Brought to you by

cisco

Advanced Email Threats

for dummies®

A Wiley Brand

Cisco Special Edition



Safeguard your inboxes

Gain visibility and threat insight

Remediate threats faster

Floyd Smith
Gabrielle Bridgers

About Cisco

As the largest enterprise cybersecurity company in the world, we lead the way with cloud-native and cloud-delivered solutions that secure everything and everyone your network touches. Cisco Security Suites help you detect and respond to the most sophisticated threats and ransomware with correlated cross-domain telemetry and AI/ML driven enrichment to increase security efficacy, improve experiences, and optimize economics.

cisco.com/go/security-cloud

Cisco XDR is an extended detection and response solution that integrates with the broad Cisco security portfolio including endpoint, network, cloud, and email as well as many third-party offerings. This ensures organizations can gain a unified view across the security stack to enable faster, more simplified investigations, to reduce false positives, and to enhance threat detection and response through clear prioritization of alerts, providing the shortest path from detection to response.

cisco.com/go/xdr

Secure Email Threat Defense provides advanced threat detection capabilities by leveraging unique Artificial Intelligence and machine learning models, including Natural Language Processing, to identify malicious techniques used in attacks targeting your organization, derive unparalleled context for specific business risks, provide searchable threat telemetry, and categorize threats to understand which parts of your organization are most vulnerable to attack. As an important part of a larger Extended Detection and Response (XDR) strategy, Secure Email Threat Defense defends against critical threats with industry-leading threat intelligence and vital telemetry that informs strategic threat protection.

cisco.com/go/etd

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Advanced Email Threats



These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



Advanced Email Threats

Cisco Special Edition

by Floyd Smith and Gabrielle Bridgers

for dummies®
A Wiley Brand

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Advanced Email Threats For Dummies®, Cisco Special Edition

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

Copyright © 2024 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco Systems, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-25296-1 (pbk); ISBN 978-1-394-25297-8 (ebk)

Publisher's Acknowledgments

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

Project Manager: Jennifer Bingham
Acquisitions Editor: Traci Martin
Editorial Manager: Rev Mengle
Client Account Manager: Jeremith Coward
Content Refinement Specialist: Tamilmani Varadharaj

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Table of Contents

INTRODUCTION 1
About This Book 1
Foolish Assumptions 2
Icons Used in This Book 2
Beyond the Book 2

CHAPTER 1: **Introducing Advanced Email Threats** 3
Identifying Advanced Email Threats 4
Understanding the Impact of AI on Advanced Threats 5
Preventing Incidents from Escalating 8

CHAPTER 2: **Identifying Common Threats** 11
Describing Incidents by Type 12
Business email compromise 13
Account takeover 14
Ransomware 15
Extortion 16
Brand and user impersonation 17
Assessing the Importance of a Platform Approach 18

CHAPTER 3: **Focusing on the Role of AI in New Threats** 19
Tracking Technology Developments in AI 20
Showing How AI Makes Attacks More Sophisticated 21
Preventing Attacks with AI 22

CHAPTER 4: **Understanding the Role of Email Security in XDR** 25
The Role of Email in XDR Strategy 26
Using people profiles to help prevent BEC attacks 26
Getting a deeper understanding of threats 27
Seeing How Telemetry Enables XDR 27
Learning How Features Make XDR Effective 29

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

CHAPTER 5: **Ten Ways to Protect Against Advanced Email Threats** 31
Use Secure Email Threat Defense to Respond Quickly and Effectively 32
Optimize Your Defenses Against Major Email Threats 32
Use AI and Advanced Threat Analysis to Understand and Categorize Threats 33
Use Threat Data to Inform and Expedite Your Response 33
Act Quickly to Ensure Maximum Protection Against Threats 34
Use Cisco XDR for Protection and Defense Against Advanced Threats 34
Unify Visibility Across Control Points 34
Embrace Automated Tools to Maximize Resources 35
Detect Sooner, Respond Faster 35
Try Secure Email Threat Defense 36

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

Email security is an increasingly important topic. Artificial intelligence (AI) has both expanded the sophistication of attacks and enhanced the protections available to defend against them. But organizations have to understand the new and enhanced threats, and the changes to what's possible on the responsive side, to halt as many attacks as possible — and to reduce the impact of those that do succeed.

Email security doesn't stand alone. Email is connected to most or all of the people, and most or all of the systems, in a company. Threats to email messages and attachments, and to the use of email credentials for logging in to company systems, have impacts well beyond the user's inbox. In the face of a growing number of advanced threats, organizations need robust defenses that protect every individual and every system in their company.

Cisco, a leader in email security, and cybersecurity more broadly, for many years, brings experience, expertise, and a suite of solutions so extensive that a company can greatly enhance its security posture, reducing both the number of breaches and the impact of those that do occur.

This book explains the broad range of security challenges that can find their way to email accounts; how AI increases the challenges, but also offers solutions; and how Cisco solutions can help.

About This Book

Advanced Email Threats For Dummies, Cisco Special Edition, consists of five short chapters that explore

- What advanced email threats are and how AI has changed them (Chapter 1).
- Specifics about the major types of threats that companies face (Chapter 2).
- How AI is making attacks more sophisticated — and prevention more challenging (Chapter 3).

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- How Cisco solutions for email and organization-wide cybersecurity work together (Chapter 4).
- How you can protect against advanced email threats (Chapter 5).

Foolish Assumptions

As possible is assumed in this book. Still, readers will understand the importance of cybersecurity and know something about how their organization currently prevents, and responds to, security breaches that arrive through email. From this basis, any new and/or specialized terms are defined.

Icons Used in This Book

Throughout this book, special icons are used to call attention to important information. Here's what to expect.


REMEMBER

This icon points out information that you should perhaps send yourself an email to remind yourself about, so you have it available going forward.


TIP

The Tip icon points out information that aids in your understanding of a topic and that may save you time, money, or headaches.


WARNING

This information tells you to steer clear of anything that might cost you big bucks, be a time sink, or hurt your cybersecurity posture.

Beyond the Book

I'm sure this book will give you a better understanding of advanced email threats, but if you're left wanting more, visit the Cisco website at `www.cisco.com`. There, you can learn more about how Cisco's expertise helps organizations procure, deploy, manage, and optimize cybersecurity solutions.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Understanding threats
- Describing the impact of AI on threats
- Stopping the escalation of breaches

Chapter 1
Introducing Advanced Email Threats

The number of messaging options continues to increase, year after year — but email continues to serve as the most important business communication tool. More than 100 billion corporate email messages are exchanged every day, according to a Cisco report.

Given that volume, it's no surprise that bad actors target email as the leading attack vector for security breaches. While the rapid advance of technology is empowering users with new capabilities, it's also providing attackers with new tools for infiltrating an organization's security.

Email attacks make up a large share of these breaches, and attacks are becoming more sophisticated. Organizations need to understand the kinds of attacks they can expect to see, how advances in technology — especially in artificial intelligence (AI) and machine learning — are making attacks more potent, and how they can prevent incidents from escalating. (Often by using those same advances in technology for defensive and responsive purposes.)

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Organizations must be empowered with the tools to prevent breaches and to limit the damage caused when attacks do occur. According to a survey of leading organizations by Osterman Research, addressing email security is the number one security and risk priority for a quarter of organizations, and a top three priority for more than half.

Identifying Advanced Email Threats

Email was designed to be easy to implement, easy to use, and open. This makes it fundamentally easy to access — and easy to attack. It takes a lot of technological sophistication to try to protect something that wasn't built to be secure from the ground up.

Email is also closely connected to other technologies, including calendaring, file attachments, and identity certification within an organization. Almost every employee uses email, and almost every employee has direct email access to every other employee, up and down the organization chart.

Advanced email threats use a wide range of methods to attack company security, including sophisticated technology and an in-depth understanding of the weak points in the way that email recipients and senders communicate. Today's advanced threats are more organized, more personal, and more pervasive than in the past. Advanced threats also use new technology to an ever-increasing degree.

There are many ways of characterizing these threats, but one framework, used by Verizon, breaks threats down into four components:

- **Actors:** Actors are the initiators of threats. According to Verizon, 83 percent of attacks in 2023 were from external sources — but a surprising 17 percent of threats were from internal sources. Internal sources are also responsible for most threats that arise from errors, so they deserve a significant share of attention in threat identification and response.
- **Actions:** Actions are the steps that actors take to cause security breaches. In order of frequency, they include the use of stolen credentials, ransomware, phishing, *pretexting*

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

(tricking the recipient into providing information), the exploitation of vulnerabilities that allow access to a computer system, and others.

- **Assets:** An asset is an entity, whether human or machine, that the attacker can exploit as part of an attack. Assets the attacker can use include people receiving a given email message; the user's devices, such as their computer or smartphone; servers, nonuser devices that process information; the network that connects user devices, servers, and other computers; and media, such as thumb drives and printed documents that can contain valuable information.
- **Attributes:** Attributes are characteristics that may apply to an asset or an actor and are relevant to the success of an attack. Attributes include the confidentiality of information (and whether that can be breached in an attack); the integrity of data, which can be lost as the result of an attack that changes information; and availability, such as limiting information access to intended individuals only, not outsiders.

This book discusses the actors who initiate attacks, the actions they undertake in doing so, the assets they attempt to gain access to or leverage as part of their attacks, and the attributes related to the success or failure of the attack.


TIP

Think twice if you hear the CIA being discussed in reference to cybersecurity; it may not be the US Central Intelligence Agency that you're hearing about. Instead, in cybersecurity, CIA may refer to *confidentiality*, *integrity*, *and availability*, the three attributes that help define the nature, and the success or failure, of an attack.

Advanced email threats typically take advantage of advances in technology, such as the growing power of AI hardware and software.

Understanding the Impact of AI on Advanced Threats

Advances in AI affect emerging threats in three ways — one obvious and two more subtle.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The obvious way that AI advances affect emerging threats is the new capabilities that AI gives to the actors who initiate cyberattacks. An easy way to understand this is by drawing an analogy to one of the legitimate uses of AI: marketing.

Marketing is strongly affected by AI because it makes several typical marketing activities easier, including:

- **Research:** AI can gather information from all across the Internet and summarize it. This is a boon for marketers, who can quickly find target markets and effective ways to approach them.
- **Content creation:** AI is good for creating lots of content, such as sales emails or blog posts. Although AI can't match the very best human creators, it can generate average work in great quantities in a very short period of time. The incipient onslaught of large amounts of mediocre AI-generated content is sometimes referred to as "gray sludge."
- **Interaction:** Chatbots are increasingly replacing humans for routine question and answer sessions and similar interactions, including in text chat boxes on websites — *chatbot* is short for *text chat robot* — and in voice interactions.

It's easy to see how these legitimate uses of AI can be leveraged by bad actors as part of cybersecurity attacks. Conducting research, creating content, and interacting with humans on the receiving end have been part of both marketing work and cybersecurity attacks for years.

Now, all these activities can suddenly be sped up, and amplified in volume, using AI. Some attributes of AI seem very well-suited for misuse by attackers. For instance, one of the hallmarks of cyberattacks — phishing — has often been the poor quality of written or spoken English used in attacks against targets who use English as their only or main business language. The recipients recognize poor English when they see it, whether this is in an initial email or during a text or spoken interaction with an attacker. And poor English usage alerts the recipients that the email is part of an attack.

AI can help improve the quality of English language and grammar used in these interactions to a level that no longer elicits

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

suspicion, while the attacker can fill in details that AI might not be able to come up with on its own. The AI-enabled attacker might be able to get much farther in an attack than either a chatbot, or a non-AI-enabled attacker, could get on their own.



WARNING

If you aren't experienced with the newest AI tools, you may not be sufficiently aware of just how capable they are. A tool such as ChatGPT can set up a website in seconds, and if an AI tool can do something once in seconds, it can do it hundreds or thousands of times in minutes. Take the time to familiarize yourself with these tools and their capabilities so you can better keep up with attackers.

AI is also helpful to attackers in researching new vulnerabilities. There has been a long-existing research technique used by attackers called Google hacking, meaning the incisive use of a search engine such as Google or Bing to dig out information that is not meant to be exposed to the public.

Commonly available AI tools, however, can be given prompts such as, "Give me a list of security vulnerabilities at company X" to go after this kind of target more directly. Although some AI tools might have been programmed to refuse to answer a direct question of this nature, attackers will find — and share — workarounds that allow them to identify more vulnerabilities, faster, with AI than with previously existing search engines.

Although the enhanced capabilities of attackers might be a relatively obvious effect of AI on cybersecurity, one subtle effect of AI is that users are suddenly in unfamiliar territory as they do their daily work. A software developer using AI to write code is likely to repeat mistakes made by the developers whose work the AI was trained on and may not exercise full diligence in preventing them. A researcher using AI to speed their research efforts may find themselves interacting with people and organizations they would not have engaged with in the past.

With change happening so quickly, attackers can represent themselves as trusted experts in order to interact with targets and extract confidential information. (An attacker may even be somewhat expert in AI, given the potential abuse of AI for cybersecurity attacks. Yet they certainly don't merit trust.) And attackers can search for code that repeats past mistakes that led to vulnerabilities.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

So, AI can both empower attackers and lead users to make mistakes they would not previously have made. Luckily, however, AI also empowers those who make it their business to maintain and enhance cybersecurity. These AI-powered improvements in cybersecurity are the topic of Chapter 3.

Preventing Incidents from Escalating

There is a great deal of focus on preventing *incidents* — successful breaches — from occurring, and rightly so. Software that screens out or flags suspicious emails; user education and training; and the selection of email clients with security features can all help prevent many breaches from occurring.

Despite these tools, however, the number of breaches continues to increase. Recent developments, such as the rapid advance in AI capabilities described in the previous section, don't give organizations any reason to think that this will change anytime soon.

So you need to think of additional lines of defense beyond prevention. When breaches do occur, how can they be mitigated — their impact reduced, so as to not cause truly serious business problems?



TIP

Think of breach mitigation as a partner to breach prevention. For each step you take today to reduce breaches, think through what you might do when those efforts fall short:

You set up your email software to block known or suspected bad senders — but there will always be some new sites that don't yet appear on the list, and AI may increase the capability of attackers to create new and seemingly innocuous sites quickly. What actions will you take when those emails arrive in your users' inboxes?

You teach your users not to click on attachments that are not from a highly trusted source — but sometimes they will anyway, and the attachment will cause a breach. How will you detect the breach and raise an alert quickly?

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TAKING BREACHES (MORE) SERIOUSLY

Security breaches are taken seriously when they occur, and even more so when they have serious consequences, whether that's at your own organization or in the media. However, a reactive approach to the most consequential breaches can actually impair an organization's capability to prevent serious problems going forward.

Focusing on one or a few "breakouts" can prevent thoughtful and balanced consideration of where problems are most likely to occur in the future. The answer is not to only take seriously the few breaches that cause significant problems; it's to take the entire topic seriously and address it in a systematic manner, just like other challenges in business.

For more about responding to breaches in a thoughtful and considered manner, turn to Chapters 4 and 5.

You set up roles and responsibilities so that only designated employees have access to your customers' personally identifiable information (PII) — but, among those trusted employees, one may accidentally or deliberately disseminate the information. How will you predict when such illicit sharing is likely to occur, and how will you detect and respond to it when it does?

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Categorizing security incidents
- Asserting the importance of a platform approach

Chapter 2
Identifying Common Threats

Although it's always important for an individual, or an organization, to learn from past mistakes (and other kinds of problems), it can be even more valuable to learn from other peoples' errors. There is now, unfortunately, enough experience with cybersecurity breaches that they have received a great deal of serious attention.

As you work to reduce the impact of breaches in your own organization, there is a lot to learn from the experience of others. One important area of self-education is to identify the different types of threats that many organizations, perhaps including your own, have already experienced.

Different types of threats have specific traits in areas such as assessment of risk, prevention of breaches, potential impacts of breaches, and mitigation of the breaches that do occur. Those types of threats are the subject of this chapter.

In addition to learning from past problems, it's worth paying attention to emerging areas of technology that might create new risk. The biggest new technology impacts occurring today are in the area of artificial intelligence (AI,) and this affects cybersecurity

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

just as much or more as many other areas of business and life. For more on these emerging threats, turn to Chapter 3.

Describing Incidents by Type

The number of cybersecurity incidents and the financial losses attributed to them are increasing year over year. Figure 2-1 shows a recent summary of cybersecurity complaints and losses received by the FBI's Internet Crime Complaint Center (IC3). Complaints more than doubled over a five-year period and reported losses nearly quadrupled.

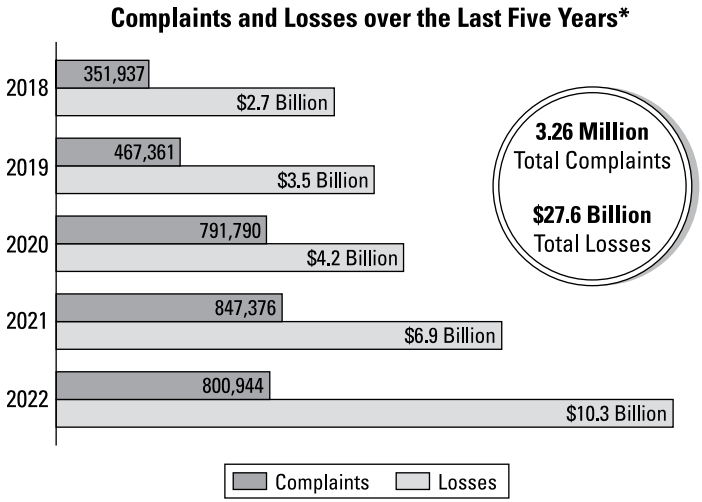


FIGURE 2-1: US cybersecurity complaints and losses recorded by the FBI.

Because crimes of all types tend to be underreported, both the number of complaints and the losses attributed to them in these reports are probably less than the actual totals. This total also doesn't include the large expenditures organizations make in an effort to prevent cybersecurity breaches from occurring.

The IC3 has a specialized group within it called the Recovery Asset Team (RAT). This team works with the government, financial institutions, and affected organizations and individuals to recover payments that victims of cybercrimes make to the criminals involved. (Such payments are often demanded, and made, in cryptocurrency.)

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

CYBERSECURITY IS SERIOUS BUSINESS

Cybersecurity breaches are such a large and impactful topic that they have attracted ongoing attention from a number of organizations, including the FBI.

The FBI runs a department called the Internet Crime Complaint Center, known in cybersecurity circles as IC3. IC3 issues an annual FBI Internet Crime Report. You can file a complaint, access the annual report, or learn more at `www.ic3.gov`.



TIP

If you do suffer a loss, you should contact any financial institution involved immediately and file a detailed complaint with the IC3. If necessary, you will be assigned an IC3 analyst who will work with you to recover funds, if possible, and reduce additional losses.

What is the best way to avoid having a complaint worth filing with the FBI, or other agencies — and how can you avoid or reduce financial losses? The first step is to understand the different kinds of email threats and some of the considerations that relate to assessing your risks, preventing problems of a specific type, and mitigating losses when they do occur.

Business email compromise

In a recent year, about 5 percent of IC3 complaints — but more than 25 percent of total losses — were attributed to *business email compromise* (BEC). BEC describes a targeted impersonation attack that persuades victims to wire money, buy gift cards, or share the targeted company's personally identifiable information (PII).

This type of attack often takes the form of a request to an employee in the finance department from an email that looks to be from a company executive. Because it's hard to see that the email is an impersonation, the receiver doesn't question the validity of the request and proceeds to process it. BECs have grown much more sophisticated and now include the use of cybercurrencies, the targeting of investment accounts as well as traditional banking accounts (both business and personal), and the spoofing of phone numbers to make fake transactions appear legitimate.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

MULTIPLE LEVELS OF LOSS

The direct costs of cybersecurity breaches are large enough, but they're only the beginning of what an organization can suffer. In addition to related financial losses, organizations face large expenditures to prevent and mitigate cybersecurity breaches. They can also suffer loss of business and significant impact on their reputation and brand to the extent that cybersecurity breaches become public. And individual employees can have their work lives and their careers severely impacted.

Breaches can include blackmail attempts in which cybercriminals threaten disclosure of a breach unless they receive further payments, compounding losses. On the other hand, organizations that take cybersecurity seriously can develop a positive reputation for managing this important emerging area of business effectively. When multiple businesses in a sector experience large and widely reported losses, as happens more and more in recent times, those that keep losses and reputational damage under control stand out in a positive way. So the potential benefits, not only the potential losses, relating to management of cybersecurity breaches are worthy of consideration.

AI is almost certain to contribute to future BEC attacks, because recently developed tools can be used to more quickly find potential victims, generate more convincing emails, conduct phone conversations using convincing syntax, accents, and response comments, and much more.

Account takeover

Account takeover is, as the name suggests, the seizing of control of an individual's online and/or financial accounts to make unauthorized transactions. This may be followed by the emptying out of financial accounts, misuse of online accounts, or blackmail to potentially prevent such abuse or simply to return control of the account to the rightful user.

According to the IC3, identity theft — which overlaps considerably with account takeover — has been associated with reported losses of roughly $200M a year for the last several years (and these are just reported instances). It's also worth noting that it's likely that some victims of account takeover fail to report it to the FBI.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Account takeover is a particular problem for businesses, which often exchange account information relatively freely with suppliers, vendors, distributors, customers, and others. And it's an even bigger problem for businesses that use cybercurrency accounts, which are often less protected against fraud than traditional bank accounts.

Ransomware

Ransomware is one of the easiest to understand and most frightening forms of cybersecurity breach. Ransomware refers to a type of attack in which malicious software, called *malware,* is activated on a targeted user device (such as a computer or mobile phone) or one or more company servers. This permanently blocks the victim's access to their files until a ransom is paid. A single breach may result in the installation of ransomware on multiple devices, or the cybercriminal may threaten to activate the software on additional devices.

Many techniques are used to infect victims' devices with ransomware. These can include:

- **Phishing emails:** In a phishing email, the cybercriminal uses social engineering techniques (such as claiming to be a known friend, work colleague, or business associate of the user) to get the user to take actions such as downloading a file or opening an email attachment that contains malware.
- **Remote Desktop Protocol exploitation:** Remote Desktop Protocol (RDP) helps users connect to remote computers over the Internet, and clients exist for Microsoft Windows, MacOS, various forms of Unix, and smartphone operating systems, among others. RDP can be exploited in several ways to gain control of a device or server.
- **Exploitation of other software vulnerabilities:** Computers are complex devices, and many vulnerabilities exist. Attackers are experts at finding and exploiting such vulnerabilities, and ransomware is a popular means to take advantage of them.

Companies and governments are targets of ransomware attacks. Perhaps the best-known cybersecurity attack of recent times was the Colonial Pipeline ransomware attack of May 2021. The attack was attributed to a Russian-based criminal gang called DarkSide.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

WHEN THE FIX IS THE PROBLEM

Software updates often contain fixes for recently discovered vulnerabilities, so installing updates as soon as you receive them is a good idea. But there are two considerations you need to be aware of with respect to such updates.

A *zero-day exploit* is a method used to attack a vulnerability that a vendor does not yet know about and has not released an update for. (The name refers to the fact that the vendor has had "zero days" to fix the vulnerability.) So even if you routinely install updates, you may still fall victim to an attack that no update yet exists for.

Fear of these vulnerabilities can cause the opposite problem: An attacker can advertise an important update to existing software, but the "update" is actually itself malware. The eagerness of users to protect themselves from malware leads them to install malware.

The existence of these subtleties illustrates the importance of using many different, overlapping approaches to prevent breaches and to manage the impact of breaches that do occur.

The Colonial Pipeline attack shut down the delivery of gasoline to gas stations, airlines, and others that received fuels delivered by the pipeline. The company that owns the pipeline paid a $4.4 million ransom, much of which was later recovered by the FBI.

This ransomware attack was the first to have such a large impact on vital US infrastructure and has caused an increase in official attention to cybersecurity in countries around the world. The existence of such a large and consequential attack also raises the bar for organizations of all kinds to treat cybersecurity as a crucially important concern.

Extortion

Extortion is among the top five types of cybercrime in the US, as ranked by IC3. Extortion is also part of other kinds of cyberattacks. For instance, a ransomware attack can include various kinds of extortion:

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- If the attacker gains access to confidential data such as trade secrets, they can threaten to release it to the public, damaging the interest of the business and its customers, suppliers, etc.
- The attacker can threaten to make the fact of the successful attack public, causing embarrassment, brand damage, and potential loss of business to a company.
- The attacker can use information they gain in the attack, such as PII for customers, to launch further attacks.

As in other kinds of extortion that aren't part of cybercrime, the FBI and other authorities recommend prompt reporting of extortion attempts to law enforcement as a vital step in reducing potential damage.

Brand and user impersonation

Cybercriminals often use one of several different types of impersonation as a threat tactic:

- **Celebrity impersonation:** Attackers impersonate the social media accounts of various celebrities to lend authority to their appeal to recipients to send them bitcoin or send funds.
- **User impersonation:** People in an organization can be impersonated to fool the public, their colleagues, or outsiders such as suppliers, customers, and so on. The impersonator can then request financial account access, other confidential information, or payments. Tech support, customer support, and government impersonation was connected to more than a billion dollars in reported losses in a recent year.



WARNING

Nearly three-quarters of user impersonation losses from tech support, customer support, and government impersonation were reported by people over 60. Some even lost their savings or homes. If your organization serves older people, your brand and personnel may be more likely to be impersonated by criminals. This is just one example of how different organizations have different risk profiles in relation to cybercrime and of how organizations need to be proactive in assessing and combating these risks.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Assessing the Importance of a Platform Approach

The sheer variety and complexity of different cybersecurity concerns may seem overwhelming. It's important to consider how threats interrelate and overlap with one another; how they're changing with advances in technology; and how your organization will have a unique risk profile based on a whole range of factors — from your industry, to your customer base, to the specific technologies that you use to run your business.



TIP

While it's critical to be proactive in addressing cybersecurity concerns, it's wise to consider a platform approach to cybersecurity.

Unifying your view across your technology stack increases visibility, context, and understanding of your vulnerability to advanced threats. In addition, you will want to consider monitoring, measurement, reporting, and other typical IT approaches to improve your awareness, readiness, responsiveness, and effectiveness in dealing with cybersecurity challenges. A platform approach can help make your efforts easier, less costly, and more effective.

To find out more about a platform approach to cybersecurity and how it can help you deal effectively with advanced email threats, turn to Chapters 4 and 5.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Spotting new advances in AI
- Investigating the impact of AI advances
- Stopping attacks driven by AI

Chapter 3
Focusing on the Role of AI in New Threats

Artificial intelligence (AI) is the most exciting technology in use today, with decades of work suddenly receiving unprecedented attention due to the emergence of generative AI. Generative AI is a newly successful approach that uses huge amounts of data to train machine learning (ML) models to produce surprisingly high-quality writing, artwork, software code, and other outputs.

Everyone involved in cybersecurity has been excited by the emergence of generative AI and other AI and ML tools and techniques. Unfortunately, this excitement is just as real for the attackers as it is for cybersecurity professionals: Both sides have gained extensive new capabilities as AI in general, and generative AI tools such as ChatGPT in particular, have made rapid advances.

This chapter discusses the steady advance of deeper currents in AI as well as the sudden emergence of new approaches in generative AI; how cybercriminals are using the technology for new attacks; and how cybersecurity professionals are integrating AI into their platform offerings.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Tracking Technology Developments in AI

Organizations have long used *predictive analytics* — the capability to use past patterns of behavior to predict future behavior. For example, if a new movie is very popular with people who like science fiction movies, a recommendation algorithm will recommend it for anyone who hasn't seen it yet — and likes science fiction movies. Age, gender, geographic location, and frequency of movie viewing are other characteristics that can be used to predict movie preferences. It's all about associations.

The latest news about AI has been about a sudden increase in capability for a certain kind of AI and ML that uses associations in a different way. These generative AI tools use associations between words, or between words and other media such as images, to answer questions. The reply might be in the form or a written or spoken response, an artwork, or a block of computer code — depending on what the user requests and which models the software has access to.

The triggering event for the latest burst of interest in AI was the public release of ChatGPT in November of 2022. ChatGPT answers questions conversationally and carries out tasks at a shockingly high level. ChatGPT can:

- Pass college and graduate school entrance exams with scores well above average
- Write convincing essays on a wide variety of topics
- Write software code that works well

In all these cases, ChatGPT does even better if it is carefully prompted by a knowledgeable person, and if that same person or a different one refines or fine-tunes its output. For instance, an essay written by ChatGPT may contain "facts" that are not true. A smart and careful human can spot and remove these assertions, resulting in a useful and "safe" piece of work.

Since the release of ChatGPT in late 2022, new updates allow it to scan the Internet for current information, and users can extend the tool with plug-ins, use images (such as software architectural diagrams) along with words for prompting, create customized versions called GPTs and share them, and more easily analyze

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

complex data structures— all capabilities that should worry anyone concerned with cybersecurity.


TIP

ChatGPT and other generative AI tools are trained on massive amounts of input, which means that they can draw on a lot of information — but also that their output, almost by definition, tends to be somewhere close to average, because their input will tend to be average overall. So ChatGPT can beat an inexperienced human writer or programmer, but it can't match experts. It can, however, handle routine tasks for experts, making them more productive.

ChatGPT is even better at quantity than it is at quality. If it takes a person half an hour to write a blog post, it will take them a full workday to write about a dozen blog posts, as they will need to eat, rest, and so on.

But if it takes ChatGPT five minutes to write a blog post, and a human five minutes to prompt the work, then check and correct it, the pair can write eight blog posts in an hour or 60 or so blog posts in a day. The work can be arranged around the human's downtimes and productivity can be very high indeed.


WARNING

There are lawsuits pending relating to generative AI tools, and more on the way. Copyright law allows both humans and machines to learn from copyrighted work but not to duplicate it in ways that qualify as plagiarism or similar violations. The legal question is whether, and to what degree, generative AI tools are learning versus copying. It will probably take years to answer these questions, and cybercriminals certainly will not raise their hands to pay their share of any penalties leveled against the creators or users of these tools. (Penalties against users are considered highly unlikely, but a final answer is of course still in the future.)

Showing How AI Makes Attacks More Sophisticated

What do these new capabilities mean for attackers? Unfortunately, generative AI solves many problems for attackers:

- **Keeping up to date:** Attacks based on new vulnerabilities may work on any relevant system that hasn't gotten the

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

latest update; attacks based on vulnerabilities that vendors have not discovered yet may work on most or all relevant systems. Staying up to date on vulnerabilities is a challenge for cybercriminals, and generative AI can scan the Internet and help.

- **Creating unique and varied attacks:** Marketers use A/B testing to identify effective email subject lines, for instance. Now attackers can carry out similar message creation and testing quite easily with generative AI. And attackers can use data analysis to match attacks to targeted groups (cybersecurity professionals, for example) or individuals (a Fortune 500 CFO, for instance) with increasing effectiveness.
- **Improving quality of content and writing style:** In the past, many attacks have been marred by flaws in the content or writing style of the attacker, but generative AI allows them to write at a higher level of quality with little effort.
- **Automating conversational capabilities:** Generative AI allows the software to carry out a conversation in text, or even using voice, at a level that will fool more and more targeted individuals as the software continues to improve. Small interventions along the way by humans on the attacker side may make such attacks impossible to differentiate from conversations with well-educated, well-informed humans with specific educational backgrounds and high levels of detailed and incisive professional knowledge.

Respondents to an Osterman Research survey believe they're already seeing AI used in email attacks, and that these efforts will increase over time.

Preventing Attacks with AI

AI will be an important tool in preventing cybersecurity attacks, whether AI-driven or not. Vendors of email software have already started to use AI as part of their security toolkit, but much more needs to be done — and customers want more than vendors are currently offering.

According to Osterman Research, two-thirds of organizations have already implanted AI-enabled email security solutions, over and above the protections included by their primary email software provider. Most of the rest are in the process of doing so.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The ability of users to detect many types of attacks will diminish rapidly as generative AI fixes many of the flaws, such as poor targeting or poor use of language, that have prevented attacks from succeeding in the past. The importance of security solutions will only continue to increase, and AI — which will certainly be part of the problem, in terms of cybersecurity — will need to be part of the solution as well.

AI can be used in many interesting ways to help boost email security:

- **Understanding the characteristics and behavior of employees and the people they correspond with.** AI can profile, for positive purposes, both employees and those outside the organization with whom they are in regular contact. Generative AI may be used by attackers to create emails that seem to be written by a professional in a given professional position. But it can also be used to detect emails that don't match existing examples of the style of the individual they're supposed to have come from.
- **Spotting cybersecurity tells.** AI can be used to scan email content and attachments for cybersecurity tells, such as emails that ask for money or attachments that contain hidden code associated with attacks. Such emails can be prevented from reaching the targeted recipient or marked with warning labels for the recipient to consider before taking action.
- **Identifying content written by generative AI.** AI can be used in efforts to detect AI-written content, or to flag suspicious content for further consideration.
- **Using attack emails for training.** When one aspect of an incoming email exposes it as a cybersecurity issue, the entire email and its metadata — surrounding data such as the sending date, the servers it passed through, and so on — can be used to train ML models that will then go on to do an even better job of detecting future suspicious emails.
- **Protecting domains.** Current domain protection technology identifies emails that are not authenticated properly that claim to be sent from a company's legitimate domain. AI could expand this protection by identifying threats from domains a company doesn't own and control, such as cousin/lookalike domains.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

FROM PREVENTION TO REMEDIATION

Preventing attacks is the ideal, of course — but experience shows us that breaches will continue to occur. AI can help to remediate breaches in multiple ways.

The same information that was used to allow an email to go through can be reexamined for clues as to the nature of the threat and possibly the identify of attackers. AI can profile attack types, their likely severity, and the scale of response an organization needs to mount. And AI can be used to suggest specific mitigation steps to security professionals.

Much of AI's value will be determined by the training and skill of the people using it. Organizations that move forward quickly in adopting and using AI-powered solutions will be able to maintain and even improve their security posture; others may fall behind.

AI could be used to, for instance, help verify that emails that appear to come from a given domain were indeed generated and processed by servers at the company or other organization in question. This kind of handshaking could serve as a digital signature to label and identify "known good" vs. suspicious organizations.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Focusing on email's role in XDR Strategy
- Using telemetry to enable XDR
- Describing the features that make XDR effective

Chapter 4
Understanding the Role of Email Security in XDR

The reason that email is so important to attackers is that it connects the vast majority of a company's employees to each other and to the systems that run your business. Email credentials are even used for identification in company systems that have nothing directly to do with email.

Because email is the hub of so many interconnections, an email security approach is unlikely to be effective if it only works to secure email interactions. Instead, email security is the central, but not the only, component in a security approach called extended detection and response, or XDR. XDR includes a range of components that work together to provide a holistic approach to securing a company's information, systems, and other assets.

Artificial intelligence (AI) and machine learning (ML) are a crucial technological platform within a comprehensive security solution. A solution with a wide range of customers has the opportunity to build in what it learns from a single attack to enhance the protection available to all customers. Attackers soon learn that new insights and approaches quickly become ineffective when used against targets who have the most advanced email threat response solutions in place.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

This chapter discusses some of the core elements that make up an email security solution such as Cisco's Secure Email Threat Defense offering. It also describes how *telemetry* — detection and measurement of threat-related indicators — ties together threat detection at all levels. Finally, the chapter covers how the features of Cisco's XDR offering help to make it effective in reducing the number of breaches and mitigating the impact of breaches when they occur.

The Role of Email in XDR Strategy

Email security plays a crucial role in an overall XDR strategy. And Cisco provides an industry-leading product, Cisco Secure Email Threat Defense. Secure Email Threat Defense is designed to be effective against many kinds of threats, with an emphasis on those that have the most potential to cause damage.

An example of the kind of response that the Cisco solution can offer is shown in the area of business email compromise (BEC) attacks (also discussed in Chapter 2). BEC attacks often claim to come from a person within the recipient's company who has a high degree of authority, in an attempt to intimidate the recipient into acting quickly and without questioning the request.

Generative AI is, unfortunately, quite useful in attacks of this type. Generative AI can help people who are skilled in technology but less skilled in English, for example, to create email messages that seem to be legitimate communications from company leaders. And generative AI makes it easy for the attacker to quickly try many subtle variations on email messages in order to find the most effective approaches.

Secure Email Threat Defense helps organizations prepare for these attacks, and to respond effectively when they occur.

Using people profiles to help prevent BEC attacks

Secure Email Threat Defense allows for the creation of lists of high-ranking executives whose identities are likely to be assumed by attackers. This list can be monitored for any activity that might indicate an account takeover so that quick action can be taken to remediate the threat.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Getting a deeper understanding of threats

Both BEC attacks and phishing emails can combine several malicious tactics in a single email, or in an attack that combines the use of email and other modalities, such as text messages and phone calls.

In recent years, Cisco's Secure Email Threat Defense has introduced a new threat detection engine that provides deep context and understanding of the level of business risk for each threat. The details displayed with each verdict empower security professionals to make informed and rapid decisions about what next steps will best protect their organization.

Seeing How Telemetry Enables XDR

Telemetry simply means transmitting (the *tele* part, as in the words telephone or television) some kind of measurement (the *metry* part, also used in phrases such as "the metric system"). An example is readings from various sensors.

Telemetry is used in a specific way in email security and solutions such as XDR. There are six telemetry sources used:

- **Email:** The email message includes the content of the message body and metadata, such as the sender, receiver, and path followed by the email.
- **Identity:** Identity servers note the identity of email senders and recipients and others involved in communication.
- **Endpoints:** Endpoints are points where changes occur within a system — the establishment of a network connection, the execution of a command, or the accessing of a file. Endpoint security is an important consideration in security systems.
- **Network:** Internal and external networks transmit information and must be kept both functioning and secure.
- **Firewall:** Firewalls protect an organization from outside inputs that may be dangerous to internal systems or to recipients, such as security attacks or unwanted content.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

» **Domain name server (DNS):** The DNS translates human-readable names, such as `cisco.com`, to IP addresses used by networks to route information.

Each of these telemetry sources is a valuable source of information that may be targeted as part of a cybersecurity attack. So, information from them is vital for identifying valid communications and activities as well as in detecting and deterring attacks.

Each telemetry source will generate one or more kinds of data, and storing the generated data for queries is an important part of the security system's operations. Multiple types of databases and data architectures may be used for managing operational and security-related data.

An advanced XDR solution such as Cisco XDR correlates information from all of these sources and looks for associations. (Associations of this type are valuable inputs to ML models and AI algorithms.) Earlier security solutions would aggregate information from each source, but not correlate information across multiple sources to determine, for example, whether to issue a security alert. The value of an integrated approach to security is shown in Figure 4-1. The integrated approach cuts the risk and cost of security breaches in half while offering large improvements in analyst time spent per incident, security operations (SecOps) efficiency, and dwell time — the window of time in which an attacker has access to what should be a protected environment.

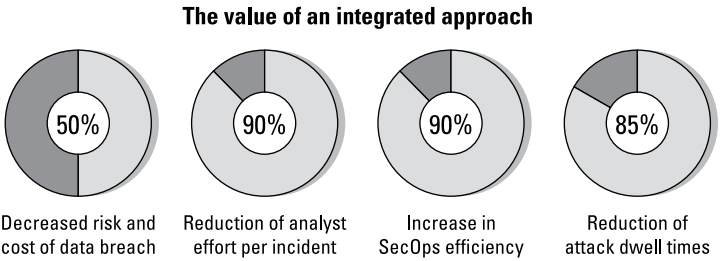


FIGURE 4-1: An integrated approach reduces the risk, cost, and impact of breaches while making the security operations more efficient.

An effective XDR solution provides five elements that demonstrate whether it's effective against the full landscape of threats. Such a system not only provides telemetry; the telemetry is actionable and prioritized, so operators know what to focus on first.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Detection in an effective XDR system is unified; operators are not simply informed of unusual readings from one telemetry source or another, but instead receive the correlations of information that make a report actionable.

An effective XDR solution supports a fast and effective response. Rather than potentially solving the wrong problem — or attempting to solve a problem in the wrong way — an effective XDR solution points the way to effective responses.

An effective solution also offers a single view of the system and potential issues. Not only is information combined into a single, integrated system — the famous single pane of glass — but data is designed to make gathering needed information faster and decision-making more effective.

And finally, an effective solution can help an organization improve its productivity and practices over time. As operators learn how to make the most of the system, they're able to identify the best response, reduce response time, and reduce both the frequency of breaches and the impact of those that do occur.

Learning How Features Make XDR Effective

The features of an XDR offering are what make it effective against cybercriminals. Features available in all Cisco XDR solutions include:

- **Security analytics and correlation engine:** The engine ingests event information and telemetry and uses advanced technology such as AI and ML to detect and help in responding to threats.
- **Threat intelligence:** Intelligence here refers to the capability to combine many sources of threat information with Cisco's built-in Talos Intelligence resources.
- **Threat hunting:** Threat hunting allows operators to proactively search for threats and either prevent them or mitigate damage before their severity increases.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Incident response actions:** A predetermined set of actions allow analysts and responders to mount the right response with no hesitation, preventing many breaches and limiting the impact of others.
- **Incident prioritization:** Incidents can be scored for greater or lesser urgency of response, with information enriched to provide breadth, depth, and context, and kept up to date as attacks unfold.
- **Asset and user context:** Context helps with understanding, prioritizing, and responding to incidents.
- **No-code and low-code workflows:** Workflows can be created with little or no code, making operators more effective and reducing the potential for errors.
- **Workflow exchange:** Existing workflows can be easily shared, installed, and put into operation.
- **Cisco Software Support Service (SWSS) Enhanced:** Users get around-the-clock support and a 30-minute service level agreement (SLA) for response and additional services.

There are also advanced features available to take your organization's security capabilities even further:

- **Third-party integrations:** Cisco XDR solutions are extensible, and third-party integrations are available as an advanced feature.
- **Cisco Talos Incident Response (Talos IR):** Talos is one of the most advanced security services available anywhere, offering a full set of services, both proactive and responsive/emergency services.
- **Cisco Managed Detection and Response:** This is a managed XDR service with select Talos IR services.
- **Cisco Technical Security Assessment:** An assessment can help an organization understand its unique vulnerability and capability profile and become more effective in preventing and mitigating breaches.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Using multiple techniques for threat defense
- Understanding the importance of acting
- Taking the opportunity to try a solution yourself

Chapter 5
Ten Ways to Protect Against Advanced Email Threats

Email threats take many different forms, exploiting weaknesses in everything from technical infrastructure to human psychology. Here are ten ways to help prevent most attacks and recover quickly when breaches do occur.

There's no single solution to preventing and mitigating security breaches that originate in email. Each of the steps mentioned here augments and reinforces the others. For instance, the more threats you stop, the more capacity you have to handle each breach that does occur; categorizing threats also helps you to respond effectively to those instances when a threat becomes a breach.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Use Secure Email Threat Defense to Respond Quickly and Effectively

Cisco Secure Email Threat Defense is your first line of, well, defense against threats. It automatically and reliably does many of the things that you might wish users would do consistently, such as:

- Assess the sender's reputation
- Asses the reputation of the email's source URL
- Scan content for concerning words and phrases
- Scan file attachments and analyze their reputation and content
- Spot and block spam
- Integrate the latest updates from Talos, the largest global provider of security research and intelligence

And it also does so much more. Cisco Secure Email Threat Defense works as an integral part of your overall Extended Detection and Response (XDR) strategy.

Optimize Your Defenses Against Major Email Threats

Every company faces a different security threat profile, so you and others at your company play a vital role in making Secure Email Threat Defense and other tools work for you.



REMEMBER

You can scan the horizon for current threats and note what threats are being blocked — or causing breaches — at your company. You can then respond by working with Cisco as your vendor; working with your email provider; training your security personnel and end users; educating upper management; and many more steps. "Forewarned is forearmed," the old saying goes, and you can help your company dodge most threats and move quickly and effectively to heal breaches when they occur.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Use AI and Advanced Threat Analysis to Understand and Categorize Threats

Unfortunately, AI is playing an increasingly large role in mounting threats against your company's security. But fortunately, AI is also becoming a more and more important part of threat response.

AI is strategically integrated into Secure Email Threat Defense and Cisco XDR offerings. AI is particularly good at taking vast amounts of input — such as the extensive telemetry provided by Cisco solutions — and using AI to identify patterns that serve as indicators of an attack.


TIP

These patterns are often so subtle that attackers aren't aware of the breadcrumbs they're leaving as they put together attempts at exploits. AI can spot these patterns before the bad actors do. An integrated offering such as Cisco's can also help to take the information from a small number of breaches and use it to enhance protection for many, many other users. The expansive telemetry provided by the broad Cisco product security suite ensures that understanding the risk level and context of threats helps to minimize attack damage.

Use Threat Data to Inform and Expedite Your Response

Before a threat arrives, you can know:

- What the recent patterns of threats look like
- The signatures left by different kinds of threats
- What attacks are leading to successful breaches
- The best response to each different kind of breach

By using threat data, you help yourself at every step of the "funnel" of security breaches: reducing the number of attacks that reach user inboxes, reducing the impact when a malignant email is opened or a toxic file attachment is downloaded, and responding quickly and effectively to the remaining breaches that do occur.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Act Quickly to Ensure Maximum Protection Against Threats

By acting automatically against many threats, and by providing alerts and information about the threats that do appear, Cisco email security solutions give you a precious gift in responding to any remaining breaches: time.



REMEMBER

With Cisco solutions in place, your best people are empowered to respond quickly and effectively to the breaches that do occur, while directing their focus to strategic efforts such as studying the breach, understanding how it occurred, and taking the steps needed to prevent a recurrence. Together, your people and your systems become more effective and more responsive.

Use Cisco XDR for Protection and Defense Against Advanced Threats

Cisco XDR solutions augment the protection provided by Secure Email Threat Defense. With Cisco XDR, you can bring together, bolster, and maximize the best efforts of many different types of professionals in your organization to help create an improved security posture. Some Cisco offerings include advanced features such as third-party integrations to help ensure the best possible fit with your organization and its unique needs.

Cisco XDR solutions can help take you from a reactive security posture to a proactive one, raising your email and associated cybersecurity responsiveness to best-in-class levels and freeing up resources for further improvements.

Unify Visibility Across Control Points

"That which gets measured gets done" is a longstanding management mantra, and you can only measure what you can observe.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cisco security solutions help you unify visibility across multiple control points so you can, for instance, tie the damage that's occurring from a successful breach to the original gaps in your defenses that allowed it to occur. You can then "mind the gap" and prevent the problem from recurring in the future.

Embrace Automated Tools to Maximize Resources

Your most precious resource is your people. If they're tied up chasing minor or repetitive problems, they're not free to be proactive, working to prevent breaches and to minimize damage when breaches occur.

Automated tools save your people's time and focus for the largest potential threats. These tools also allow your team to find a solution and then "set it and forget it," using the automated tools to prevent the same problem from happening again.

Finally, automated tools enhance the job satisfaction of your people, ensuring them that they have the means to take on the ever-changing challenges presented by cybersecurity breaches. You can earn a reputation as a nimble and effective organization, enhancing your appeal to the most talented professionals who want to work with the latest and best tools.

Detect Sooner, Respond Faster

You can't solve a problem you don't know you have — and most cybersecurity breaches get worse the longer it takes you to respond. Cisco email security solutions buy you time, removing some threats and giving you early notice of others.

This gives you the opportunity to put more resources toward prevention and to require less effort for mitigation. You experience less damage from breaches and have more time and focus to devote to further improving your defenses, rather than repairing the damage from past problems.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Try Secure Email Threat Defense

You can experience a 30-day free trial of Cisco Secure Email Threat Defense to protect you against a broad array of advanced email threats. Sign up today through the free trial page at:

https://www.cisco.com/c/en/us/products/security/email-threat-defense-free-trial.html

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



Experience Simplified

Ensuring the highest levels of protection from advanced email threats means deploying a state of the art extended detection and response solution like Cisco XDR. The telemetry from Secure Email Threat Defense, other Cisco security products, and select third-party tools unifies visibility and streamlines incident response.

See how Cisco XDR brings you from investigation to remediating the highest priority incidents with greater speed, efficiency, and confidence.

© 2024 Cisco and/or its affiliates. All rights reserved.

Protect your most important business communication tool — email

Email security is an increasingly important topic. Artificial intelligence (AI) has both expanded the sophistication of attacks and enhanced the protections available to defend against them. But organizations have to understand the new and enhanced threats, and the changes to what's possible on the responsive side, to halt as many attacks as possible. This book explains the broad range of security challenges that can find their way to email accounts and how AI both increases the challenges and also offers solutions.

Inside...

- The impact of AI on threats
- Ten ways to defend against advanced email threats
- Using telemetry to enable XDR
- The importance of a platform approach
- How Cisco solutions can help



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

ISBN: 978-1-394-25296-1
Not For Resale



for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

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