LEARNING MADE EASY

Securonix Special Edition

Security Analytics

for dummies®
A Wiley Brand

Discover security analytics fundamentals

Read key cyber and insider threat use cases

Learn steps for successful deployment

Brought to you by

SECURONIX
Security Analytics. Delivered.

Aaron Pritz

About Securonix

Securonix is redefining the next generation of cyber threat detection by using the power of machine learning and big data. Its purpose-built security analytics platform delivers real-time threat detection, threat hunting, and incident response capabilities on a single unified platform.

The Securonix security analytics platform has four key capabilities:

- Built on an open Hadoop stack, the solution provides unlimited scalability and data retention.
- Machine learning based analytics enables you to detect unknown and advanced cyber threats.
- Integration text-based search and threat hunting capabilities enable rapid investigation.
- Automated incident response and case management enable consistent and rapid response to incidents.

Securonix offers a visionary security analytics platform that's built for the next-generation of threat detection and response. The solution is priced by identity to provide consistent low pricing that doesn't increase exponentially with data. Learn more at **www.securonix.com**.

Security Analytics

Securonix Special Edition

by Aaron Pritz

for dummies®
A Wiley Brand

Security Analytics For Dummies®, Securonix Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-54513-2 (pbk); ISBN: 978-1-119-54514-9 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie A. Burchfield
Acquisitions Editor: Ashley Barth
Editorial Manager: Rev Mengle
Business Development Representative: Molly Daugherty
Production Editor: G. Vasanth Koilraj

Table of Contents

Introduction

Security operations centers and Security Information Event Management (SIEM) have represented a heavy investment from many companies as the SIEM technology has been the center of the security monitoring universe. At the 2015 RSA conference in San Francisco, Amit Yoran (then the president of RSA) stated, "The security industry is failing," and then he paused before delivering a knockout blow: "It has failed." Yoran's keynote address was aptly titled "Escaping Security's Dark Ages," and he extended the analogy saying, "We need to stop thinking of taller castle walls and deeper moats."

The part of the discussion that stuck with me the most was when he said that many security programs focus on aggregating numerous logs blindly and "implementing that glorious and increasingly useless money pit known as SIEM. He even cited the Verizon Data Breach report's assertion that less than 1 percent of successful advanced threat attacks were spotted using SIEM systems.

Over the next few years, a few key players in the market began shifting thinking from log aggregation and rule-based event monitoring to big data security analytics and user and entity behavior analytics (UEBA). While these capabilities haven't eliminated the concerns about the ability to efficiently respond to real threats and events, they've provided a new map to direct and address execution and critical resourcing issues that plague the industry. Many industries, including customer service, automation, and "bot" technology driven by artificial intelligence, have begun taking over basic interactions, answering questions, and handling tasks. The same concepts are being leveraged in security.

About This Book

This book is written with the expectation that anyone in your company should be able to read it, understand the content, and articulate the need for action around advanced cyber threats. Executives and board members are becoming more aware and eager to find better ways to enable security teams to detect

something happening to a company. Often, cybersecurity books go into significant technical depth, which is great for IT and security professionals, but little material is available for everyone else. This book helps you discover the basics about security analytics and be more conversational at parties — just in case you're ever at a party where information security talk is cool. (If you find this scenario, please forward me the invite!)

Icons Used in This Book


REMEMBER

Similar to trying to act on billions of security logs, you have to identify what's most important. Unless you have a photographic memory or a machine learning brain, pay attention to these points.


TECHNICAL STUFF

These nuggets are great pieces of technical information that the average reader doesn't need to know but may find interesting.


TIP

For time- or frustration-saving ideas, pay attention to these tips. There are plenty of ways in cybersecurity where you can get tripped up and make something more complicated than it needs to be. These tips help you focus on what matters and be effective in your efforts.


WARNING

Warning icons are for serious situations, where the reader can cause personal harm or harm to his or her work. These are things that can keep you out of trouble or help you avoid mistakes others have made in the security analytics space.

Beyond the Book

This book gives you an orientation to security analytics and the key things to know to help transform your cybersecurity program, but there's only so much that can be covered in a book this size. If you want to learn more about Next-Gen SIEM and security analytics, check out `www.securonix.com`.

IN THIS CHAPTER

- Looking at evolving security operations and detection tactics
- Defining security analytics
- Crafting your business case for security analytics
- Working on your strategy for security analytics

Chapter 1
Making the Business Case for Security Analytics

Information security and cybersecurity have always been about protecting companies, people, information, and assets. However, as technology has changed and the world has become more and more digitally integrated, the cyber risks have become more pervasive. To combat this, many companies are focusing their efforts and limited resources on monitoring and detecting security events or signals of early compromise. Monitoring technology isn't new, but it's starting to rapidly evolve.

Security Information and Event Management (SIEM) has a long and rocky history with many companies as they've realized some of the complexities and challenges of integrating logs and data across their organization and are able to respond to all flagged security events. Companies continue to implement these technologies for many reasons, including compliance monitoring, threat monitoring, log collection and retention, detecting hygiene issues, and incident management, but regardless of why, detecting actionable security threats is desired, as companies seek to reduce their risk profile.

In this chapter, you explore a bit of the past and present of security operations, how the world is evolving in the cyber event detection game, and how you can formulate a business case for and strategy around security analytics.

Security Operations: Past and Present

The IT landscape has evolved. Computing has shifted from highly centralized mainframe environments (large computers that handled all the processing within the server) in the 70s and 80s, to semi-decentralized with client-server applications (where computing power happened both on the PC and on an application server). In the 90s, perimeter/data center-based security approaches were the dominant approach. This was often referred to with an analogy of a "hard candy shell with a soft center." The focus was only on the perimeter, and security was lax inside. Today, while elements of these historical approaches can still be found within companies, much of computing has shifted to cloud-based systems and mobile devices such as smartphones and tablets.

Information security has struggled to lead or even keep pace with some of these shifts. While device, application, and infrastructure log collection and security event detection somewhat worked for mature organizations, security teams struggled with the volume and complexity to get to the right scale. Additionally, it was difficult to keep pace with attackers' new methods of penetrating a company because SIEM was similar to selecting which flu strains will be added to the annual flu shot using past (known) strains. Legacy SIEMs use rule-based correlation of logs, which is dependent on known historical patterns of "what is bad."

Evolving Detection Tactics

With today's threat landscape, your detection tactics must evolve. Today, sensitive data, applications, and critical business processes occur in a distributed landscape. Cloud hosting, Software-as-a-Service (SaaS) providers, mobile devices, mobile apps, and the Internet of Things (IoT) all collect, process, and store data. So, if it was historically difficult to get to scale and

value with a traditional SIEM, with the complexity and volume of today's hybrid datacenters, it seems nearly impossible to be successful in today's environment. Enter security analytics and real-time behavior analytics.

The next generation security technology leverages machine learning (ML) and artificial intelligence (AI) to automate sifting through massive amounts of data and statistical algorithms to find patterns of highly advanced threats. Additionally, the cybersecurity talent crisis makes it difficult to support and staff large classic SIEM-related operations. The staffing issues keep security programs from progressing and effectively supporting what's created.

TIP

Security analytics platforms aim to provide ready-to-deploy content to minimize the manual effort required to configure and maintain the system and provide quick return on investment. Security analytics platforms and SIEMs have multiple hosting and implementation options based on the size and needs of a company. Three common options are

- On-premises
- Hosted/cloud (hosted by a third-party or in a cloud provider)
- Managed security service provider (MSSP) that hosts and operates your capabilities

Figure 1-1 gives you the advantages of the various hosting and support options.

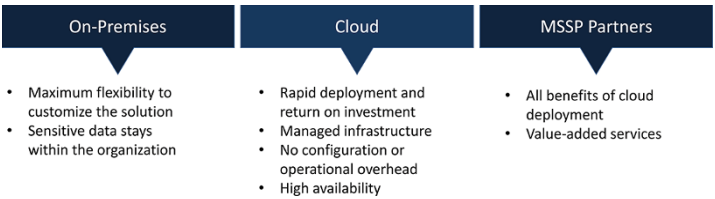

FIGURE 1-1: The advantages of different hosting options.

Understanding Security Analytics

Analytics is the discovery, interpretation, and communication of meaningful patterns in data. Within business (marketing, IT, science, and even the game of baseball), analytics, predictive

analytics, and statistical methods have been around and practiced for many years. And in cybersecurity, forms of data analysis have been around since security pioneers realized that historical logs and records contained meaningful insights that could detect problems.

However, in recent years, companies claiming to be pioneering in ML and AI have skyrocketed. Yet, if you ask some marketers and sales personnel, they can't articulate how these technologies are or aren't fundamental to their solution(s). However, these capabilities are enabling components of security analytics. Stated simply, there's a lot of promise in using ML and AI to intelligently analyze large sets of data and to automate and constantly make the process smarter and more efficient.

REMEMBER

Separating the features from the fluff is key to determining how you can build or enhance your security analytics opportunity. Ask vendors the specifics on how these technologies and approaches are used and how mature their capabilities are.

Four key concepts define security analytics. I cover them in this section.

Behavior profiling

You can leverage behavior profiling to baseline normal, which means taking measurements of normal so you can know when something measures as not normal. For instance, within your own healthcare, you may manually take your temperature using a thermometer for 30 days, and on average your body temperature is at or around 98.6 degrees Fahrenheit. However, on one day of that month, your thermometer reads 101 degrees. You must be getting sick! Now, imagine that your smartphone constantly and accurately measures your body temperature and alerts you if your body temp goes above 99.5 degrees. This is an example of profiling the behaviors of your body, setting a baseline, and prompting alerts if it exceeds a threshold.

However, temperature is something that almost everyone knows to watch for whether you regularly take your temp or just take it if you start to feel sick. More advanced analytics could measure all (or many) conditions of your body. By using this broader and massive set of data, you could compare what's normal to sudden or gradual changes and potentially anticipate or more earlier catch many issues.

Now flip this analogy back to security. Behavior profiling is essentially the same. Security analytics draws in massive amounts of data about what your workforce, computers, servers, routers, networking equipment, and so on are doing normally and is able to trigger alerts when things become abnormal. Figure 1-2 shows an example of a baseline behavior for normal patient data access pattern and a sudden deviation that's identified as a outlier.

FIGURE 1-2: A baseline for behavior profiling.

TIP

Baselining data to get a view of normal must be captured over a sufficiently long period of time to normalize any anomalies. Seek input from your platform providers and any benchmarking peers that you partner with on what they recommend. The recommendations may vary based on your company size and other dynamics. Typical time to baseline is 30 days.

Peer group analysis

Use peer group analysis to compare actions against peers. Continuously measuring the normal operation of your body and flagging changes alone would be great. However, imagine that you were able to measure groups of people that share characteristics within families, cities, and countries. Experts may be able to better predict outbreaks of disease, epidemics, and pandemics and where they may be starting and spreading.

Similarly, leveraging peer group analysis and behavior profiling within a company also has value. Peer group analysis has two aspects: comparing actions of an entity against other similar entities within the same organization, and comparing actions across industry, vendors, and so on.

Comparing actions of an entity against peers involves grouping entities by common attributes. For example, you can group a user into peer groups based on department, division, title, and reporting manager. Taking the example further, the action of the user is now compared with peers to detect any outlier activity (such as access to confidential data).

REMEMBER

If companies and security analytics platforms can begin to share more non-confidential security trends, events, and peer group data across companies and industries, the collective security of everyone will be better protected.

Business and threat intelligence

You should leverage business and threat intelligence context to elevate risk scores. Certain unique factors may trigger false alarms or provide meaningful additional information that warrants concern to a specific alarm being higher or lower. For example, consider the following life example questions:

- Did you just get out of a hot tub, bath, or spa?
- Do you have any known health issues that may be causing an explainable rise or fall in body temperature?
- Did you just run a marathon in 110-degree heat?
- Are you already taking acetaminophen or ibuprofen?
- Is your thermometer accurate?

All these things can affect your body temperature and are "your business" that you typically don't share broadly.

Your company and industry likely has certain threat actors (attackers that focus on your specific business). Your company also likely has a mix of different internal roles, departments, and organizational units, each possessing different purposes, behaviors, and tasks. Lastly, within each group, there are specific business assets (intellectual property, trade secrets, confidential information, personal information, and so on) that are handled by individuals. Combining this type of business and threat intelligence can help you prioritize security team actions appropriately as you're working through incidents. Your threat intelligence and business risk management processes and practices are highly valuable to security analytics because they allow you to provide business risk and threat context that may help you more broadly

prioritize your limited security resources (people, projects, money, and so on) on the most important potential threats and incidents.

Threat modeling

You can use threat modeling to predict and prioritize investigation and response. *Threat modeling* is a process by which potential threats can be identified and prioritized. It typically involves visual diagramming to map out the various threats, motivations, and attack paths.

In cybersecurity, mapping out or "threat modeling" various attacks, how they're detected, which ones are more impactful, and which deserve prioritized attention are great ways to determine how and where to focus. Numerous security events can occur at the same time, and an informed leader must help direct the team to what's critical, avoiding all unrelated distractions.

Threat modeling isn't a new concept. It's been used in cybersecurity, physical security, military, and broader business risk programs. However, it has traditionally been modeled through white board exercises that are driven out of workshops and feed incident response playbooks. Today's tools are starting to integrate the value of behavior profiling, all forms of intelligence that have been consolidated, and business risk and threat information to inform the best diagnoses and action. The health and livelihood of your company depends on security analytics coupled with business and threat intelligence. Threat models can also help you predict what may happen next. For example, if two out of five things have happened in a cyber threat model (for example, ransomware), it can predict the attack in progress as well as help you anticipate future actions and suggest remediation steps.

Crafting Your Business Case for Security Analytics

Building a business case for any project, approach, or purchase of cybersecurity requires telling a clear and compelling story of the "why" and the outcomes you wish to attain. The six-step cyberattack life cycle is often used to depict the tactics and phases of how attacks happen. While industry professionals largely agree with it and use it heavily, it doesn't necessarily translate for

business executives, board members, or other key stakeholders that may influence a decision. The six steps are

1. **Reconnaissance**
2. **Initial compromise**
3. **Command and control**
4. **Lateral movement**
5. **Target attainment**
6. **Exfiltration, corruption, and/or disruption**

For the purposes of this book, I reduce the cycle to the analogy of a burglar breaking into a house:

1. **Scan for target houses (reconnaissance).**
2. **Break in through an unlocked door or window, whatever is easiest (initial compromise).**
3. **Hide and/or create a way back in by copying the house key or cloning the garage door opener, so the burglar can get back in (command and control).**
4. **Visit all the rooms in the house and garage (lateral movement).**
5. **Find the good stuff, such as expensive electronics, watches, and jewelry (target attainment).**
6. **Steal/break the stuff, cut the electrical power (Exfiltration, corruption, and/or disruption).**

REMEMBER

Whatever terms and analogies you use, always make sure that your story is clear. Now, how does the attack life cycle matter to security analytics? Essentially, the attackers are becoming better at the attack path and doing it quietly. Also, your home security system and the company or yourself that monitors the system can't keep up with enabling, understanding, or acting on the alarms (if there are any). Security analytics essentially takes much of the voluminous and manual challenges out of protecting your house by determining what a normal day looks like, what signals, alarms, or signs may indicate a break-in, and how to prioritize the most concerning alarms.

Additionally, a few other nuggets that a security analytics tool can provide include improved signal to noise ratio. The goal is

potentially less alerts to have to act on and more meaningful alerts that aren't "false positives" or false alarms.

You can put this into context of a business case that you can take to executives or a board by using this four-step example:

- **Write an executive summary/problem statement:** This includes a high-level overview of the proposal and the problem you're trying to solve. Expect that some people won't read the whole thing. Here's an example of something you could use:

  Cyber attackers are becoming better at breaking into companies and oftentimes staying in. Companies also are using IT resources in a much more distributed fashion (such as cloud hosting, mobile application/storage, and Internet connected devices). This makes detection and responding to security incidents more and more challenging. Adequately interpreting and acting on alarms across the company is almost impossible to achieve with legacy methods and technology. Security analytics essentially takes much of the voluminous and manual challenges out of protecting your business by determining what a "normal day" looks like, what signals, alarms, or signs may indicate a breach, and how to prioritize the most concerning alarms.

- **Present a solution and desired outcomes (with alternatives, if relevant):** This is where you put your desired solution(s) on the table. Be clear about the outcomes you expect to achieve. While obvious, some programs focus more on the tool purchase itself or suffer from silver-bullet-syndrome (over-represent that any single tool or purchase can do much more than is realistic). Take the opportunity to articulate the specific solutions and needs based on your "use cases" (things that you define you need and will accomplish with a tool). State the key value elements (reduced false positives, time and cost savings from automation, better coverage of risk and the "attack surface") and how your solution achieves these outcomes.

- **Share the financials:** Sharing the cost is key to any business case because decisions are often made based on other company efforts and funding. Initial costs for purchasing a product are always fairly straightforward. However, implementation and ongoing costs are often miscalculated or forgotten. The implementation, operation, and sustainment

of these tools are what makes the difference. Additionally, factor in any cost savings expected to tell a balanced story of how the total cost of ownership may be offset.

- **Set a timeline:** Be clear about the implementation and time it will take to achieve the risk reduction value. This information is critical to both initial and ongoing support. Overcommitting and under-delivering are unfortunate symptoms of the complexities and underestimation in executing these cybersecurity projects. Your project should consider iterations and milestones as part of an overall journey versus a simple "buy-and-install" type of effort. Getting benchmarks from other companies that have accomplished a similar goal is a good idea because cybersecurity vendor "marketing estimates" can often be overly ambitious if not impossible to hit.

Developing Your Strategy for Security Analytics

A good business case is typically a decent start to a strategy but doesn't constitute a strategy. In the fluid cybersecurity risk, you must know your business risks and how the business is changing (acquisitions, divestitures, growth, decline, and so on). A strategy that links the business environment to the current state of maturity of the security program can help you articulate a crisp strategy for how security analytics should be positioned. This should also align (or be part of) your broader information security strategy.


TIP

Base your strategy on risk tolerance and cost considerations. Risk tolerance is your business's willingness to accept the risk versus spend time/effort in implementing additional security controls. If your risk tolerance is high, you can get away with lesser controls. Also make sure to prioritize in your strategy. You can't do everything at once, and this is especially tempting with security analytics because you want to analyze everything for all threats. This could be a recipe for disaster. Instead, identify what's the most pressing concerns related to your security needs. Identify low hanging fruit and then follow a phased approach with periodic milestones and measurements.

IN THIS CHAPTER

- Triangulating business risks and credible threats
- Making agile decisions for use cases
- Using the cloud and knowing how it matters to security analytics

Chapter 2
Defining and Accelerating Your Use Cases and Needs

The phrase *use cases* is IT and security vernacular for the various meaningful ways that you can leverage a tool, application, or system. Your use cases should tie directly back to your business case and strategy that you have prioritized to protect your company (see Chapter 1 for more on making your business case). If the use cases that your staff have for any tool are either unclear or don't align with the top goals and risks related to your strategy, you're probably not going to maximize the focus of your limited funding, personnel, and personal time. Not being clear on this can also cause re-work, spin, or lack of focused direction, which can cause frustration for yourself or your staff.

This chapter explores how understanding true business risks, credible threats, and potential use cases can be assessed together to determine the best path for your team with security analytics. This information can be governed by a committee or a decision framework to help your team make the best decisions. Lastly, you explore the infamous "cloud" and how modern IT movement to the cloud may change your security analytics strategy over time.

Assessing Business Risks and Credible Threats

Make sure that you triangulate your business risks and threats into a prioritization engine. *Triangulating* means connecting the dots and weaving together the right inputs to help you define your focus.

So how do you do that? First, evaluate the most significant cybersecurity risks to your business. Don't think about whether it's a malicious insider, a hacker, or a foreign government sponsored penetration. Instead, focus on the following:

- **Your inherent business risks:** How could your trade secrets, research, product development, manufacturing, or commercialization efforts be most compromised or disrupted?
- **Critical objectives or business outcomes for the year:** Could these goals, or goals with a broader time horizon, be hurt?
- **Do your business leaders have holistic input on this?** This is a rhetorical question. If you aren't asking and discussing with them in business terms they can understand, you probably aren't managing the business of security.

There isn't any super-secret formula or "easy button" you can push to make these answers appear. I've developed a methodology for accomplishing this, and I continually refine and improve it with every iteration. It all starts with seeking to understand, checking the "tech talk" at the door, and being a humble business partner who's trying to help your business leader(s) figure out how you can be helping them most. Additionally, it's *not* all about you and your team. Inevitably, these conversations should allow you to help them help themselves. Information security is more than IT or the security team's problem. Unless an employee or contractor for your company handles only public information that your CEO would be comfortable giving away for free, this person has a responsibility to help protect the company and all stakeholders (including your customers).

After you've evaluated the cybersecurity risks, focus on understanding credible threats to your business from a cybersecurity standpoint. This part is actually a bit more uncertain because you

can only go off what you know from other companies that have had problems and that are willing to share, or from making an educated guess to what attackers may do tomorrow.

TIP

You can learn more about these threats through industry Information Security Action Committees (ISACs) that are available from not-for-profit organizations in most industries. These organizations offer threat feeds (online sharing of specific threats or vulnerabilities each of the member companies are seeing) and share best practices so companies can utilize the collective experience to improve as a whole industry or avoid common mistakes. Additionally, some information security vendors provide threat feeds that you can purchase and ingest into your systems and/or management dashboards.

After you've done your homework on understanding threats, business risks, and what you need for protection, you need to pick and prioritize the use cases you want to implement. I recommend documenting how you connect risks, threats, and use cases that you believe most reduce the risks.

Making Agile Decisions

You'll inevitably have more use cases than you'll be capable of implementing at one time, so prioritization is key. Corporate culture hands-on leadership makes a big difference in how you and your team make decisions. You have three options:

- **Use case governance:** This involves having a carefully selected team of individuals that can provide cross functional or value-added input to the decision-making process. Who you pick really depends on the company, engagement outside of information security, and culture. At a minimum, you'll want representation from information security, IT, relevant business areas, and support functions such as HR, Investigations (if separate from HR), Legal, and physical security. You may need to adjust membership based on what works as you learn.
- **Use case decision framework:** A decision framework is a logical plan that depicts rules or tactics about how decisions are made. For more mature organizations, you can empower lower levels of the organization for speed. The challenge with

this is that you need to know what the "rules" of use case decisions should be before you can build a framework. This comes with practice.

- **Hybrid option:** This option provides the best of both worlds. You can create a committee of the most motivated and helpful people and then iterate your way through a decision framework that enables the governance team to meet less often. People's time is valuable, and empowering decisions at the lowest appropriate level is key to speed. In this cybersecurity business, speed can be the difference between a confirmed breach and a near miss. Additionally, speed-driven mistakes can cause errors in judgment or the evaporation of an HR case against an attacker.

Making Good Use of the Cloud

The term *cloud* grew in popularity almost ten years ago. However, here we are in the latter half of the second decade of the 21st century and it seems like companies are only now finally going to the cloud. Adoption is on the rise, and in the next three to four years, more than 50 percent of the infrastructure will be in the cloud.

Even with the delay between the hype and action, this migration of computing power and storage matters for information security professionals. Historically, you could theoretically monitor everything in your network because it was in your network. Now, your data and computing power can be spread across one or more cloud providers. There are cloud software, database, and infrastructure providers and a lot of competition.

As infrastructure, application, and data is moving to the cloud, security teams are faced with a huge challenge to secure this environment. This expands the attention from monitoring corporate networks to monitoring cloud (or leveraging third-party monitoring). Any security solution you choose, including security analytics needs to be cloud ready. The questions to ask your vendors include, "Do you offer a Software-as-a-Service solution in cloud?" and "Do you have the connectors to integrate with my cloud infrastructure to collect and analyze data?"

To give a better idea of how your IT infrastructure and cloud presence can affect the things you need to be able to monitor, Figure 2-1 shows a sample of cloud providers by service type and the types of use cases you need to be able to achieve with Securonix.

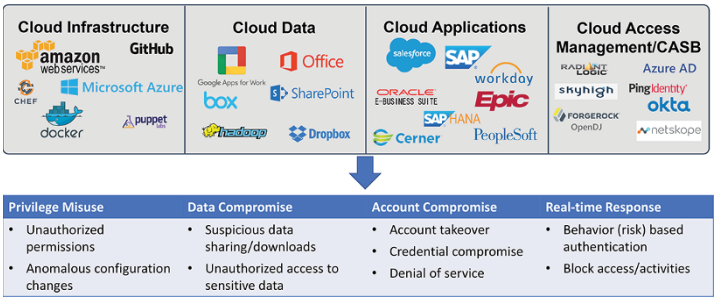

FIGURE 2-1: Securonix cloud security analytics.

Looking at Security Analytics Use Cases

Security analytics has a variety of use cases, from improving data visibility and threat detection to network traffic analysis and user behavior monitoring. Security analytics use cases can be categorized into four major buckets — insider threat, cyber threat, fraud analytics, and cloud security analytics. I've provided some of the most common (and necessary) use cases:

- Data exfiltration analytics
- Monitoring for misuse of privileged and service accounts
- Detecting credential compromise or account takeover
- Application monitoring to detect suspicious transactions
- Monitoring for suspicious login patterns
- Monitoring for advanced cyber threat patterns such as phishing, beaconing, and lateral movement
- Monitoring of cloud infrastructure and applications for misuse and data theft
- Detecting fraud

- Insider threat monitoring
- Threat hunting and investigation
- Incident response and case management
- Compliance and management reporting and dashboards

REMEMBER

The primary goals of security analytics are to analyze massive volume and variety of data to detect suspicious behavior that requires immediate attention and provide the investigation and incident response capabilities to take immediate action on such threat.

IN THIS CHAPTER

- Defining threat hunting
- Analyzing historical data
- Managing workflow and escalations
- Automating playbooks and incident response

Chapter 3
Threat Hunting and Incident Response

Threat hunting is the practice of proactively looking for threats to the organization or information assets that you aren't already aware of. When threat hunting, you don't actually know what the use cases are. Threat hunting can result in additional use cases needing to be added to your security analytics solution when you find new threats and vulnerabilities through your hunt that you think may be repeatable.

Incident response is how you respond and also how quickly you respond. The quicker you can respond the lesser the damage. You don't want to be winging it when you have a potential security incident. You also want to respond as quickly as possible, so you can contain the threat and the damage it may cause.

This chapter discusses the process of threat hunting as well as various considerations like workflow, escalating issues, and incident response playbooks and what automating some of them can do for you.

Diving Deeper into Threat Hunting

Threat hunting isn't new. However, it's becoming more popular because of the continued realization that you can't automatically anticipate every threat that may exist in your organization through conventional methods. A threat hunt team can be a single individual or a larger team of individuals whose job it is to find new threats and vulnerabilities across the organization.

The key to threat hunting is learning the right skills, equipping yourself with the right tools, and organizing and planning your hunts. In your planning stages, you may ask the following questions:

- What tools do I have?
- How much ground can I cover?
- How much can I carry with me?
- How many hunters do I have in my group?
- What will the roles of the various hunters be in my group?

REMEMBER

In the simplest form, you can literally apply these questions to your cybersecurity threat hunting tool. Having a plan of attack can make the difference in how effective your team will be in bringing home the target(s).

Leveraging Search and Data Visualization to Analyze Historical Data

Interactive search capabilities in threat hunting allow hunters to make text-based searches on raw and enriched security data and events. You're asking questions to narrow down your search to the most interesting event(s). Searching with enriched data means data that has been cleaned, improved with context information, and organized to make it more usable. Searching allows threat hunters (as well as incident response analysts) to accelerate their investigations into potential vulnerabilities and incidents.

When you couple interactive text-based searching capabilities with the ability to visualize potential linkages and insights across

enriched data, you allow threat hunters to see things they might not see with the raw or even enriched data.

Figure 3-1 shows a Securonix example of what data enrichment can look like as it analyzes the "raw event" shown at the top.

FIGURE 3-1: Securonix real-time enrichment.

Within the visualization from a search, the analyst should be able to visually get into more detail of a specific root cause. This helps keep everything organized and bucketed so the hunters don't get confused, waste time, or make incorrect assumptions. Other forms of visualization would be creating dashboards that provide insights on anything from security events, outliers, or trends.

Managing Workflow, Cases, and Incident Response

Workflow and escalation are the heart of your incident response and case management process. These management processes and tools allow you to deal with security events, prioritize focus, and work to ensure that the right actions are taken. I break this down in a bit more detail:

- **Workflow:** Workflow is a typical term used in IT and other business applications to describe and guide a user through a process and routing of activities to follow a defined sequence. For example, a security analyst sees a potential security event and flags it and then is guided to do some initial analysis and triage. He confirms it as a potential incident, and then it goes up to the next level team to look at.

- **Escalation:** This is the process of bumping a potential security event or incident up to the next level team or any required leadership overview. Escalation is an important part of workflow so that the right people and teams are getting engaged.
- **Incident response and orchestration:** These are the steps and actions to follow when a potential incident is discovered. Many teams use the term *playbook* to describe and document this process. Your security analytics solution should include native capabilities to enable you to automate response to an incident. This is usually done through direct integrations with endpoint, network, and identity management solutions. There are also many third-party incident response tools such as Phantom and Demisto (to name a couple). Your security analytics solution should integrate with these tools if you prefer to use these specialized tools. Two key incident automation actions are critical:
  - **Get context:** You automatically get more context about the event to assist the analyst. For example, you check if the IP address is malicious or you scan your environment to see if it has vulnerabilities that could be exploited.
  - **Take action:** You take action to stop or contain the incident. For example, you disable a user account, quarantine a file, or block a connection using an automatic or semi-automatic action based on a click of a button.
- **Case management process:** Case management is the process and tool(s) to enable documentation and relevant communication about specific security cases. Your security analytics platform should include capabilities to create and manage cases natively. The more that these case management tools and features can be integrated to common IT service tools like Remedy and Service Now, the more you can reduce re-work in driving actions with related teams (such as IT infrastructure or application support teams).

REMEMBER

Getting these approaches and processes nailed down is critical to operating a successful security operation. If these rules aren't clear, people can be inconsistent, which could result in an undesired outcome. The more that can be automated, the more time your security experts will have to focus on higher value activities or building new threat detection methods.

Automated Playbooks and Incident Response

Organizations often create playbooks to help teams respond in an organized fashion. This is similar to a football or basketball team having a playbook so the team can be more effective instead of just running down the field or court in a chaotic manner.

Automated playbooks are enabled when you program a security tool through your security analytics platform to conduct a certain action if a certain condition or potential exists. This may be as simple as taking a device offline or conducting a series of known actions to rectify a potential problem before it escalates into something more.

WARNING

Regardless of what you hear (at least in 2018), no holistic tool or capability exists that's so fully automated that it doesn't require human decisions and actions from security and IT teams. The key to maximizing the autonomy and automation that's available today is understanding what's possible and where to use it and rely on it.

IN THIS CHAPTER

- Getting past the marketing hype
- Leveraging your current state assessment and risk analysis to determine technology needs
- Looking for critical capabilities and features
- Creating a decision matrix to help you make an informed decision
- Understanding the vision and capability road maps of security analytics suppliers

Chapter 4
Evaluating Security Analytics Platforms

Evaluating a security analytics platform can be critically important. Many security programs in the last decade have sunk millions of dollars into traditional Security Information Event Management (SIEM) and log management solutions to face complicated integrations and less than expected results. As you approach the next generation technology for security analytics, you must get past the marketing hype and thoroughly evaluate the maturity of the product and the potential growth in features, capabilities, and integration. Probably most important is picking a platform that has features and capabilities that most align to your business risks and credible threats.

In this chapter, I walk you through helpful recommendations and tactics for evaluating security analytics platforms. Your goal is to focus on what's real and conduct a requirements- and features-driven analysis with the least bias possible.

Getting Past the Marketing Hype

If you've been to a security conference lately (and probably long after this book is published), you will hear a few choice words when discussing security analytics platforms (as well as a number of other tools). These aren't bad words, but they just get to a level of hype that everyone starts using them even if their technology doesn't exactly live up to the promise of the buzzword. This is why it's important to understand the hype and dive into the right details with your team and provider to understand what the tool or platform can (or can't) do both now and in the future.

Make sure that you understand what's on the company's road map (outline of what will be in releases in the future). The term *vaporware* is common in IT, and it means that certain features are promised as if they're ready or almost ready and then they are either never delivered or there is a significant delayed release of the touted capability. It's helpful to use peer company benchmarks that already use the vendor of the tool or platform you want so that you understand what their experience has been like. This is critical to getting past the marketing hype and truly making the best decision for your team and company.

Determining Technology Needs

Your company's risk profile should heavily influence the security analytics platform you select. For example, do you have a segmented manufacturing network that controls devices that power and run the manufacturing operations? Do you have a significant insider threat risk? Have you had specific types of security incidents or breaches in the past pertaining to specific business areas? Are your business leaders more concerned about a certain portion of the business? Read Chapter 2 to learn more about how to ensure that you thoroughly understand your business's risk landscape.

Additionally, your information security current state analysis and maturity should also be a factor. For example, what required capabilities, data sources, integrations, and tools are prerequisites to

your security analytics provider options? If you must have things enabled that you don't own or have implemented before you can get the full value, you need to see if you *can* achieve those things within your desired timeline. Otherwise, you may be owning cool technology that you can't actually use.

Choosing Critical Capabilities and Features

In this section, I provide you with key questions to ask when evaluating security analytics platform providers. These seven focal areas aren't exhaustive but are critical to your overall decision process, so consider them when choosing a provider. I always recommend creating a spreadsheet or decision matrix to help rank suppliers against the questions and criteria you're looking for. (See the later section in the chapter, "Creating a Decision Matrix," for more information.) These sections should help you accelerate your analysis and decision.

Architecture and scalability

Architecture questions you should ask include

- Is the architecture on an open data platform (such as Hadoop) allowing maximum flexibility and scale?
- Are all components of the security analytics (Logger, SIEM, user and entity behavioral analytics, or UEBA) solution on the single platform or will you be required to purchase and manage different platforms?
- Does the solution provide deployment options that could be on-premises, in the cloud Software-as-a-Service (SaaS), or run as a managed security service provider (MSSP)?

Scalability questions include

- How does your solution scale in larger deployment?
- Do you pay by data to scale (by GB, EPS, or no cost for scale)?

Analytics and content

Areas you should ask about in the analytics and content area include

- How does your platform leverage machine learning?
- Does the tool provide native UEBA capability?
- What type of analytics capabilities and processing exists out of the box? (Behavior anomaly, ability to use default or configured correlation rules, peer analytics, and so on.)
- What are the features to allow you to build your own analytics from the platform?
- Does your solution support risk modeling and prioritization? If so, how does it work?

Cloud security monitoring

When considering cloud monitoring, make sure to ask

- How does your solution interface with cloud-based solutions to do the following?
  - Monitor cloud applications that host sensitive data
  - Monitor cloud-hosted infrastructure
  - Support across the relevant platforms for your company (AWS, Azure, O365, Salesforce, and so on)
- Can your security analytics platform be deployed as a SaaS solution?
- If yes, is your cloud-hosted SaaS solution evaluated for compliance, quality, and security through the following?
  - SOC2 Type 2 certification
  - Segregated by customer/tenant (i.e. multi-tenancy)

Out-of-the-box content and ongoing updates

For out-of-the-box (OOTB) content and ongoing updates consider these questions:

- What various OOTB content and planned updates are available?
- How quickly can the OOTB features be enabled?
- What kind of threat library and threat exchange (across platform customers) is available?

Search and investigation

Questions to ask in the realm of search investigation include the following:

- What manual and interactive search capabilities exist on the platform?
- What search and investigation features do you have?
  - Text-based search?
  - Visualization?
  - Machine learning operators?
  - Search on historical data?
  - Ad-hoc reporting?
  - Data linkages?
  - Investigation workbench?

Automated response

Good areas to question in the category of automated response include the following:

- What types of built-in playbooks are available and how can they be configured or added to?
- How does your solution offer playbook automation?
- What incident orchestration and automation capabilities are provided natively?
- What case management features are provided natively?
- Is integration possible with existing incident response or case management tools that you already own and use?

Data privacy concerns

For areas in data privacy, consider the following:

- **Masking:** Can you hide or "mask" certain fields that contain sensitive data, so they're exposed only to the necessary individuals?
- **Role-based access controls (RBAC):** Does your solution have granular role-based access controls so you can ensure only the right individuals are seeing the most sensitive aspects of the platform?
- **Auditing:** Do you have auditing right for the solution and hosting environment (if applicable) and audit trails that are accessible?
- **European requirements:** Do you have any features or capabilities that assist in alignment or showing compliance to European requirements such as the General Data Protection Regulation (GDPR)?

Creating a Decision Matrix

A decision matrix can help you organize your requirements, questions, and responses from the security analytics platforms you're evaluating. In the preceding section in this chapter, you see a lot of questions that I would ask. To keep track of all this, I use a matrix like the one in Table 4-1. This sample shows how you can create your own decision matrix to complete a tab for each supplier you're evaluating, and then you can compare the results.

After you complete your analysis, total the final score. Tools like this help eliminate any solution bias. However, make sure to take a step back and reflect on the big picture, which is why you should include the last column of Table 4-1 for additional factors to consider.

TABLE 4-1 Security Analytics Decision Matrix

Criteria or Question	Supplier Response	Importance Weighting (% adding to 100)	Raw Score (1 Low, 10 High)	Weighted Score	Decision Notes and Additional Factors
How does the solution enact user and entity behavior monitoring?	This solution doesn't enable UEBA except for one experimental module.	20% (1.2)	2	2.4	This supplier has UEBA on its road map but it seems to be just getting into this capability.

Understanding the Vision and Capability Road Maps

There is no magic science or automated decision matrix you can use to understand and evaluate suppliers' visions and road maps. Ultimately, I recommend the following considerations:

- **Trust:** Do the vendor supplier representatives seem trustworthy and consistent in their messages, commitments, and general narrative?
- **Strategic vision:** Does the supplier seem to articulate its vision for how its product will evolve and stay ahead of competition?
- **Integration:** Does the product road map show a good current and future story for integration with other products you have?
- **Peer references:** Do you have peers at other companies within your industry or beyond that have experience with the performance and commitment to the preceding questions in this list?

REMEMBER

Determining the reality and sustainability of a vendor's strategy and promised road map items is more of an art than a science. You can try to ask questions to determine how thorough the vendor is or sounds when representing the road map. However, in many cases, this selection criteria probably relies the most on gut feel compared to other criteria.

IN THIS CHAPTER

- Preparing and planning
- Designing the solution
- Deploying the solution
- Tuning and operationalizing
- Supporting your capability

Chapter 5
Taking Steps Toward Successful Deployment

Very few projects in information security are successful without planning, good design, and an organized deployment process. Understanding your environment, goals, use cases, and data sources is critical. Getting this right upfront can save you money and time, and create better results.

This chapter walks you through some tips and tricks from start to finish on your security analytics deployment journey.

Preparation and Planning

Preparation and planning include a number of inputs:

- Your cybersecurity strategy
- Business security risk evaluation
- Information and data classification framework
- Compliance requirements
- Cost, resource, and timeline constraints

These inputs help prepare your team to meet requirements, scope the deployment, and prepare you to work with your provider.


TIP

Think about your journey as an iterative process. Taking on too much can result in slow or failed delivery. Taking on too little can result in lack of continued buy-in or support. An iterative delivery is a great option for maximizing your progress and scope. Regardless of your initial scope, clearly understand and state your requirements and use cases that you plan to address first. Understand your overall IT strategy and architecture (current and planned) to ensure your solution will be designed and implemented to maximize the coverage and effectiveness.

Planning and preparation steps include

- Defining success criteria and identifying in-scope use cases with input from business stakeholders
- Identifying data feed requirements and how to integrate them into the security analytics platform


WARNING

Not being able to get the right source data, logs, or application access is one of the biggest pitfalls. Your security analytics will only be as good as the data that's being analyzed.

Design

A security analytics program is more than just selecting a security analytics platform. To be successful, the design should include all related security tools and products that will interface with your platform. This could include your existing SIEM, data sources, ticketing systems, SOC tools, and procedures or standards that are required to operate processes (especially if they're online, automated, or integrated with your solutions).

Another critical aspect of design is identifying the expected data velocity (how fast data is flowing into the system), volume (how much data will exist over time), and retention requirements (how long to keep the data).

TIP

Create a visual design diagram both to understand the big picture as well as to educate the team that is responsible for supporting and operating the system. Here are some factors to consider in your design:

- Hardware required (on-premises servers, virtual servers, or cloud-hosted servers)
- System performance requirements based on expected velocity and volume of data to be processed
- Disaster recovery options (mirror, hot site, cold site backups)
- Data source inputs
- Required manipulation or filtering of incoming data
- Log/data retention handling (auto purge/archive)
- System outputs (downstream feeds) to other security tools
- Initial use cases (both feasible and value add)
- Automated workflow design (and any integrations with HR, legal, and security processes)

Deployment

Being prepared for deployment is critical because of how important security analytics systems are.

REMEMBER

You typically can't add *all* available data sources at the beginning, so prioritize an initial set and gradually add more on a continuous basis.

WARNING

Getting the right data sources is like feeding your dog. Dogs aren't happy when they don't get fed (and they may chew your furniture). Not feeding your security analytics platform can have similar results. Your results will be weak and, while your staff members may not chew office furniture, they definitely won't be as effective as they could be.

Another factor in your deployment is training staff on the new technology and capabilities. While artificial intelligence and machine learning makes these systems smarter, they don't implement and support themselves. Because you're already making the

financial investment, it's also important to invest in your people in order to get security analytics right.

Lastly, use out-of-the-box (OOTB) features, available content, and industry threat sharing. This can include leveraging industry specific threat models available in the platform as a starting point. Additionally, there are standard reports, rules, and other key value drivers that you can use right away.

Tuning and Operationalization

Tuning is important for security tools. This allows you to focus on what you're analyzing to make it more relevant. Because modern security analytics tools rely on statistical methods and machine learning, creating an initial baseline of data allows the system to determine what "normal" looks like.

Additionally, no OOTB solution comes automatically customized to your organizational needs. Reviewing and adjusting settings, features, and how you use various components is important to get the maximum value out of the platform. Talking with industry peers who've implemented the same platform you've purchased helps you accelerate your learning and helps you avoid other's mistakes.

Support

Thinking proactively about your support model for security analytics is critical to your short- and long-term success. You need to decide early on if you'll have the necessary trained subject matter experts to manage and support the security analytics platform internally, utilize third parties on-site at your company, or host the platform externally and have a third-party support and operate it.

REMEMBER

Ensure that your support model has appropriate coverage. Not being able to keep up with responding to and analyzing potential security events can create legal issues. You have probably heard of companies that had security alerts from their security tools but didn't have enough staff, the right staff, or the right focus to realize what was happening until it was too late.

IN THIS CHAPTER

- Being educated about your security environment
- Managing your use cases and data collection
- Working with a threat hunting team
- Making sure your dashboards and reporting are up to par

Chapter 6
Ten Considerations for Enabling Security Analytics and How Securonix Can Help

As you approach the security analytics space, Securonix can help. This chapter gives you ten considerations for enabling security analytics and what Securonix offers to assist you.

Know Your Environment

Knowing your technology environment and getting the right coverage within your company are critical. Some information security organizations don't have a full knowledge or inventory of their digital assets, which makes it nearly impossible for many security efforts to have the right level of assurance and coverage. Make sure that you understand what parts of your environment the security analytics solutions you're evaluating touch.

You should also know your information security resourcing environment. What skills and expertise do you have, can you hire, and can you buy externally? All those factors come into play when selecting a security analytics provider. Almost every information security team in this industry complains about not having enough talent or the right types of talent. It may be important for you to select a platform that has low operational overhead and enables rapid out-of-the-box (OOTB) connectors, features, and use cases. If you're adopting a cloud strategy, you may want to consider platforms that have an *option* for hosting and operating it for you as a Software-as-a-Service (SaaS) or a managed security service provider (MSSP).


TIP

Securonix provides flexible deployment options such as on-premises, SecuronixCloud (SaaS), and MSSP-partner operated. Securonix also provides comprehensive OOTB content delivered via its threat library to enable rapid deployment and quick time to value.

Identify Your Use Cases

Triangulate business risks and credible threats into a use case prioritization engine for a more comprehensive look into your environment from a business risk and threat standpoint. Knowing these two things in addition to your available use case potentials is key to making security analytics active. See Chapter 2 for more information.


TIP

Securonix provides packaged applications with built-in use cases for advanced cyber threat, insider threat, cloud security, and fraud. The packaged content enables you to deploy use cases with minimal overhead and get quick value for investment. To explore Securonix application options, visit `www.securonix.com/products/security-apps`.

Understand Your Data Collection Requirements

Security analytics is all about data. The more high-quality data you have the better the results. You need to plan your data requirements carefully. It comes down to knowing the three Vs: volume,

velocity, and variety. Knowing the volume and velocity helps you plan the architecture that can scale to support your data needs. Variety helps you evaluate the vendor to see if it supports the data types you have (for example, vertical application logs).


TIP

Securonix proves a unified platform based on a native Hadoop stack, shown in Figure 6-1, that enables unlimited scalability and data retention. Securonix is priced by identity so you don't get penalized for collecting data. Securonix connector library provides you OOTB integration with a variety of data sources and applications. The built-in REGEX feature enables you to parse any custom data feed through simple configuration steps from the user interface.

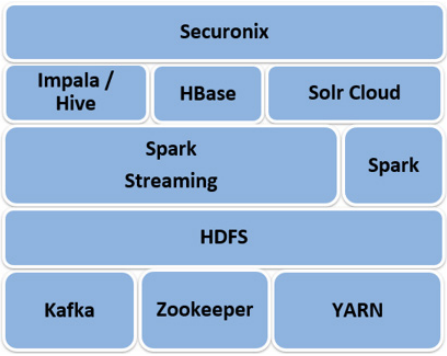

FIGURE 6-1: Securonix Hadoop Stack.

Consider Your Cloud Assets and Applications

We live in a perimeter-less IT world; firewalls and network security controls are no longer sufficiently protecting your data. You need controls where the data sits — in your application and your cloud assets. Your company's collection of cloud assets is critical to your selection of a security analytics platform. Obviously, if your company is 60 percent cloud hosted, it would be incredibly shortsighted to pick a solution that can only integrate with servers hosted within your company walls.

TIP

Securonix provides customers an option of fully managed SaaS deployment with robust integration with numerous cloud infrastructure, data, application, and access providers. The direct API integration ensures you get visibility to all your cloud data, assets, and users. Don't let lack of cloud integration be a reason to fly blind in security.

Factor in Threat Hunting and Investigation

Threat hunting is an important component to any modern security program. You can identify indicators of compromise with advanced machine learning algorithms, but you may still need to dig through your data to investigate the root cause and the extent of damage the threat may have caused. You need solutions that can allow your threat hunters to hunt effectively across massive volumes of data and with speed. For more information on threat hunting, check out Chapter 3.

TIP

Securonix provides comprehensive search and hunt capabilities. Securonix Spotter, a search feature supported by Apache Lucene, provides high-performance, text-based search and visualization capability. Securonix also provides a link analysis feature to enable you to create and visualize connections between data elements to trace a suspicious pattern quickly and efficiently.

Define Automated Response for Routine Tasks

Assuming your selected security analytics provider has the capability to enable automated response and playbooks, taking the time to do this for known and routine tasks can save your team time and allow it to focus on more of the unknowns or more difficult security events. It also ensures consistency of response to such tasks.

TIP

Securonix provides incident response playbooks and automation capabilities through direct integration with third-party solutions to take action in real time. Securonix Response Bot, a supervised learning engine, provides recommended actions for responding to threats based on a previous pattern of actions by the analyst. Discover more about Securonix incident response capabilities at `www.securonix.com/products/securonix-security-analytics-platform`.

Map Out IR Workflow and Case Management Processes

Mapping out your incident response workflow processes and how they interact with your case management tool can ensure that everyone is on the same page and consistent in executing high quality processes. These processes can also give you great references to leverage during audits, when partnering with company attorneys and HR professionals that may be part of your process. For more information on incident management, see Chapter 3.

TIP

Securonix provides built-in workflow and case management capability. The workflow can be fully customized based on your requirements. Securonix also supports metric reports and dashboards based on case status.

Understand Your Dashboards and Management Reporting Requirements

Dashboarding and insights driven from reporting help the security team tell a comprehensive story to leadership and key stakeholders. You don't want your team spending time searching through cases manually to pull out key insights. Think through how to routinely produce the most relevant metrics and insights in an automated fashion.

TIP

Securonix provides both standard and configurable insights through data insights, and reports:

- With the Data Insights function, you can
  - See activity and violation dashboards
  - Build your own, customize
  - Share dashboards with peers
- In the Reports feature, you can
  - Run ad-hoc reports
  - Categorize reports by user, resource, and compliance requirements

Operations, Performance, and Stability

Implementing a security analytics solution is Step One. Ensuring it's operating as expected requires monitoring of the various components and jobs for any failures or inconsistencies. Make sure that your security analytics platform provides capabilities to monitor and alert on the health of the platform.

TIP

Securonix SNYPR-Eye provides simplified operations with centralized monitoring and management of the platform. Notification alerts can be configured based on user preferences and service level agreements (SLAs).

Train Your Users

Even the best systems can't be fully successful without the right training for those that will use it. Everyone learns differently so provide a variety of ways for your users and administrators to engage. Examples include

- A hands on class or lab
- Reading (providing a manual)
- Videos
- On the job training or having a peer assistant

Formulating a mix of these options and having ongoing training and continuing education are key to the growth and progressive maturity of your staff and overall capability.


TIP

Securonix, through its global education program, provides classroom and online training courses to customers and partners. You can check out Securonix's training options at `www.securonix.com/services/training`.

Respond to threats with security analytics

Today, data is exploding. Enterprises generate terabytes of data across a multitude of sources. Collecting and analyzing this data to identify actionable threats is like finding a needle in a haystack. Traditional SIEM solutions fail, but security analytics leverages the power of machine learning and big data to analyze data at scale and detect "real" threats. This book helps you understand the tenets of security analytics and strategies to evaluate and deploy it in your environment.

Inside...

- Challenges with traditional SIEM
- The evolution of security analytics
- Use cases to combat modern threats
- Strategy to deploy security analytics

Aaron Pritz is an IT and security leader with 20+ years of experience in healthcare. He's a creative strategist that brings strategy to life through successful execution. He runs a consulting company in successfully applying industry experience within security, privacy, IT, and risk management.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-54513-2
Not For Resale

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.