeted and used in the same manner.

Valuable Information to Steal

Hackers do not only go after these organizations because they are useful as part of their attack infrastructure. Universities and governments also have valuable information that can be stolen. Colleges and Universities are obviously targets for such information, particularly those that perform a large amount of cutting-edge research.

APT's generally have two primary motivations: espionage and intellectual-property theft. Universities have valuable information that suit both of those classifications. Why develop your own technology when you can just steal it? That

3 Reasons Why Hackers Love Universities and State Governments

seems to be the mantra of APT hackers.

Governments and colleges have useful personal information (PII) on residents and students and maintain legal, driving, health and other records that can be used for any number of purposes ranging from identity theft to blackmail.

Finally, as exemplified by the controversy of Russian meddling in the 2016 Presidential elections, there is significant opportunity for hackers to influence or throw into doubt America's electoral processes and results. Each state is responsible for conducting elections on their own terms, rules, and security. Often this trickles down to the cities, towns, and villages who have even less money to sufficiently secure themselves.

Considering such circumstances it should come as no surprise that hackers love to exploit universities and governments. A veritable smorgasbord of value within questionably secured organizations.

At Security On-Demand, we have government and university customers who rely on us to help them prevent such exploitation. We regularly see hackers attempting to compromise these groups. We recommend that information security teams employ strong security monitoring, detection, and response services as well as harden the enterprise network through decreasing the attack surface, installing and properly configuring security devices, and segmenting the network to protect critical data.

###

More posts like these can be found on our blog, **Smarter Cybersecurity**. New posts from all aspects of the cybersecurity industry are available weekly.

securityondemand.com/blog