ANDREW GORECKI

CYBER BREACH RESPONSE THAT ACTUALLY WORKS

ORGANIZATIONAL APPROACH TO MANAGING RESIDUAL RISK

WILEY

Table of Contents

List of Tables

List of Illustrations

Cyber Breach Response That Actually Works

Organizational Approach to Managing Residual Risk

Andrew Gorecki

WILEY

Foreword

It is often said that air traffic controllers have the most stressful job in the world. Being able to coordinate the safe takeoff and landing of dozens of commercial airliners, each carrying hundreds of passengers per day, all while dealing with a myriad of externalities, including the weather, ground control, controlled and noncontrolled airspaces, regulators like the FAA, flight crews, and airport operators, must seem like an impossible task. That is why in the United States, air traffic controllers must undergo a series of background checks and psychological exams, a rigorous training program, and certification testing, all before they ever set foot in a control tower.

If air traffic controllers have the most stressful job, cybersecurity incident responders might be a close second. As an incident responder, you're responsible for performing technical forensic investigations of highly complex environments as well as ensuring that the response team is maintaining its composure and working toward a common goal of mapping the full extent of attacker activity and eliminating their access to the network. It requires producing answers to questions that do not have an easy answer. It demands a deep level of technical knowledge in addition to a militaristic ability to lead a team toward a common objective. A responder must also consider the potential ramifications of a breach that may only surface much further down the line and take measures to protect the organization involved in the scenario, however improbable, that events unfold in such a way. It is part art form, part science.

When I interview people for incident responder positions, I often ask candidates to describe a situation where they

were able to thrive under adverse conditions, because they will absolutely find themselves in an even more difficult position as an incident responder. During a cybersecurity breach, stress levels are at their peak, people fear for their jobs and for the survival of their business, and in some circumstances, even fear for the physical safety of the general public. Attacks against critical infrastructure are not unheard of and seem to become even more prevalent as time goes on. In addition to the high-stress environment, financial budgets and higher-level business objectives undermine every step of the process. If you're not prepared to have the CEO of a Fortune 500 company channel his or her anger and frustration by yelling at you, you might not be cut out for the job. It is for these reasons that most incident responders do not stay in the field for very long. They move on to other roles and apply their experience in a proactive way to prevent organizations from experiencing their worst day. A responder with 10 years of experience is considered a relic.

All of this helps to explain why I always believed that there was no manual for how to do incident response, no textbook you could give to an inexperienced responder that tells them everything they need to know to be able to respond to incidents. The cybersecurity industry does not have a standard training curriculum and testing process to admit new entrants into the field, like the aviation industry has for air traffic controllers. Incident response is one of those things that you can truly learn only by doing, and you can only succeed after you have failed several times. It is baptism by fire, and the anointed need no other teacher.

That's why this book is so ambitious—it is an attempt to bring order to an inherently chaotic process. Over the past several years that Andrew and I have worked together, I have learned that he has a knack for reading complex situations, digesting critical information, and building

structure around the process that allows various elements to operate more efficiently. Most responders get so “into the weeds” in trying to solve the immediate problem that they don't have either the time or the ability to step back and consider the bigger picture. Andrew has taken his experience and engineered a framework for doing incident response more effectively. Take his advice and run with it—and if even one paragraph of this book helps your organization avoid the worst-case scenario in a cybersecurity incident, you'll know who to thank.

— Kurt Rohrbacher

Introduction

Cybersecurity has taken the media by storm in recent years, and cyberattacks are now headline news, from destructive ransomware attacks that impact manufacturing plants to data breaches that involve Fortune 500 companies.

Organizations have experienced notable disruptive cyberattacks in recent years. A ransomware attack on a global shipping company, A. P. Møller – Mærsk, wiped out their entire IT infrastructure across 600 sites in 130 countries. As a result of the cyberattack, Maersk had to rebuild their entire infrastructure in a heroic effort over 10 days. The total losses are estimated to have cost Mærsk up to $300 million.[1]

The National Health Service (NHS) in the U.K. incurred a cost of £92 million ($120 million) as a result of the WannaCry ransomware outbreak in June 2017. The cyberattack also resulted in the cancellation of 19,000 appointments.[2]

There are also numerous examples of data breaches resulting in significant financial losses, damage to brand reputation, and fines imposed by regulators. One of the most significant data breaches in recent years was the Equifax breach that led to the disclosure of personal data of 145 million U.S. consumers, including Social Security numbers, credit card information, addresses, and birth dates.[3]

As businesses and other organizations increase their digital footprint and online presence, the need to secure their information assets is more critical than ever before. The Ponemon Institute's Cost of a Data Breach Study (2019)

determined an average cost of a data breach across various industries was $3.92 million.[4] Furthermore, the World Economic Forum identifies cyberattacks as the fifth top risk in terms of likelihood and the seventh top risk in terms of impact.[5]

Many organizations are increasingly concerned about their exposure to cyberattacks. Businesses exist to generate value for their shareholders, and cyberattacks ultimately impact the bottom line. Even nonprofit organizations can suffer severe financial consequences as the result of a cyberattack.

In my consulting engagements, I have observed that cyber risk has become a frequent topic of board-level conversations, and enterprises increasingly perceive exposure to cyberattacks as a business issue. To address cyber risk, organizations build information security programs to protect critical assets and reduce risk to an acceptable level. As residual risk is inevitable, incident response is a critical control in the risk management process that allows organizations to address the aftermath of an incident, reduce the impact of a cyberattack, and restore the affected assets to a fully operational state.

An effective cyber breach response program is like a fire department. Organizations design a set of capabilities based on their needs and requirements, build an incident response team, acquire the necessary technology, and operationalize those capabilities. When the inevitable happens, the affected stakeholders can call the fire department, who might be able to extinguish the fire before the real damage is done, or at least reduce the amount of damage.

The benefits of developing an effective cyber breach response program include the following:

Minimize the impact of cyberattacks. The sooner an organization detects and responds to a cyberattack, the lesser the impact to business operations, brand reputation, and financial standing.

Decrease the cost of response. Effective incident response helps organizations decrease the overall attacker dwell time on their network, leading to a decreased cost of response. *Dwell time* is the time a threat actor remains on your network from the initial compromise to eradication.

Prevent enterprisewide incidents. Undetected intrusions can swiftly progress into enterprisewide incidents within weeks. The response effort is usually proportional to the time an attacker dwells on the network. Furthermore, enterprisewide incidents usually require disruptive remediation and can impact the bottom line of the victim organization.

Improve security posture. Incident response is an iterative process, with evaluation being one of its core components. The lessons-learned outcome can help organizations improve their policies, controls, and the incident response process itself. This approach ultimately leads to an enhanced security posture and cyber resilience.

Ensure compliance. Specific regulations and standards require organizations to have incident response capabilities, including an incident response plan.

Enhance service quality. Information technology is a business enabler, and its mission is to provide value to the business. The role of information security, on the other hand, is to protect that value. By building incident response capabilities, organizations can

minimize the impact of cyberattacks on their services and core business functions, leading to overall better service quality to internal and external clients.

Who Should Read This Book

I have written this book for anyone who is looking for an authoritative source of information on building and managing a cyber breach response program, including senior cybersecurity managers and chief information security officers (CISOs).

This book is also a valuable source of information for executive leaders, business and technology professionals, legal counsel, risk managers, and other stakeholders who have an active interest in cyber breach response in their organizations or who are planning to transition into a career in this field.

In this book, I explain cyber breach response concepts in a clear, concise, and technology-agnostic language that anyone with a grasp of fundamental cybersecurity and risk management concepts can understand.

How This Book Is Organized

I organized this book into six chapters that provide a comprehensive discussion of various topics relating to cyber breach response. I designed the book to serve both as a guide for building cyber breach response programs from scratch and as a reference guide for organizations that strive to grow and evolve their capabilities. Although the book consists of progressive chapters, each chapter provides stand-alone content that the reader can reference. Where appropriate, I also direct the reader to other chapters for specific information.

Chapter 1: Understanding the Bigger Picture This chapter defines cyber breach response and discusses foundational concepts. It starts with a brief overview of the threat landscape and discusses drivers for cyber breach response and their role within an overall cybersecurity program. A discussion of the critical building blocks of a sound cyber breach response strategy concludes this chapter.

Chapter 2: Building a Cybersecurity Incident Response Team Chapter 2 discusses the various considerations that organizations need to take into account when building an incident response team. The topics in this chapter include incident response competencies and functions, team models, skills, the hiring and retaining of talent, and cross-functional team development. A brief discussion on outsourcing considerations concludes this chapter.

Chapter 3: Technology Considerations in Cyber Breach Investigations This chapter focuses on building the technical capabilities necessary to support incident response investigations. The chapter starts with a discussion on general considerations for

sourcing incident response technology. Then it progresses into a discussion on data acquisition in on-premises and virtualized environments, including cloud computing. The final two sections discuss sources of network data and log management solutions.

Chapter 4: Crafting an Incident Response Plan Chapter 4 starts with a discussion on the incident response lifecycle. Then it dives into various incident management concepts before concluding with a discussion on post-incident activities and continual improvement.

Chapter 5: Investigating and Remediating Cyber Breaches This chapter takes an in-depth look at a methodology that incident responders employ during investigations. It discusses topics such as digital forensics and data analysis, cyber threat intelligence, malware analysis, threat hunting, and reporting. This chapter also discusses evidence types before concluding with a discussion on remediating cyber breaches.

Chapter 6: Legal and Regulatory Considerations in Cyber Breach Response Chapter 6 discusses how the legal and regulatory landscape impacts cyber breach investigations. It goes in-depth into considerations that organizations need to keep in mind to establish a defensible protocol for the handling of digital evidence. The chapter concludes with a brief discussion on data privacy considerations in investigations.

How to Contact Wiley or the Author

You can contact the author at andrew@agorecki.net.

If you believe you have found an error in this book, and it is not listed on the book's page at www.wiley.com, you can

report the issue to our customer technical support team at support.wiley.com.

Notes

1. "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million," Forbes, August 16, 2017, www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#21c48af04f9a.

2. "WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled," The Telegraph, October 11, 2018, www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled.

3. Federal Trade Commission, Equifax Data Breach Settlement, January 2020, www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

4. IBM Security, "How much would a data breach cost your business?" www.ibm.com/security/data-breach.

5. World Economic Forum, The Global Risks Report 2019, 14th Edition, www.weforum.org/reports/the-global-risks-report-2019.

CHAPTER 1
Understanding the Bigger Picture

Organizations across all industries increasingly rely on digital information to execute their business processes and support core business functions. Digital information that is of value to enterprises is also often a valuable and appealing target for threat actors. As a result, it requires protection in the same way as assets do in the physical world. Organizations implement safeguards to minimize risk arising from internal and external factors that might have a detrimental impact on their business. Cyber breach response plays a vital role in this process.

Building an effective cyber breach response program starts with strategy. *Strategy* is a process that allows organizations to achieve a vision and ensure that everyone is working toward the same goal. It enables this by providing a sense of direction and helping enterprises set measurable goals. A sound strategy also allows organizations to align capabilities to business objectives and manage residual risk when other controls fail.

This chapter discusses relevant foundational cybersecurity concepts, explains drivers for cyber breach response, and discusses the critical building blocks of strategy relating to cyber breach response.

Evolving Threat Landscape

Cyber breach response is typically a part of a more comprehensive cybersecurity program. Enterprises build cybersecurity programs to manage cyber risk and to ensure that they can continue business operations during

significant cyber events. This section discusses the cyberattack lifecycle and the different types of threat actors who pose a threat to enterprises.

Identifying Threat Actors

The cyber threat intelligence (CTI) community coined the term *threat actor* to describe an individual or a group who is responsible for cyberattacks or who poses a threat to an organization. Cybersecurity professionals and business stakeholders often use the term *attacker* or *adversary* instead. I use these terms interchangeably throughout this book.

Digital information has inherent risks associated with it. The World Economic Forum ranks cyberattacks as the fifth top risk in terms of likelihood and the seventh top risk in terms of impact.[1] The majority of medium-sized and large enterprises rely on critical digital assets that threat actors seek to exploit for a variety of purposes.

Historically, individuals and small groups engaged in hacking for notoriety or even fun. Their tactics typically focused on exploiting vulnerabilities in perimeter security in order to gain unauthorized access to computer networks. However, the rise of hacktivism, advanced persistent threats (APTs), and organized cybercrime have significantly increased cyber risk. The following list discusses common threat actor types and their motivations:

Advanced Persistent Threats *Advanced persistent threats*, also referred to as *nation-state actors*, are sophisticated threat actors who work on behalf of nation-states and foreign intelligence agencies, typically engaging in social espionage and stealing foreign intellectual property. What truly differentiates APTs from other threat actors is seemingly unlimited

resources and substantial funding. APT actors target specific organizations with clear objectives in mind. For example, the Chinese state-sponsored espionage group APT41 has targeted organizations in 14 countries over 7 years, and their operations have been consistent with Chinese national policy priorities.[2] Another key differentiator is that APTs often create custom malware that they tailor for the target. The meaning of APT has blurred in recent years, and it is not uncommon for cybersecurity professionals to use the term to refer to advanced cybercrime adversaries.

Organized Cybercrime Organized cybercrime has been on a steep rise over the last several years.[3] According the Federal Bureau of Investigation (FBI), its Internet Crime Complaint Center (IC3) received 351,937 complaints in 2018, as compared to 288,012 complaints in 2015.[4] With no geographic boundaries and the ability to stay anonymous, the Internet is a very attractive place for cybercriminals. The Internet made it possible for traditional crimes, such as theft or fraud, to evolve into cybercrime and maximize profits in the shortest time possible.[5] Organized cybercriminals have become increasingly sophisticated and often specialize in certain aspects of cybercrime. It is also not uncommon for cybercriminals to leverage models such as malware-as-a-service or pay-per-infection. Cybercriminals exploit organizations for financial gain in numerous ways. Examples include stealing intellectual property and other highly confidential information, stealing financial information and payment card data, planting ransomware, and cyber extortion through distributed denial-of-service (DDoS) attacks.

Insider Threats *Insider threats* come from within an organization and are particularly dangerous to

enterprises due to the amount of trust their employers give them. Another concern is the level of access insider threats have to valuable digital assets. Examples of insider threats include current and former employees, contractors, and even business partners who have inside information or access to digital assets. The industry also coined the term *unintentional insider threat* to describe individuals who unintentionally cause damage—for example, by sharing passwords or leaving sensitive documents in plain view.[6]

Hacktivists *Hacktivism* is a blend of computer hacking and activism. Hacktivists use technology and cyberattacks to draw attention to their ideology and political, social, or religious views. Common targets of cyber hacktivists may include corporations, government agencies, or any other entities that hacktivists consider or perceive as corrupt or not aligned with their ideology. Hacktivist attacks can cause severe disruption to enterprises. For example, a cyber hacktivist group may launch a DDoS attack against the victim or deface their website and leave a visible message to draw attention to the hacktivist's ideology. An example of a notable hacktivist attack is “Operation Tunisia,” where the Anonymous group with the help of Tunisian hackers took down eight government websites using DDoS attacks in support of the Arab Spring movement in 2010.[7] It is also worth mentioning that hacktivist attacks have dropped nearly 95 percent since 2015.[8]

Script Kiddies *Script kiddies* are the least sophisticated threat actor discussed thus far. They lack programming knowledge and computer expertise of their own. Instead, they use scripts, open source software tools, and other freely available hacking tools

to launch cyberattacks. In some cases, script kiddies may be experimenting with a tool that they downloaded from the Internet without being aware that they are launching a cyberattack. There are plenty of freely available tools and tutorials on the Internet that script kiddies can leverage.

In many cases, script kiddies are just a nuisance to organizations. However, their actions can also negatively impact enterprises. For example, a script kiddie may unleash a DDoS attack that could cause interruption of applications or use social engineering toolkits to steal sensitive data from employees, even if the attack is relatively unsophisticated. Also, script kiddies commonly engage in cyberstalking and cyberbullying. Cyberstalking and cyberbullying refer to the stalking and bullying that occurs by means of electronic communications technologies, often over the Internet.

Cyberattack Lifecycle

Some threat actors operate predictably, and the threat intelligence community created models to describe their operations. A *cyberattack lifecycle* is a sequence of steps that typically more sophisticated attackers move through to attain their goals. The threat intelligence community sometimes classifies those steps into two categories: preparation and execution. Understanding a cyberattack lifecycle is essential because breaking one of the stages can prevent a threat actor from attaining their goals. Cyber breach response plays a vital role in this process.

Various organizations have created their own models of the cyberattack lifecycle, such as the Lockheed Martin Cyber Kill Chain[9] or the MITRE ATT&CK framework.[10] This book discusses the *cyberattack preparation and execution*

frameworks that IBM X-Force Incident Response and Intelligence Services (X-Force IRIS) created to provide a conceptual representation of how sophisticated threat actors prepare and execute their attacks against a target. I chose this model because it clearly distinguishes between the preparation and execution phases of a cyberattack. It also incorporates additional steps, such as building an infrastructure for an attack that other approaches lack. Another crucial differentiator of the model is that it incorporates the idea of an attack "feedback loop." The attacker feedback loop allows for continuous engagement and refinement by the attacker to reach their objectives. This approach is more consistent with real-life incidents where threat actors adjust their operations in response to detection in order to remain in a compromised environment.

The threat intelligence community uses the concept of *tools, tactics, and procedures (TTPs)* to define behavioral characteristics that describe how threat actors operate. The term *TTPs* also refers to tactics, techniques, and procedures. However, in the context of cyber breach response, the terms are interchangeable. I discuss this concept in-depth in Chapter 5.

The X-Force IRIS cyberattack preparation and execution frameworks characterize threat data and communicate threat intelligence. These frameworks explain the full range of activities that occur before and during an actual compromise. This process provides incident responders and threat intelligence analysts with a model they can use to track data, conduct peer review research, and communicate analysis with greater clarity and consistency.

IBM X-Force IRIS Cyberattack Preparation and Execution Frameworks

Cyberattack Preparation Framework

The cyberattack preparation framework addresses activities that threat actors execute before the initial comprise.

The X-Force IRIS cyberattack preparation framework consists of eight phases, beginning with the determine objective phase and ending with the launch attack phase, where the attacker determines whether the attack resulted in a successful compromise or not. Between those initial and final phases, the attacker has several options to design an attack and may use any combination of the prepare attack phases. Upon determining the success or failure of the launch attack phase, the attacker will either move on to the execution framework in the case of success, or revise, change, or cancel the attack plan in the case of a failure.

IBM X-Force IRIS Cyberattack Preparation and Execution Frameworks

Each phase within the preparation framework describes unique activities that an attacker can execute to prepare a cyberattack:

- **External reconnaissance:** Determine a target and perform research on the target to identify exploitable access points.
- **Align TTPs to target:** Identify and determine TTPs necessary to conduct a successful attack.
- **Infrastructure:** Build a command and control (C2) infrastructure to access and control malware planted on the victim's network.
- **Malware and software tools:** Prepare an attack toolset necessary to launch and carry out the attack.

When all of the prerequisites are in place, an attacker launches an attack using either direct or indirect methods.

A *direct attack* refers to a situation where the attacker directly compromises the target. In contrast, an *indirect attack* involves an intermediary step. For example, an attacker may choose to compromise a third-party website or launch a supply-chain attack.

The operational security component underpins the entire preparation process. It represents the actions that an attacker takes to remain undetected. Examples include using obfuscation techniques, hiding their infrastructure behind different network addresses, or performing a reconnaissance from a different network. Finally, there is a feedback loop from the preparation process that allows attackers to revise and adjust their strategies.

Cyberattack Execution Framework

The cyberattack execution framework addresses activities that attackers execute after a successful compromise and focuses on access to the compromised environment, as well as expanding that access to attain the attacker's objectives, as depicted in Figure 1.1.

> **The X-Force IRIS cyberattack execution framework includes the phases that occur after the attacker moves through the key phases of the X-Force IRIS cyberattack preparation framework, and successfully gains access to at least one host within a network, or has logged in to one or more user account.**
>
> ***IBM X-Force IRIS Cyberattack Preparation and Execution Framework***

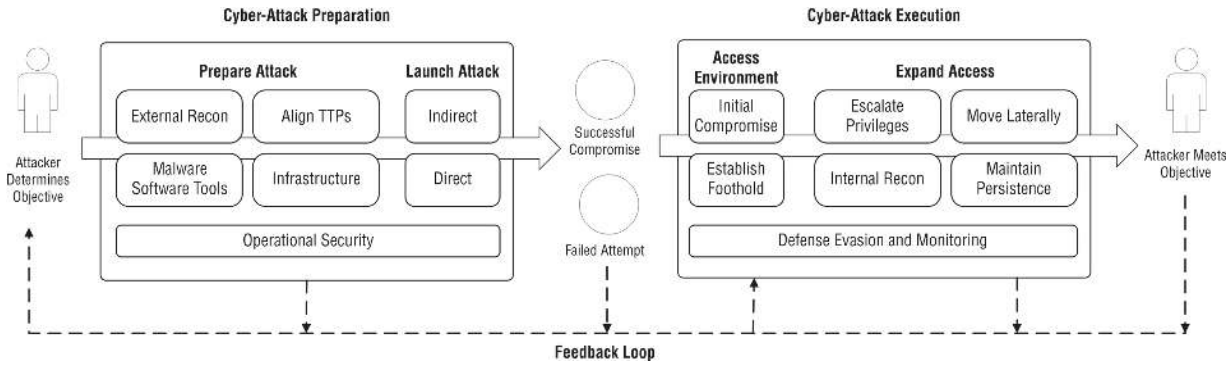

Figure 1.1: X-Force IRIS cyberattack preparation and execution frameworks

As with the preparation framework, each phase of the execution framework describes the activities that an attacker progresses through to execute an attack:

- **Initial compromise:** Occurs when an attacker successfully executes an attack and gains unauthorized access to the victim's system or network.
- **Establish foothold:** Allows an attacker to maintain access to the compromised network—for example, by planting backdoor malware.
- **Escalate privileges:** Attacker gains elevated access to system resources.
- **Internal reconnaissance:** Attacker collects internal information about the victim's network necessary to carry out the attack.
- **Move laterally:** Attacker compromises other systems and acquires additional privileges.
- **Maintain persistence:** Attacker maintains access to the compromised network.

Defense evasion and monitoring underpin each phase of the *execution* framework. As in the preparation phase, an attacker takes operational measures to evade security

controls and remain undetected on the victim's network. Finally, there is a feedback cycle, as with the preparation framework, that allows the attacker to revisit some of the stages and execute additional activities.

When an attacker successfully progresses through all the stages of both frameworks, they have accomplished their objectives. It is vital to emphasize that the preparation and execution frameworks model demonstrates how attackers often operate. However, in practice, an attacker may choose to skip certain phases, depending on their objectives and level of sophistication.

That said, the frameworks are an indispensable tool that can help cybersecurity professionals explain to nonsecurity personnel and business leaders the risks associated with sophisticated attackers and why cyber breach response is critical to managing those risks.

Defining Cyber Breach Response

Now that you have an essential understanding of threat actors and how they operate, it is time to explain some crucial cyber breach response terms. There is a great deal of confusion in the cybersecurity community when it comes to terminology. At times, even seasoned professionals incorrectly use basic terms relating to cyber breach response. This section discusses the basic terminology of cyber breach response and articulates important differences between fundamental concepts.

Events, Alerts, Observations, Incidents, and Breaches

It is essential to understand the difference between events, alerts, observations, incidents, and breaches in order to avoid confusion and to ensure an appropriate response.

Although these terms may be obvious to cybersecurity professionals, cyber breach response also includes business and technology stakeholders who may not be familiar with essential terms relating to cyber breach response. The following paragraphs explain the difference between these terms.

Events

An *event* is a change in the state of a computer system.[11] Systems and software applications change their state frequently in the course of their operations. For example, a state change occurs when a user authenticates into a system in order to perform some activities and the system captures the state change information in a log. This behavior is normal, and the generated log data provides a chronological record of system activities. For example, in my experience it is not uncommon for a medium-sized domain controller to generate more than 20,000 events a day, or for a demilitarized zone (DMZ) firewall to generate more than 70,000 events a day.

Some events may be indicative of an adverse activity that threatens the confidentiality, integrity, or availability of a computer system, including software applications and digital information that the system handles. For example, an *adverse event* occurs when a system or a software application generates errors in response to an unauthorized activity, such as an attempt to exploit a vulnerability.

Alerts

Organizations often use the terms *event* and *alert* interchangeably. However, there is a significant difference between them. An *alert* is a notification that a particular adverse event has occurred and may be indicative of a cybersecurity incident. Administrators configure systems

and tools to trigger alerts when a specific event or a series of events occurs. For example, an administrator might configure an alert in a security information and event management (SIEM) tool for conditions such as a high number of failed authentication events within a short period associated with a particular user account.

Over the years, cybersecurity vendors and the open source community have developed systems and tools that inspect data in motion and data at rest to alert on adverse events, and in some cases to prevent them. For example, network-based *intrusion detection systems (IDSs)* inspect network traffic and trigger alerts for events that match patterns of known attack vectors.

Observations

Observations is a term that is associated with events. Some organizations collect significant amounts of data, such as security events, social media data, email, data gathered through honeypots, and web crawling data, among others. By processing the data and applying algorithms to it, enterprises can generate observations that they can consume to identify patterns and formulate a threat hypothesis. For example, an organization may create an observation in the form of a graph diagram that shows particular malware connecting to a specific C2 domain that is associated with a phishing email address. Observations augment CTI capabilities, can help make informed decisions regarding defenses, and are invaluable in incident response investigations.[12]

Incidents

An adverse event becomes a *cybersecurity incident* when it either negatively impacts or poses an imminent threat to the confidentiality, integrity, or availability of a digital asset. Organization also often classify explicit or implied