Compliments of IBM

IBM Security Limited Edition

Integrated Threat Management

FOR DUMMIES®

A Wiley Brand

Learn:

- To prevent, detect, and respond to security incidents
- The principles of attack prevention
- The sources of threat intelligence data
- Ten techniques for integrated threat protection

Peter Gregory

About IBM Security

For over 50 years, since the introduction of the mainframe in 1970s, IBM has been committed to providing comprehensive security that meets evolving technological needs. By investing substantially in inorganic growth to supplement and enhance our organically developed security solutions, IBM has built a comprehensive portfolio that can help clients move up the maturity model from basic, to proficient, to advanced.

This progression was formalized in 2012 with the creation of the IBM Security Systems Division that brought multiple solutions together to increase the focus and help drive long-term strategy for enterprise IT security. In 2015, IBM Security Systems Division became a primary Business Unit of IBM, called "IBM Security."

IBM is a proven leader in enterprise security that helps organizations and defends against new and unknown threats. IBM continues to invest substantially in research and development to build a comprehensive, integrated portfolio to help organizations innovate while reducing risk with

- **Intelligence:** Security intelligence is at the core of the IBM Security portfolio. With its field professionals, IBM Security can provide the deep analytics and visibility that organizations need to help ward off the wide range of threats.

- **Integration:** IBM Security solutions and services systematically integrate both new and existing security capabilities across security domains, giving critical visibility, providing comprehensive controls, and helping reduce complexity.

- **Expertise:** IBM expertise stems from more than 6,000 hands-on professionals and researchers supporting customers in more than 130 countries. Their knowledge, along with the deep insights gathered from monitoring more than 270 million endpoints and managing 20 billion events per day, are built into IBM products and services, provided via real-time client feeds and embedded in professional engagements.

Integrated Threat Management

FOR DUMMIES®
A Wiley Brand

IBM Security Limited Edition

by Peter Gregory

FOR DUMMIES®
A Wiley Brand

Integrated Threat Management For Dummies®, IBM Security Limited Edition

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

The Magic Quadrant was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The link to the Gartner report is available upon request from IBM.

ISBN: 978-1-119-18585-7 (pbk); ISBN: 978-1-119-18586-4 (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. Johnson
Editorial Manager: Rev Mengle
Acquisitions Editor: Amy Fandrei
Business Development Representative: Sue Blessing
Production Editor: Siddique Shaik

IBM Acknowledgments

IBM Security would like to acknowledge the expertise and contributions of the following people:

Pamela Cobb, IBM Threat Protection System

Sam Dillingham, IBM Threat Protection System

Paul Griswold, IBM Infrastructure Portfolio

Patrick Vandenberg, IBM Security

Jordan Carlson, IBM Security Network Protection

Jay Bretzmann, IBM Security QRadar SIEM

George Tubin, IBM Security Trusteer

Rohan Ramesh, IBM BigFix

Leslie Wiggins, IBM Security Guardium

Leslie Kittredge, IBM Managed Security Services

Table of Contents

Introduction

Every industry sector has recent history of organizations that have been hit — and hit hard — by hackers and cybercriminal organizations. I don't need to mention names — you know who they are. Each week, more are added to the hit parade of organizations that, for one reason or another, didn't have the right measures in place to adequately prevent, detect, or respond to incidents.

Security tools vendors are everywhere, selling their wares to all who will listen and believe that this vendor's tools or that vendor's tools will solve all their problems. Often, organizations have a collection of tools that don't work well together. The result: no comprehensive big picture that shows the organization where its risks are and what can be done about them.

About This Book

Integrated Threat Management For Dummies, IBM Security Limited Edition, lays the foundation for effective tools and techniques that work together to help counter today's advanced threats. Regardless of your role in the IT security organization, threat management tools and techniques will influence your job. Your role determines the part you play to effectively manage threats, including those targeting the cloud and your company's data.

If you are a Chief Information Security Officer (CISO) or security manager, this book explains in detail the types of tools you need to effectively prevent, detect, and respond to security incidents. If you're in general business management, you'll better understand the risks associated with enterprise computing and the reasons why a comprehensive portfolio of security tools that work well together is so important.

Icons Used in This Book

Icons are used throughout this book to call attention to material worth noting in a special way. Here is a list of the icons along with a description of what each means:

Some points bear repeating, and others bear remembering. When you see this icon, take special note of what you're about to read.

Watch out! This information tells you to steer clear of things that may leave you vulnerable, cost you big bucks, suck your time, or are bad practices.

This icon indicates technical information that is probably most interesting to technology planners and architects.

If you see a Tip icon, pay attention — you're about to find out how to save some aggravation and time.

Chapter 1

Looking at Today's Threat Landscape

In This Chapter

- Understanding threats and risks that organizations face today
- Examining the potency of advanced threats
- Reviewing a few recent data breaches

We are well into the perfect storm where organizations and individuals of all types are doing practically everything online, combined with advanced cybercriminal organizations that are many steps ahead of us and can "own" our systems and our data with minimal effort. Often we feel we are up a creek without a duck and nearly defenseless against these attacks. Our adversaries are becoming so effective that security professionals have adopted a new mindset — to assume that breaches have occurred and will continue to occur, despite all efforts to stop them.

In this chapter, I look at today's threats and what they mean to organizations and their security professionals who try — often in vain — to stop them.

The Threat Evolution

Security professionals with even a little grey hair remember an era when firewalls and antivirus software was sufficient to stop most threats. It didn't seem easy at the time, but they were becoming increasingly reactive to the endless parade of threats and attacks. They were daunted by the thousands of new malware variants that appeared every year — today it's

more like thousands every hour! In this section, you see the threats that put sensitive data and systems at risk.

Mutating malware

Traditional, signature-based antivirus software as a primary defense is dead. While still essential for stopping older and still potent attacks, antivirus software, which still relies on signatures to recognize and stop viruses, worms, and Trojan horses, is all but useless against today's mutating malware.

Today's malware packs a new weapon: the capability to mutate itself on every individual host that it infects. The result: Every infected system is attacked with a unique piece of malware. When the antivirus software manufacturers create a new signature for this type of malware, chances are the signature is already outdated by the time it's deployed on an endpoint because each victim's computer has a unique copy. It's like stopping snowflakes in a blizzard.

The insider threat

When security professionals talk about the "insider threat," they're talking about an entire class of potentially harmful activities. Many think that means just malicious employees, but the insider threat actually goes much further than that.

Today's notion of insider threat includes these:

- **Innocent mistakes:** Accidents happen. Employees click on things they shouldn't and they send emails to unintended recipients (darn that auto-complete feature). You're sometimes pulled in many directions at once and sometimes drop the ball.
- **Poor judgment:** Employees should know better, but they reuse passwords, store sensitive data in personal clouds, and install toolbars in their browsers. Just call it poor hygiene.
- **Lack of training:** Oh, you didn't get the memo about the new way to store sensitive data? Workers can be proficient, but they may not understand how to do certain things. Sometimes this can put sensitive data and systems at risk.

- **Malice:** This is the classic employee who thinks she's about to be fired and downloads the entire customer database and the prized program source code, or a developer who plants a time bomb to orchestrate the future destruction of critical data.

The insider threat is difficult to stop, primarily because information systems just do what you tell them to, regardless of company policy or the intent of the user. Everything that can be used for good can be misused and abused for darker purposes.

The disappearing perimeter

Once upon a time, you could protect internal networks with a firewall, end of story. Fast-forward to modern IT where customers and business partners can access external and internal systems from within the network, employee laptops are connecting to the corporate network from all over the world, and also where organizations are storing their critical data in the cloud. For all intents and purposes, the perimeter now has so many holes in it that these defenses aren't comprehensive anymore.

Moving to the cloud

Many organizations are no longer purchasing hardware to internally host business applications in their own data centers. Nowadays, they're leasing cloud-based applications (through Software as a Service, or SaaS) or operating systems from Infrastructure as a Service (IaaS) providers like IBM Softlayer, Amazon Web Services, and Microsoft Azure.

Moving to the cloud makes great economic sense for many organizations, but few understand the seismic shift in risks and threats when doing so. Often, organizations assume that cloud providers are providing far more security than they actually are, and contracts with cloud providers often give customers too few rights and too little visibility. Ignorance is bliss, at least until a breach occurs — if and when the organization finds out about it.

Bringing your own anything and shadow-IT

Like the character "Agent Smith" said in the movie *The Matrix,* humans have a tendency to disrupt and disobey. Companies like Apple fueled our hunger for better endpoint devices such as MacBook Air laptops, as well as iPads and iPhones, which people all promptly brought to their workplaces and connected to the employers' internal networks. Most IT organizations were unable to stop them, particularly when it was senior executives who were oft to say, "I want to connect my iPad to the internal network — from anywhere."

With that, IT had formally lost control of corporate endpoints and critical data. But it didn't stop there. It seems like every day there's a new cloud application that's either free or so inexpensive that an employee can purchase a license and get reimbursed on next week's expense report check run. Now, organizations have completely lost control and visibility of critical data, because employees and departments are moving to the cloud without the approval or even the knowledge of corporate IT, corporate legal, and corporate security.

Corporate IT departments have been disintermediated and not for the first time (or the last). New innovative technologies are enabling non-IT workers to easily go around corporate IT and do whatever they want. While this agility might be good for business in some respects, many risks exist that the organization implicitly accepts through such practices, and most businesspeople who make these decisions to bring and use their own devices and adopt cloud services do so without recognizing the risks that such actions bring.

Just like in the famous dinosaur movie, users will find a way (to go around the IT department).

Advanced Persistent Threats

Advanced Persistent Threats (APTs) is one of those buzzwords that has as many definitions as people you ask. So before I go any further on this topic, let me help you understand what this means. An APT, or advanced attack, refers

to a threat actor (which could be an individual or a group) that has specifically targeted an individual or an organization that it intends to compromise, for the purpose of stealing or destroying data or information systems. More than just portraying the threat actor, an APT is the multiple tools and techniques employed by those actors that they use to gather intelligence about their target and then systematically take steps to achieve their objective.

In an APT campaign, threat actors often create custom malware that hasn't ever been seen before, anywhere in the world. Further, they may research and identify previously unknown vulnerabilities and craft malware to exploit them (this is known as a *zero-day threat,* by the way).

Selected Breaches

I've been mostly theoretical so far in this chapter. I think it's time to examine some breaches to better understand what they were about.

Large U.S. home improvement retailer

This particular breach resulted in the theft of 56 million credit cards used for purchase at retail stores from April through September 2014. Malware was installed on the checkout terminals in self-service checkout lanes in most retail stores. The malware used advanced techniques to "scrape" plain-text credit cards as well as customer email addresses from memory on the checkout terminals, which ran a version of Microsoft Windows as the underlying operating system.

Intruders used login credentials from a vendor that had access to corporate networks. It's likely that intruders obtained those login credentials in a typical phishing campaign, where users in the vendor company were tricked into providing logon credentials to a fake website they believed was legitimate.

U.S. health insurance provider

In early 2015, a large U.S. health insurer reported the "potential" theft of personal information on nearly 80 million citizens. The methods used to compromise and steal this data haven't been made public, but you can bet that it probably started with a relatively simple malware attack through a phishing campaign or a watering hole attack.

Large U.S. retail chain

The breach at this company resulted in the theft of credit card numbers for as many as 110 million customers who purchased merchandise in stores in late 2013. Similar to the home improvement retail breach, malware that stole plaintext credit card numbers was implanted on checkout terminals. The company had a security tool that detected the malware, but security operations personnel failed to disrupt or remove the malware. Also similar to the other retail breaches, intruders initially entered the network through the login credentials of one of its vendors.

A large computer and network security provider

This company was hacked in 2011, despite being the sort of company that tries to prevent this type of breach! The target: secrets related to its two-factor authentication product, so that intruders would be able to attempt to infiltrate organizations using the product itself for remote access authentication. This break-in, like many, started with phishing emails containing malware that were sent to Human Resources. One or more persons opened the attached documents, which signaled the initial compromise.

Chapter 2

Preventing Sophisticated Attacks

In This Chapter

- Exploring the principles of attack prevention
- Preventing network intrusions
- Preventing endpoint and data intrusions
- Understanding the attack chain

Security professionals devote almost every working moment to preventing attacks in an organization. Given the number of security breaches in the news, preventing attacks isn't altogether easy, unless you have good working knowledge about attacks as well as effective tools in place to help prevent and detect attacks. In this chapter, I discuss the principles of attack prevention as well as tools and techniques used to help prevent attacks on systems and data.

Attack Prevention

Attack prevention is mandatory — prevention isn't optional. Organizations willing to invest in information systems in support of business processes must be willing to invest in training their staff and acquiring tools to help protect those systems.

Principles of attack prevention

Because a variety of attack methods exist, there are naturally several ways to help prevent attacks from occurring. But before you begin looking at attack and prevention techniques,

it's important to understand the underlying principles of attack prevention. These principles are portrayed in Table 2-1.

Table 2-1 Attack Prevention Principles

Topic	*Principle*
Vulnerabilities	Eliminate all vulnerabilities; attackers exploit the vulnerability of choice.
Attack technique	Protect against all attack techniques; attackers will employ an attack technique of their choosing.
Target choice	Protect all targets; attackers may attack a target of their choosing.
Time of attack	Protect at all times; attackers will attack at a time of their choosing.

If you contemplate these principles, you may come to the same conclusion as many security professionals: Cyber warfare isn't fair, and the principles in Table 2-1 are nearly impossible to achieve! Clearly, the attackers have the advantage; while you may hold the moral high ground (the loftier position of defending critical and sensitive data from attack), attackers have a strategic battlefield advantage.

Attack prevention practices

While you might feel like you're at a disadvantage, you can do several things to help prevent attacks:

- **Vulnerability management:** This essential business practice consists of several activities for identifying vulnerabilities, including leveraging knowledge of the environment to conduct vulnerability scanning, keeping software and firmware versions up to date, consuming vulnerability data feeds, and patching systems. This helps to eliminate exploitable vulnerabilities, thereby making it more difficult for an attacker to access target systems.
- **Patch management:** This involves receiving information about available patches, conducting risk analysis on associated vulnerabilities, and prioritizing and applying security patches through an established change management process.

- **System hardening:** This is the decades-old practice of tightening up system and component configurations, removing unnecessary modules and tools, and removing unneeded user accounts. These techniques are typically documented in system and component hardening standards, and should be included in "master images" that are used to deploy new laptops, servers, and network devices within the organization.
- **Privilege reduction:** Here, you reduce the access of administrative and ordinary users to workable levels. This will limit the capabilities of an attacker who's able to take over a user account.
- **Attack surface reduction:** Prevent attacks by removing components and systems from an environment that are not critical for the environment's proper functioning. This helps to reduce the number of potential targets that an attacker can choose as an entry point into an organization.
- **Security awareness training:** This is the practice of educating end-users on the principles of resisting social engineering attacks, on good security practices such as strong passwords, following security policies and procedures, and limiting the use and dissemination of sensitive and critical information.

Network Intrusion Prevention

Network intrusion prevention is the practice of using tools and techniques to help detect and block network-based attacks. Because networks are the conduits of choice for attackers to conduct reconnaissance, deliver attacks, and steal sensitive information, it's important to employ some means for detecting and blocking any and all of these activities.

The principle tool for preventing network intrusions is the Intrusion Prevention System (IPS). Sometimes it's known as a Network IPS (NIPS). There is this distinction because there are also host-based intrusion prevention systems, known as HIPS, as well as wireless intrusion prevention systems (WIPS). In this book, I just use IPS, and you can assume that I'm always talking about the network kind.

An IPS is typically an *inline device,* connected to a network at a traffic aggregation point such as an Internet ingress-egress

point. An IPS accepts all inbound and outbound network traffic and examines each individual network packet and compares them against a set of policies, rules, and anomalous behavior to determine whether the packet should be allowed to pass, or be blocked. See Figure 2-1 for a depiction of an IPS in an enterprise network. Whenever a packet is blocked, the IPS creates a log entry for the event. Many IPSs also have an option for a monitoring or detection-only mode, to permit all traffic to pass but log or alert on any suspect packets.

IBM Security Network Protection (XGS) is one of several choices available for an IPS. Powered by IBM X-Force real-time threat intelligence, XGS is a next-generation IPS that uses behavior-based threat analysis to help protect against zero-day and those mutating threats I mention in Chapter 1. Customers using XGS appreciate the visibility (including on-board SSL/TLS inspection) and control over application network activities and flexible performance licensing, as well as thorough reporting, event metadata, rich security event detail, and the ability to "drill down" into individual events to understand the most minute details. XGS also integrates nicely with IBM Security QRadar SIEM, which is discussed in Chapter 3.

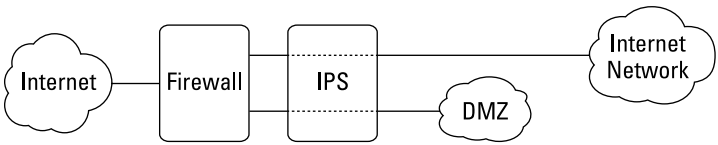

Figure 2-1: An IPS in an enterprise network.

Endpoint Malware Protection

Because they are so often the targets of attacks to an organization, endpoints are a logical and effective place to employ attack prevention tools. Most breaches begin with social engineering perpetrated against end-users, typically in phishing attacks (emails that attempt to trick users into clicking on links or opening attachments) and watering hole attacks (attacks on websites frequented by targeted users). The result of these attacks is the installation of malware on one or more endpoints, and this beachhead is the first step of a planned attack on an organization. Preventing the installation of malware on an endpoint is a key defense against an attack

that may lead to the compromise of sensitive data or critical systems.

Security professionals agree that the era of effective signature-based anti-malware software has passed. Traditional antivirus software is no longer effective at detecting and blocking today's potent malware threats. IBM Security Trusteer Apex Enterprise Malware Protection is one of several newer advanced malware prevention tools that can help disrupt the behavior of advanced malware by stopping the exploitation of vulnerabilities in specific applications that are commonly used by cybercriminals to secretly install malware, whether it's a typical old-school virus, a mutated virus, or a custom never-seen-before malware program in a targeted attack.

Trusteer Apex's secret sauce is its capability to passively observe running processes for specific applications to identify exploitation events and help block them if they begin doing something unexpected. Partly it achieves this through crowd-sourcing information from over 270 million protected endpoints. As an added bonus, Trusteer Apex can also help detect and block users from using a password from any enterprise application in any personal user accounts such as personal email, social media, or banking. Trusteer Apex also integrates with IBM Security QRadar SIEM, discussed in Chapter 3.

Data Protection

Information security is all about the data. While it's essential to detect and block intrusions at the perimeter with an IPS, and block malware on endpoints with advanced malware prevention tools, it's also logical to closely monitor the organization's crown jewels.

The best way to explain the need to protect the data itself is this: Several techniques for compromising data wouldn't trigger an event in an intrusion prevention system (IPS) or an advanced malware prevention system, especially if these techniques are executed by a trusted user. For example, a user who's about to resign could first extract a complete customer list from the customer database. While no malware is involved here, the intent of this action would certainly

be seen as provocative if not outright malicious. A data protection tool would recognize and create an alert on just such an occurrence.

IBM Security Guardium Data Activity Monitor closely observes all data access activities in databases, data warehouses, big data platforms, and file shares, and generates alerts for all out-of-the-ordinary activity that could be a sign of a costly data compromise. Guardium Data Activity Monitor also integrates with QRadar SIEM, which is discussed in Chapter 3.

The companion IBM Security Guardium Vulnerability Assessment tool is used to scan database infrastructures to help detect vulnerabilities that could be exploited by attackers. This tool also can help detect unwanted activities such as account sharing, excessive administrative logins, and unusual after-hours activity.

Breaking the attack chain

The *attack chain* is the sequence of events that occurs in most security breaches and typically consists of these activities:

- **Break-In:** The attacker infiltrates the corporate network using an attack weapon like a phishing email or drive-by download to install remote control tools on the host, which is most commonly an employee endpoint.
- **Latch-On:** The remote control tools execute code to contact a malicious host to download and install malware.
- **Expand:** Through remote code, the attacker expands his access to the desired corporate system containing the sensitive data.
- **Gather:** Data is accessed and consolidated from critical resources.
- **Exfiltrate:** The sensitive data is siphoned out of the corporate network via an unprotected system (for example, one that's not protected against malicious data exfiltration, but may have other protections in place) to an external system owned by the attacker.

Each of these activities is distinct from the others, but each is an important link in the chain leading to the successful breach that the attacker desires. While you want to block incidents as early as possible, blocking a breach at any point along the attack chain is considered a win.

Chapter 3

Detecting Threats in Your Infrastructure

In This Chapter

- Exploring threat detection
- Obtaining and using threat intelligence
- Understanding sources of threat intelligence data

Certainly, if we could prevent all threats and attacks, we would be able to sleep better at night. But the fact of the matter is that we can't prevent all threats and attacks, so the next best thing to do is detect threats that are getting through our defenses. In this chapter, I discuss the principles of threat detection as well as techniques and tools that can be used for threat detection.

Understanding the Principles of Threat Detection

If someone or something is attempting to compromise your environment, one or more systems or network components are going to notice. *What* they notice may not appear to be threatening at first, but there will be signs of intrusion.

There are important, time-honored principles of threat detection that are essential for every organization:

- **Collect all possible security data.** Every system and device that stores, processes, or transmits sensitive data should be logging important events that occur on the

device. Advanced attacks can turn off logs, edit them, or delete them altogether, so it's important to collect not just log data, but also data like network flow data, which can't be erased.

- **Store security event data in a consolidated database.** It's nice to have all your devices logging events, but when the data is scattered all over the organization, it's going to be a lot of trouble viewing it. Chances are, that log data will be ignored.
- **Protect logs from tampering.** Remember that first bullet on collecting security data? Anyone intent on compromising a system is going to want to erase her tracks, and this can make the central logging system a secondary target. The device or system where logs are stored must be particularly well fortified and configured so that even administrative personnel are unable to alter, delete, or add fictitious log entries.
- **Generate alerts for meaningful events.** The smallest systems can create megabytes of log data per day, and larger systems can create gigabytes or more. There's no way that people are going to, or even can, review this data in search of threats. Instead, the centralized system needs to know how to generate alerts and send them to relevant personnel when critical security events are taking place.
- **Follow written response procedures.** For each type of alert that can be generated, personnel need to know what action they're supposed to take. Response procedures need to be documented, reviewed, and practiced.
- **Record responses to threat alerts.** Whenever an actionable alert is created, the steps taken in response to the alert need to be recorded. This includes what action was taken, when it was taken, and who performed the action.
- **Review significant events.** A review of significant events needs to be performed, to discuss the cause of the event, what changes need to be made to help prevent a recurrence of the event, and the effectiveness of the response.

Threat detection isn't just about technology, but about having the right business processes and procedures in place, and training staff so they know how to use tools and make good decisions about what they observe.

Defining Threat Intelligence

Threat intelligence is certainly the buzzword of the year. Like other trendy terms such as *cloud computing,* "threat intel" conjures up a lot of different ideas. After sweeping the fluff aside, you can settle on a good, core definition of enterprise threat intelligence:

> *An ecosystem of contextually relevant and evidence-based knowledge — integrated into platforms and tools — to quickly and accurately address dangers to individuals, organizations, or assets in a standardized, consumable format.*

Organizations want threat intel — they *need* threat intel if they are going to effectively anticipate and respond to incidents in near real time. But making threat intel work as a valuable business process isn't straightforward: The security industry hasn't achieved a consensus on how threat intel can best be managed.

Threat intelligence sources fall into three categories:

- **Targeted intelligence:** This consists of information about threat actors and their techniques, their command and control infrastructure, and may include information on targeted vertical industries and victims.
- M**alware intelligence:** This is information about known malware and malware techniques, targeted vulnerabilities, and information about malware that has been reverse engineered.
- **Reputation intelligence:** This is information about known bad IP addresses, domains, and URLs.

Looking into Threat Visibility

Earlier in this chapter, I describe the principles of threat detection (see the section "Understanding the Principles of Threat Detection"). There, I discuss logging almost *ad nauseum*. Logging isn't cool or sexy, but it's absolutely necessary for every organization. There are other types of threat data that are discussed in this section.

Internal sources of threat data

The only way you're going to possibly be aware of security incidents is through comprehensive log data collection. Any organization's centralized log collection and event detection should include this list of log sources:

- Firewalls
- Routers and switches
- Intrusion prevention systems (IPS)
- Netflow systems
- Web filters
- Data loss prevention (DLP) systems
- Email servers and spam filters
- Servers, database management systems, and applications
- Endpoints
- Physical security systems
- Environmental control systems
- Proxies
- Wireless Access Points
- Vulnerability scans, like IBM Security QRadar Vulnerability Manager

Any device on the network that stores, processes, or transmits sensitive data should be logging events to a central management system.

External sources of threat data

Organizations need to look beyond their borders for threat intelligence data that will enable them to anticipate and respond to potential threats. There are both tactical and strategic sources of threat data. Consider tactical sources first:

- **Vendor security advisories:** Mature manufacturers of hardware and software products publish their own security advisories to warn their customers about threats as well as solutions (usually in the form of patches, but sometimes in other forms of remediation).

- **Open source security advisories:** Organizations such as Mitre and Secunia publish threat information. Sometimes these advisories are released earlier than manufacturers' advisories.
- **Law enforcement and news media:** Larger law enforcement organizations such as the U.S. Department of Homeland Security and the Federal Bureau of Investigation publish advisories to the public or to trusted parties.
- **Commercial solutions:** Threat intelligence feed sources, including IBM X-Force threat intelligence, are available in the form of advisories as well as electronic feeds.

Processing threat data

I've made the case for centralized log collection — bringing together log data from virtually everything in an organization's infrastructure. But there's a lot more to it than just storing gigabytes or petabytes of log data: It's got to be analyzed in real time so that actual threats can be immediately identified, giving humans an opportunity to respond and stop the threat.

IBM QRadar Security Intelligence Platform provides intelligence with effective high-level views, drill-down, and remediation. According to the 2015 Gartner Magic Quadrant for SIEM, QRadar is the leader for security information and event management (SIEM) platforms that bring log collection and management, anomaly detection, forensics, and vulnerability management into a single platform. QRadar's analytics capabilities can permit an organization to recognize the few relevant incidents hiding in the haystacks, thereby helping to provide the organization with the means to recognize and respond to incidents. Figure 3-1 shows QRadar's main dashboard.

Anomaly detection

One effective means for detecting threats is the capability to detect anomalies in systems and networks. This works through long-term observation of system behavior and network traffic, which acts as a baseline. Then, whenever there's anything on the system or network that has not been seen before, an alert is generated and personnel can take action and investigate.

Figure 3-1: QRadar's main dashboard.

Anomaly detection has three main components:

- User, application, and data profiling
- Thresholding
- Seasonality

Anomalies can be discovered through both automatic rules and specific search criteria. The basic point is to identify significant changes in the way people are acting (or acting up), the number of network connections occurring for applications, the amount of data being transferred between local and external IP addresses, or just oddball logins during early morning hours. All these conditions warrant investigation.

IBM Security QRadar solutions can analyze log data and create alerts that personnel can investigate. Often this gives organizations an opportunity to avert an incident before damage occurs.

Chapter 4

Responding to Threats

In This Chapter

- Viewing the sequence of incident response
- Getting outside help when you need it
- Understanding compliance monitoring

As we say in the information security profession, threats happen. Do you know what your organization will do when a serious threat or incident occurs? Security incident response is pretty mature — there's not much left to invent, but still, many organizations are woefully underprepared for even minor incidents. But first, you've got to know when an incident has occurred or is occurring — turn back to Chapter 3 to learn more about incident detection.

In this chapter, I discuss end-to-end security incident response. Pull up a seat and join me.

Responding to Security Incidents

In Chapter 3, I discuss the components necessary for an organization to detect security incidents. The other side of the same coin is an organization's capability to respond to a security incident. *Who you gonna call?*

Incident response steps

Security incident response is well established. Take this journey through the technique:

1. **Detection**

   Here, the existence of a security incident is first realized. It may be manifested in the form of an alert sent from a SIEM (security information and event management) platform, or notification from an external party.

2. **Analysis**

   Indicators of an incident are studied to determine their legitimacy. Often precursors are also studied to see if they're related. Analysts may need to run further tests and gather additional information to build a more complete picture of the suspected incident.

3. **Prioritization**

   In their analysis of the incident, personnel will quickly seek to understand the impact of the incident on the organization's capability to continue processing, as well as the impact on the integrity and confidentiality of critical information. Prioritizing an incident helps management understand the resources that must be utilized in subsequent steps.

4. **Notification**

   Incident responders need to notify appropriate personnel within the organization. The organization itself may need to notify external parties, such as customers, business partners, regulators, law enforcement, or the general public. Typically, a decision to notify any external party rests with a senior executive.

5. **Containment and forensics**

   Incident responders and possibly other personnel begin to take steps to halt the incident in progress, and make short-term changes to stop the incident and help prevent it from recurring. At the same time, it may be necessary to begin the process of forensic evidence collection for possible future legal proceedings.

6. **Recovery**

   Here, incident responders remove malware, rebuild systems, recover from backups, patch systems, and take steps to prevent similar incidents from happening again.

7. **Incident review**

   The purpose of a post-incident review is to review the steps leading to incident detection, as well as incident response. This helps to identify aspects of incident detection and response that went well, as well as opportunities for improving systems, tools, processes, and personnel training. The idea here is to meal prevent recurrence and improve response.

NIST Special Publication 800-61, *Computer Security Incident Handling Guide,* is an excellent resource for organizations that need to build an incident response plan.

Getting it right with training

Major incidents don't occur often in most organizations, so incident responders may be unfamiliar with their procedures. To get incident responders more familiar with response procedures, you have a couple of options:

- **Training:** An instructor (perhaps one of the senior or experienced incident responders) will conduct training on procedures.
- **Tabletop exercises:** The more useful type of training, where incident responders are guided through one or more simulated incidents by a moderator who is himself an experienced security incident responder. The tabletop exercise is really just training that simulates an actual incident, making the experience more real and memorable.

It's recommended that incident responders be trained at least once per year.

Automating remediation

With its automatic quarantine and custom remediation capabilities, IBM BigFix can respond to advanced threats and vulnerabilities in minutes. That means you have an incident response

system that can help minimize damage in the event of a breach or attack. The continuous, closed-loop remediation of endpoints helps ensure that a fix or patch has been successfully applied to all vulnerable endpoints on and off the corporate network.

Calling in the cavalry

Despite the best planning, the best security incident procedures, tools, and training, organizations often need outside help with serious security incidents such as the theft of sensitive information and intellectual property. Outside help is available.

IBM Emergency Response Services provides security incident response to help organizations manage security incidents, perform forensics, remediate vulnerabilities, and improve security policies, procedures, and operations.

Continuous improvement

In all things related to IT, security, and incident response, organizations should adopt a culture of continuous improvement. In the context of security incident response, this means:

- **Reviewing process documentation at least annually** to look for changes that will improve the documents.
- **Reviewing existing tools and their capabilities** to look for opportunities to accelerate incident detection, response, and remediation.
- **Reviewing incidents** (all big ones, and some smaller ones) to look for improvement opportunities in response procedures, as well as changes or improvements in systems and processes to help reduce the probability and impact of incidents in the first place.
- **Practice makes perfect!** You have to practice the procedures laid out in the response plan in order for them to be effective when the time comes.

Improvements can take many forms, including advances in technology, additional details in procedure documents, updates in industry standards, better incident response and forensics tools, and more training for personnel.

Performing Network Forensics

Unless an intruder walks into an office or data center and steals a computer or electronic media, chances are good that the intruder will use the organization's network to carry out surveillance, attack target systems, and steal data. Given this high probability that intruders will use your networks to steal your data, it's important to have tools in place to make the job of network forensics an effective means for piecing together the incident to see what happened.

This requires tools that perform continuous data collection, in the event that an incident requires forensics of network traffic. This is similar to continuous video surveillance that can be used later to review events that may have occurred.

IBM Security QRadar Incident Forensics includes full network packet collection that enables incident responders to examine an incident step-by-step, packet-by-packet. This helps incident responders quickly identify anomalies on the network and retrace the path the attack took.

But not all network forensics tools are created equally. Some are pretty rudimentary packet analysis tools that take considerable training to make sense out of the "hieroglyphics" of network content.

Monitoring for Compliance

Practically every organization is on the radar for one or more sets of laws, regulations, or standards that it must follow to be compliant. Some of the things that organizations must monitor include

- **Compliance:** Laws and industry standards mandate requirements on things such as data storage and transmission for particular pieces of information. For example, in the retail industry, the Payment Card Industry Data Security Standard (PCI DSS) sets standards related to credit card information security.

- **Anti-malware status and malware infections:** Logging all attempts by malware to infect systems or alter their behavior, as well as the health of anti-malware software on each endpoint and server.
- **Firewall rule exceptions:** Firewalls are configured to record attempts by outsiders (or insiders) to send traffic through them that violates security policy. Some of these events may indicate upcoming or active security events in progress that require immediate action.
- **Intrusion Prevention Systems (IPS) alerts:** These alerts are often good indications of reconnaissance, attempts to break in to an organization, or signs that a break-in has already taken place.
- **Invalid logon attempts to privileged accounts:** Insiders or outsiders often try to log in to privileged accounts on network devices, servers, endpoints, and applications in order to steal information or disrupt operations.
- **Unauthorized changes to systems and devices:** Insiders or outsiders may make unauthorized changes to systems and devices. In the case of insiders, this is sometimes just carelessness, but it could be malicious as well.
- **Unauthorized changes to applications and application configuration:** Actors may attempt (and sometimes succeed) to make unauthorized changes to applications and their configuration, sometimes as a result of poor judgment, but sometimes as a part of a scheme to separate an organization from its money or its sensitive data.
- **Attempts to bypass authentication controls:** Intruders have a lot of tricks they can use to trick systems and devices into letting them log in without providing logon credentials.
- **Attempts to alter or disable activity logs:** If an intruder can erase her tracks by altering activity logs, she'll go ahead and do so, making incident detection and forensics that much more difficult.
- **Attempts to access sensitive areas such as data centers:** Walking into sensitive areas to steal components, backup media, laptops, and even servers is just another tool of the intruder's trade.

I could go on and on, but you probably get the idea. There are a lot of ways in which poor judgment and misbehavior manifest themselves, and most organizations are required to perform monitoring to detect these and other activities. Just try to do all of this without a SIEM!

IBM BigFix can help you secure all your endpoints from laptops, desktops, and servers to point-of-sale devices, ATMs, and kiosks. It helps you to continuously monitor each endpoint for potential threats and helps enforce compliance with security, regulatory, and operational policies. With BigFix, you get real-time situational awareness and incident response across all endpoints. Because when it comes to protecting your data, minutes matter.

Chapter 5

Integrating Threat Protection Solutions

In This Chapter

- Understanding how security tools work together to help protect an organization
- Reviewing IBM's tools to aid in the prevention, detection, and response to incidents
- Taking a look at threat management communications protocols

Organizations use a wide range of information technologies to enable smart and agile business, but these technologies provide a wealth of opportunities for adversaries to stroll in and steal sensitive or critical data. Many organizations don't have the means to even know when such a theft occurs, and still others don't have the capability to effectively respond.

The Security Vendor Ecosystem

A surprising number of organizations purchase security tools from a variety of manufacturers, without regard for how one tool works with another. Even when organizations select the "best of breed" for each type of tool, the results can be a patchwork quilt of tools that overlap in some areas while leaving other needs unaddressed.

There's a better way to do this. Instead of gambling with your organization's security, you can build an ecosystem of security tools that work together and help give you the protection you need from today's threats.

Integrating Threat Management Solutions

The suite of tools in the IBM Threat Protection System can help defend an organization against the most advanced, potent threats. This starts with *IBM X-Force Exchange,* a cloud-based threat intelligence sharing platform that delivers actionable threat intel that is updated every minute. IBM X-Force Exchange is brought to you by IBM X-Force Research and Development, a world class organization that catalogs vulnerabilities, web pages, and collects data from almost 300 *million* endpoints to thwart advanced attacks.

The strategy for defeating today's persistent and sophisticated threats requires a three-part approach. These steps are

- **Prevent:** The first step involves implementing tools that help prevent attacks. These types of tools include IBM Security Network Protection (XGS) for network based protection, IBM Security Trusteer Apex for endpoint based protection, and IBM Security Guardium Data Activity Monitor for data protection.
- **Detect:** Because it's not possible to prevent all attacks, or because there may already be malware in your network, detection is the second key step. Attacks that wiggle their way through even the best defenses must be detected, so that organizations can quickly and effectively respond. One solution is IBM QRadar Security Intelligence Platform for a unified SIEM (security information and event management) that brings together information from an organization's IT systems, devices, and security systems including anti-malware, web filtering, firewalls, and data loss prevention (DLP) systems. One addition to this solution is the IBM Security QRadar Vulnerability Manager, which helps prioritize and address critical vulnerabilities.
- **Respond:** For those threats that get past defenses, organizations need the tools and know-how to quickly and effectively respond. This starts with IBM Security QRadar Incident Forensics, which gives incident responders the ability to examine an incident step-by-step. Next, IBM BigFix gives incident responders visibility into every

endpoint and what's going on and can help enforce policy updates or even quarantine a non-compliant endpoint. Finally, IBM Emergency Response Services is an organization of expert emergency response personnel ready to assist your organization with forensics and incident response.

Tying It All Together with SIEM

Prevention, detection, and response all require access to comprehensive data. A security information and event management (SIEM) system is the core of every threat management environment. Ingesting gigabytes or terabytes of log data each day, a SIEM such as IBM Security QRadar unlocks several capabilities that can help a security operations team detect anomalies and trends that may be early indicators of attack reconnaissance, attempted (or successful) exploitation of vulnerabilities, command and control, or data exfiltration.

A SIEM collects log data from every kind of system and device, then performs real-time analysis and correlation in order to quickly alert personnel of unwanted activities occurring in the environment that require priority attention.

Communication Protocols

There are several established standards for electronically transmitting threat information between systems. The existence of these standards makes it easier for organizations to integrate isolated point products into a threat management system.

In particular, IBM uses STIX (Structured Threat Information eXpression). It was developed by Mitre as a machine- and human-readable language for conveying threat information. IBM X-Force Exchange uses this protocol to communicate threat intelligence to third-party software and products.

Standard protocols make it easier for IBM Threat Protection System to communicate with other IBM systems and software, as well as products and services from other vendors.

Chapter 6

Ten Techniques for Integrated Threat Management

In This Chapter

- Understanding exposure analysis
- Prioritizing the risk of each threat, vulnerability, and incident
- Preventing and detecting security incidents
- Investigating and responding to incidents
- Stopping and containing security risks
- Planning for attacks before they happen
- Reviewing incident response documentation for continuous improvement

This chapter gives you ten techniques that every organization needs to master in order to be able to respond effectively to threats.

Exposure Analysis

It's necessary to understand the meaning of each particular vulnerability and threat in terms of real business impact to your organization. Analysts need to ascertain the risk of each vulnerability and threat, and deduce what incident scenarios are possible with each. In turn, analysts will be able to understand the kinds of incident scenarios possible, along with their potential impact to the organization.

Prioritize Risk

Each threat has a probability of occurrence and potential impact to the organization. Each vulnerability has a probability of exploitation, as well as the impact if exploitation occurs. Each incident has a particular level of impact to an organization.

To avoid overburdening security response teams, it's necessary to prioritize the risk of each threat, vulnerability, and incident to determine the appropriate level of resources to apply to each one.

Prevent

This is job number one in an organization — the prevention of security incidents. This is achieved through sound security architecture, training of staff, and having modern tools in place, such as firewalls, anti-malware, intrusion prevention systems, and data loss prevention systems.

Preventing cybercrime with IBM

IBM Security Trusteer Apex Advanced Malware Protection delivers a holistic endpoint cybercrime prevention platform that helps protect organizations against financial fraud and data breaches. Hundreds of organizations and tens of millions of end-users rely on these products from IBM Security to protect their web applications, computers, and mobile devices from online threats (such as advanced malware and phishing attacks).

IBM Security Network Protection is designed to protect business-critical network infrastructure through a unique combination of threat protection, visibility and control. IBM extends the abilities of traditional intrusion prevention systems by offering a next-generation solution that provides network security professionals with tools to help protect their network, and provide visibility and control over it. By delivering superior zero-day threat protection and threat intelligence powered by IBM X-Force, the XGS series provides critical insight and visibility into network activity, including encrypted traffic.

IBM Security Guardium Data Activity Monitor prevents unauthorized data access, alerts on changes or leaks

to help ensure data integrity, automates compliance controls and protects against internal and external threats. Continuous monitoring and real time security policies protect data across the enterprise, without changes or performance impact to data sources or applications. Guardium Data Activity Monitor protects data wherever it resides, and centralizes risk controls and analytics with a scalable architecture that provides 100 percent visibility on data activity.

Detect

This is job number two in a security organization: Detect each threat that makes it through prevention defenses. A SIEM (security information and event management) system that collects data from all possible sources — such as log data, network flows, configuration information, and vulnerability data, to name a few sources — then correlates that data to be able to determine if an incident is occurring and will alert personnel appropriately.

Detecting threats using IBM products

IBM QRadar Security Intelligence Platform offers an integrated solution for security intelligence and event management (SIEM), log management, configuration management, vulnerability assessment, and anomaly detection. It provides a unified dashboard and real-time insight into security and compliance risks across people, data, applications and infrastructure.

IBM X-Force Exchange is a robust, global threat-intelligence sharing platform designed to consume, share, and act on threat intelligence — all backed by the scale and reputation of IBM X-Force. Users can search for various threat indicators pulled from machine-generated intelligence, and add context via human intelligence for a collaborative way to research and help stop threats.

IBM Security QRadar Vulnerability Manager proactively discovers network device and application security vulnerabilities, adds context and supports the prioritization of remediation and mitigation activities. It helps you develop an optimized plan for addressing security exposures. IBM Security QRadar Vulnerability Manager is fully integrated with the

(continued)

(continued)

IBM QRadar Security Intelligence Platform, and enriches the results of both scheduled and dynamic vulnerability scans with network asset information, security configurations, flow data, logs and threat intelligence to manage vulnerabilities and achieve compliance.

Investigate

When an incident occurs, one or more security analysts will start with an alert and drill down into increasingly detailed data to determine how an attack was able to take place and what the attacker or malware did in affected systems and devices.

Respond

When the extent of an incident has been determined, personnel take steps to mount an appropriate response, to stop the incident from proceeding further and to limit impact on the organization or its customers.

Responding with IBM security

IBM Security QRadar Incident Forensics is designed to give enterprise security teams visibility into network activities and clarity around user actions. It can index both metadata and payload content within packet-capture (PCAP) files to fully reconstruct sessions, build digital impressions, highlight suspect content, and facilitate search-driven data explorations aided by visualizations. QRadar Incident Forensics easily integrates with QRadar Security Intelligence Platform and can be accessed using the QRadar one-console management interface.

IBM BigFix provides continuous, dynamic, granular endpoint monitoring, threat protection, incident response and compliance control throughout the threat lifecycle. The BigFix platform integrates and automates assessment and remediation, allowing security and operations teams to operate in unison to remediate and address risk, moving your

organization closer to continuous compliance, while reducing costs.

IBM Emergency Response Services (ERS) helps reduce risks and exposure to cyber threats with a more proactive and preventive approach, providing access to key resources that can enable faster incident recovery and reduced business impact. ERS enables a broader view and deeper understanding of incidents through intelligence data and analytics.

Contain

Incidents must be stopped dead in their tracks. This means removing malware and restoring systems to their pre-incident state. It may also include the steps taken to prevent recurrence of a similar incident in the future.

Plan

Organizations need to plan for incident response, so that individuals and teams at every level of the organization will know their roles and responsibilities when an incident occurs. To do this, an organization will need to develop a high-level policy regarding roles and responsibilities for incident management, as well as detailed "playbooks" that describe the steps taken for various types of incidents.

Organizations need to ensure that incident responders have the tools and training they need to effectively and quickly respond to an incident, and just like a fire drill, these response techniques must be practiced frequently.

Speed to Action

Threat actors are improving their techniques: They have improved their tools, which enables them to compromise even advanced defenses more quickly and easily than before. This requires organizations to reduce speed to action, so incidents can be contained as quickly as possible.

Improve

Threat management is an arms race, and your adversaries have a natural advantage at all times. This requires organizations to strategize and operate in a spirit of continuous improvement so that they have the best measure of parity against their enemies at all times.

Practically speaking, an organization should review all its incident response documentation at least once each year; train its personnel in incident management techniques and response; and review its prevention, detection, and response capabilities at least annually.

Notes

Notes

Notes

Notes

Manage threats against hackers and cybercriminals

Every industry has been hit hard by hackers and cybercriminal organizations. If you don't have the right measures in place to adequately prevent, detect, or respond to incidents, you can pay the price. *Integrated Threat Management For Dummies*, IBM Security Limited Edition, lays the foundation for effective tools and techniques that work together to counter today's advanced threats.

- ***Understand the risks associated with enterprise computing* — see the importance of a comprehensive portfolio of security tools**
- ***Look at today's threat landscape* — examine advanced threats**
- ***Handle your security breaches* — see how other companies manage their threats**

Open the book and find:

- **Threat management solutions**
- **How security tools work together to protect an organization**
- **IBM's tools for prevention, detection, and response**
- **Ten techniques for integrated threat protection**

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

FOR DUMMIES®
A Wiley Brand

Also available as an e-book

ISBN: 978-1-119-18585-7
Part # WGM12352-USEN-00
Not for resale

WILEY END USER LICENSE AGREEMENT

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