CHAPTER 7

Security Intelligence and Next Steps

INFORMATION IN THIS CHAPTER:

OVERVIEW

In the previous chapters we provided an overview of the data and analysis steps of the security analytics process. In this chapter, we will explain how you develop security intelligence so that you may increase your security response posture. See Figure 7.1 for the security analytics process. The goal of this chapter is to provide you with the knowledge to apply what we have discussed in this book and to address the next steps to implementing security analytics in your organization.

SECURITY INTELLIGENCE

We want to develop security intelligence so that we can make accurate and timely decisions to respond to threats. Although security intelligence may seem like the newest buzzword people are using when talking about using security analytics,

Information Security Analytics. http://dx.doi.org/10.1016/B978-0-12-800207-0.00007-1

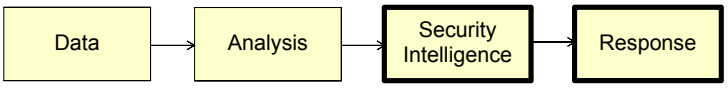

FIGURE 7.1
Security analytics process.

there is no clear definition of what exactly security intelligence entails. So, let us start with a discussion about the differences between information and intelligence. Information is raw data (think of it as your log files), whereas intelligence is analyzed and refined material (think of it as the result from looking through your log files and finding an anomaly). Intelligence provides you with the means to take action by aiding you in your decision-making and reducing your security risk. In other words, intelligence is processed information allowing you to address a threat. By generating security intelligence using the tools discussed in this book, you will be better prepared to respond to threats to your organization.

Basic Security Intelligence Analysis

Security intelligence is especially relevant because experts have found that companies failed to identify a security breach until a third party notified the companies, even though they had evidence of the intrusion in their log files. We all know that it is impossible to review every log file collected, but with security analytics, you will be able to set up your tools to help you to identify and prioritize security action items. While you still may be dealing with historical data, you are able to optimize your response time to incidents by quickly converting your raw data into security intelligence.

Once you have your security intelligence, you have two options: take action or take no action. You would think that the most obvious option is to take action to address your threat, but security intelligence is often tricky because things are not always as "clear-cut" as we would like them to be. Sometimes, your intelligence is the "smoking gun" identifying a security incident. For example, in the case where you find "two concurrent virtual private network (VPN) logins" or "two VPN logins from different parts of the country," you would probably call the employee and ask about the suspicious logins. In the best case scenario, the employee may have a completely legitimate reason for the logins from two different IP addresses. In the worst case scenario, the employee's credentials have been compromised. Either way, you will be able to quickly mitigate the potential threat (unauthorized access).

Other times, the intelligence you found is just an indicator of something bigger that you have not quite figured out yet. For example, the intelligence you identified may be an indicator of a hacker, who is in the reconnaissance phase, sending probing packets to your network ports to observe the response. More often

than not, it may just be an unexplained anomaly or a false positive for which you will find no answers. Such is the nature of working with intelligence—you never have complete visibility of the threat actors or their actions, but you still must do your best to protect your organization.

Security intelligence is oftentimes used for explanatory analysis (or retrospective analysis) to determine what happened during a security incident so that steps can be taken to mitigate a threat. Exploratory analysis is very valuable to increasing an organization's defenses. Yet, the ultimate goal with security intelligence is to be able to conduct predictive analysis: to guess what your attacker will do so that you can implement countermeasures to thwart your attacker. Predictive analysis may seem more relevant in a real-time incident, such as ongoing distributed denial of service (DDOS) or a live intrusion. However, it is also relevant for dealing with day-to-day situations: by knowing your environment and your operational baseline, you are able to identify your strengths and weaknesses, which will assist you in developing responsive strategies.

It is impossible to protect against every threat, so one way to address this is by knowing your organization's landscape and your intelligence gaps, which are the areas in which you lack information on your threats. By understanding your intelligence gaps, you will be able to focus your efforts to address these gaps and to set up early warning sensors. These sensors are usually a combination of tools to include vendor solutions (e.g., security information and event management) and the security analytics techniques discussed in this book.

Additionally, you will be able to address your internal security gaps. For example, suppose you know that your antivirus (AV) vendor's product is not as robust as you would like, but your budget does not allow you to purchase a better product. Knowing that this is one of your intelligence gaps, you may be more vigilant at reviewing your logs and at checking your quarantined e-mail. You may be also looking for information to cover this gap through other means (increasing security education or frequent system tests).

As you develop your organization's security intelligence, you will have a better understanding of your organization's threat landscape and you will develop greater confidence in your ability to respond to the threats. Once you start using security intelligence, your mind-set changes from "reacting to events" to "methodically addressing top threats." Our goal in this section is to have you start thinking about how security intelligence can increase your overall effectiveness and productivity. To cover all aspects of intelligence analysis in this section was not possible, but we hope to give you a basic understanding of how it works and how it can help you. If you are interested in learning more about this topic, you will find a resource by searching the Internet for "security intelligence analysis" or "intelligence analysis."

Business Extension of Security Analytics

There is no doubt that your organization already collects data for different business processes (marketing, accounting, operations, network management, etc.). However, most organizations conduct data analysis using standard analysis methods (i.e., spreadsheets) from their databases; therefore, they have yet to harness the power of analytics.

We provided you with the knowledge to conduct an analysis of your existing security data to extract intelligence for security decisions by using the powerful, open-source software tools to examine structured and unstructured data. If you expand this to all of your organization's businesses processes, you will be able to examine data in ways that you could never have imagined. You will be able to do this in real time to make proactive business decisions, instead of just using historical data to make reactive decisions. In fact, the real power of analytics is realized when you are able to take data across different departments to generate predictive security intelligence. The techniques we cover may also be applied to any of your organization's business processes—it is just a matter of expanding your skillset and applying the proper techniques to the right data set.

SECURITY BREACHES

As you start examining your data, it is inevitable that you will discover a security incident; thus, we would be remiss if we did not touch upon the steps to take when you have identified a security incident. If your organization has a preexisting security incident response policy in place, you would naturally follow those procedures. For those who do not have established policies or procedures, we encourage you to begin creating a plan to address the key phases of incident response: prepare, notify, analyze, mitigate, and recovery. As a starting point, there is a plethora of security policy samples that you can find by searching the Internet for "security policy templates" or for a specific type of security policy (information security, network security, mobile security, etc.).

Depending on the severity of the intrusion, you may want to consider hiring forensic and/or intrusion-response experts to assist you with a security breach investigation and to identify procedures to protect against future intrusions. You may also have legally mandated reporting requirements to federal or state authorities and/or risk management reporting requirements, which will depend on the type of data compromised (intellectual property, personal identifying information, etc.). In addition, you may need to seek legal counsel to determine if law enforcement reporting is necessary. We encourage you to develop these procedures now and to conduct "table-top" (e.g., dry run) exercises, so that in the event of an incident, you are able to quickly respond.

PRACTICAL APPLICATION

Insider Threat

When we look at security, we often focus on threats external to our organization, rather than internal to the organization, because the probability of a threat coming from the outside seems greater than one coming from the inside. However, while less likely to occur, an insider oftentimes causes more harm to a company than an external threat could because an insider knows how you operate and where your keep your valuable information. So, let us start by examining a scenario with an insider threat.

The owners of a small, start-up company found it strange when several of their programmers quit the company at the same time. When company executives "got wind" that the individuals had gone to work for a competitor, they began to ask questions about whether or not the company's intellectual property had been stolen, since these programmers were working on key pieces of their product. Since this was a small company, the management did not have a security officer, so they looked to the IT personnel to examine the problem and to look for evidence. The first area the IT personnel examined was the e-mail of the employees. Through the e-mail, they were able to piece together that the employees who left the company were collaborating and they intended to steal the code they developed at this company. These e-mails were key evidence that the company saved to an external storage device for preservation. The company made a secondary copy so that they could review the data.

Once the e-mails are preserved, rather than manually reading through the e-mails, you could use the text mining technique covered in this book to see if you can identify patterns that are not readily apparent, such as other associates involved in the source-code theft and when they initiated the plan to steal the code. You may also find other clues, which may cause you to expand your investigation. For example, the former employees in our scenario continued to correspond with current employees at the company even after they left the company. The company was able to identify the personal e-mail accounts of the former employees because they forwarded e-mail to themselves prior to quitting. From the e-mail accounts, the company was able to determine that they were still e-mailing current employees. One of the current employees, who had not left the company yet, was involved in the source-code theft and was still feeding the former employees with details about how the company knew of the theft and still providing insider information.

To expand upon this scenario, for the sake of showing you further applications, let us say you were able to determine that one of the former employee physically downloaded the source code onto a removable USB device on a particular date. What types of security data would law enforcement need from your organization? First, the system used to download the data would have important

evidence of the USB device connections, to include artifacts in the registry keys (link files, USB removable devices connected to the system, timeline information, etc.). Second, showing that the employee was physically present in the building would be beneficial to building your case. Other areas to examine would include employee access logs (building entry, parking entry, computer logins, etc.). If you are lucky enough to have physical access log data to your building, you could run security analytics on employee patterns to identify anomalies—which may or may not serve as an indicator of when the criminal activity began. While video surveillance data will provide you with additional evidence to support your case, current techniques in video analytics have not yet fully developed—robust tools that can handle large amounts of data from multiple video feeds and conduct facial recognition at a granular level are still being developed.

A final consideration in our insider threat scenario that we will discuss, which is often overlooked because companies do not expect it to occur, is an unauthorized access after the employee has resigned. Sometimes a company's IT department may not remove accesses to systems immediately, thereby offering a way for the employee to return to the company. Or, in the case where a former employee, who managed the IT network or was technically sophisticated, may leave a backdoor from which the employee may access the company's system. Why is it important to examine these areas? Besides the obvious point that it poses a threat to the organization, if you can show that the employee accessed the company's system while no longer employed, you are able to show another form of criminal activity—unauthorized access. An Internet search for "mitigating insider threats" will provide you with additional resources and ideas to better protect your organization.

Finally, you must also consider the situation in which an employee's credentials were stolen. Should you call the person and start asking questions or should you just report it to your management? This highlights the importance of having an incident response plan—it assists you in knowing what steps to take and when to involve your management. Depending on your organization's policy and management decisions, the next steps could include any of following: consult with legal counsel or human resources personnel, interview the employee, or notify your board of directors. Inaction is also action—your company may choose to do nothing, which tends to be common in smaller organizations. After determining if there was any wrongdoing by the employee, your management could also opt to pursue criminal enforcement and/or civil litigation.

Resource Justification

There is a great difference between telling your management that the number of security incidents is increasing and showing your management a simulation tool depicting intrusion attempts during a certain time period. In the former example, your management probably will not grasp the significance

of the threat or the impact to your organization. In the latter example, your management can see the rapid increase of attempts and better comprehend the scope of the threats. It is often the case where management cannot understand the impact of security incidents because it seems far removed from everyday business processes. Thus, they only seem concerned with security when an incident is identified because they expect you to protect the organization. Security analytics can help you to elevate your management's security awareness by providing you with ways to transform your data into easily understood security intelligence, thereby bringing security information up to their level of comprehension.

Security analytics can also support your justification for resources. By using the techniques covered in this book, you can support your claim for resources to support your security initiatives. For example, if you want to justify the need to purchase a new intrusion detection system, you can easily do so by first showing the statistics on the growth of the threats within your organization's network. This coupled with the identification of what the current system is not identifying (intelligence gaps) and a simulation of the effects from not identifying the threats translates your security concern into a business problem. Your management may be more inclined to pay for a system to support security, even when there are competing business interests, because you are able to show a compelling need. Most importantly, you are able to translate how this compelling need affects your organization's profits and/or productivity. You could also use this technique to justify hiring more security personnel and to change internal business practices and/or policies.

Risk Management

A big concern with the use of analytics is the collection and use of sensitive data. There is always the risk of inadvertently exposing sensitive data, no matter what policies are in place. We simply cannot be prepared for every type of security response because the threat of malicious attacks continues to increase unabated. Moreover, the trend for allowing "personal devices" to be used in the workplace (also known as Bring Your Own Device (BYOD)) creates an even more complex risk management situation because sensitive data can now reside on these devices. When you add the trend of sharing the analytics data with partners and suppliers to increase collaboration and innovation, the risks escalates even more because now the sensitive data reside outside of your organization.

The ability to collect large volumes of data containing sensitive personal, financial, or medical information places a greater social responsibility upon those using analytics. No matter where the data reside (in the cloud or within an organization), a security practitioner should be acutely aware of the risks associated with data reuse, sharing, and ownership. Therefore, you need to know the types of data you are handling, so you may take the appropriate steps to

safeguard the data through information management and organizational policies. Additionally, if you are working with other individuals handling the data, they should be trained on how to safeguard the data and the ethics of properly using the data.

One way to protect the data is to use data anonymizing tools prior to or after conducting analytics processes. You can do this by using the techniques provided in Chapter 5, through the use of a script, to convert the data of concern into anonymized data. In addition, once your organization determines the need to involve law enforcement or to pursue civil litigation, you may be given the responsibility to produce the evidence supporting the incident. Prior to disclosing the information, you should review the data for any sensitive information, such as personally identifiable information, financial data (i.e., credit cards and bank accounts), Health Insurance Portability and Accountability Act and Gramm–Leach–Bliley Act protected data, and intellectual property. Your legal counsel will be able to provide you with more details on other data needing special protection.

Challenges

We realize that there are many challenges to using security analytics, since the field is still evolving and people are still trying to figure out how to effectively implement the techniques in their organization. If you are reading this book, you probably are not considering using a vendor for your security analytics; therefore, you may be thinking of the logistics involved with implementing it within your organization.

Data

When it relates to data, you should consider two aspects: identifying the "right" data and normalizing the data. First, you will need to examine the security-related data collected within your organization. Most people think of network, mail, and firewall logs when you mention data collection for security; however, other peripheral log files (e.g., building access, telephone, and VPN logs) are also relevant. You will need to assess if the data you are collecting is relevant to achieving your goals as a security practitioner. If you are not collecting the "right" data, no matter what types of security analytics tools are used, you will not produce actionable intelligence.

One way to identify which logs are important for your organization is by looking at what is on your network that must be protected (your organization's "crown jewels") from the perspective of an attacker. For example, a bank's "crown jewels" would be the customer and bank financial data and a software company's "crown jewels" would be its source code. One way to access the "crown jewels" is through a back-office server, which is accessed by an employee's desktop computer via e-mail. Another way to access the "crown jewels" is through the

Web server in the demilitarized zone (DMZ), from which a database behind the firewall is accessed to get to the back-office server. Therefore, all of the processes related to accessing the "crown jewels" should be considered your critical log files. These log files should be collected and analyzed using security analytics.

Now that you have the "right" data, you need to normalize the data before transforming it into security intelligence. Normalization techniques are used to arrange the data into logical groupings and to minimize data redundancy. Conversely, it may be necessary to denormalize the data structure to enable faster querying, but the downside is that there will be data redundancies and loss in flexibility. To normalize or denormalize the data, you could use the Hadoop and MapReduce tools, but it would involve writing a program. An Internet search for normalization or denormalization techniques or programs will provide you with more in-depth information.

We stress in this book the need for you to use security analytics on your data so that you have an idea of your organization's baseline. For example, your baseline could include IP address logins via VPN from the Philippines because your company outsourced the development of a specific function to a company located there. This baseline could trigger you to conduct more monitoring of the VPN from the Philippines (because you feel this is a higher risk to your network) or it may allow you to direct your resources to other threat areas because you are confident that the logins pose a lower threat.

Integration of Equipment and Personnel

In implementing security analytics, it will be necessary to integrate a data warehouse into your existing architecture. This is no easy task, as there are many considerations in collecting data from various sources and integrating the data into a data warehouse using the extraction, transformation, and loading process. Designing a data warehouse is out of the scope for this book; however, we have listed a few questions to consider as a starting point.

- Will this data warehouse contain an SQL or a NoSQL database?
- Will the data reside in the cloud or on your organization's network?
- What are the risks involved with protecting the data?
- Do you have enough storage capacity?
- Do you have robust servers and how does the location of your data affect your server performance?
- What type of schema model (star, snowflake, etc.) will you use?

The security analytics tools will help you to generate security information, but you need the skilled personnel to interpret and transform the information into security intelligence. However, there is a critical shortage of cybersecurity practitioners and analytics professionals, and this trend is expected to continue for the foreseeable future. Even if you are working for a large organization with the

resources to hire security analytics personnel, it will be difficult to staff your team with experienced personnel. You will most likely have to train personnel to evolve into the security analytics roles.

False Positives

As you begin to use security analytics, you may notice high false-positive rates or that you are not seeing what you thought you would see. It may be necessary for you to adjust your strategy to accommodate your data. For example, let us say that you are looking at end-user domain name server (DNS) lookups to identify possible malicious activity of an attacker who has compromised your system. You are wanting to do this because you suspect there could be an advanced persistent threat in your network. Therefore, you are searching for evidence that DNS manipulation is being used to hide the IP addresses of remote servers or is being used as a covert channel for data exfiltration. The assumption in conducting this analysis is that an attacker would have a higher DNS lookup rate when compared to your average user's DNS lookup rate. You find that your initial analysis reveals a lot of false positives. If you shift your strategy by looking at second-level domains, removing internationalized domain names, or using a public suffix list (also known as effective top-level domain list), you may obtain better results.

You may also run into a situation where after adjusting your strategy, you still do not find any security incidents. It is at this time that you will need to view your results using a "different lens" to search for meaning in what you have already found. In going back to the DNS lookup scenario, perhaps even after you have shifted your strategy, you still cannot seem to find malicious DNS lookups. Let us look at what you have—a list of your organization's DNS lookups, which is baseline over a certain period of time. As we have stressed before, this information is very important in security—you must know your organization's baseline before you can detect anomalies. In addition, you have also identified the DNS lookups, so you could run these domain names against a domain watch list to check that there are no suspicious lookups. We want to stress that what may initially seem like a dead end, may actually be an opportunity—security intelligence of your organization or your threat landscape. Once you have figured out the security intelligence of importance to your organization, you can automate these tasks to assist you in protecting your organization. This is the beauty of security analytics.

CONCLUDING REMARKS

Our goal with this book was to demonstrate how security practitioners may use open-source technologies to implement security analytics in the workplace. We

are confident that you are already well on your way to developing your organization's security intelligence with the techniques we covered in this book. Most importantly, we encourage you to use security analytics to increase your organization's overall security, thereby reducing risks and security breaches. While you may initially find yourself using security analytics to do specific tasks (i.e., reduce enterprise costs and identify anomalies), as your sophistication with analytics grows, we believe you will see many more applications for the techniques. As you begin to implement security analytics in your organization, your efforts to increase security will become more apparent. Rather than using a traditional, reactive model of security, you will be implementing a proactive model of security. Specifically, security analytics should contribute to developing your security intelligence.

Learning the tools presented in this book is the starting point of your security analytics journey. We have given you several techniques to add to your tool kit, but we hope that you expand your knowledge. As analytics is a rapidly expanding field, you will, indeed, have no shortage of proprietary or open-source technologies to learn. In fact, open-source technologies may outpace proprietary software!

We challenge you to "think outside the box" and to look for ways to integrate security analytics solutions in your organization. The possibilities for applying the techniques are endless. More importantly, you will be providing your organization with value-added intelligence to answer questions it never knew could be answered using the data your organization already collects.

We are convinced that these security analytics tools are extremely effective. We also believe that if more organizations utilized these open-source tools, they would be better prepared to protect their organization by spotting an activity while it is occurring, rather than responding to an event after-the-fact. Good luck on your journey!