Brought to you by:

ATTACKIQ

MITRE ATT&CK®

for dummies®

A Wiley Brand

Implement ATT&CK for effective cybersecurity

Execute a threat-informed defense strategy

Optimize your cybersecurity program

Jonathan Reiber

Carl Wright

AttackIQ Special Edition

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat Informed Defense.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

MITRE ATT&CK®

AttackIQ Special Edition

by Jonathan Reiber and Carl Wright

for dummies®
A Wiley Brand

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

MITRE ATT&CK® For Dummies®, AttackIQ Special Edition

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

Copyright © 2021 by John Wiley & Sons, Inc.

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. AttackIQ and the AttackIQ logo are trademarks or registered trademarks of AttackIQ or its subsidiaries in the United States and other countries. 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: THE PUBLISHER AND THE AUTHOR 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 WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

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: 978-1-119-74809-0 (pbk); ISBN: 978-1-119-74810-6 (ebk) Some blank pages in the print version may not be included in the ePDF version.

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 Manager: Carrie Burchfield-Leighton

Acquisitions Editor: Ashley Coffey

Sr. Managing Editor: Rev Mengle

Business Development Representative: Molly Daugherty

Production Editor: Siddique Shaik

AttackIQ's Acknowledgments

The MITRE ATT&CK team's analytic content inspired or formed the basis of the majority of the writing in this book. AttackIQ offers its profound thanks to the entire MITRE ATT&CK team and the Center for Threat-Informed Defense for their close partnerships in creating this book. MITRE has built a transformative framework for cybersecurity, and as public servants and cybersecurity professionals, we believe that the ATT&CK framework is materially improving the world's cybersecurity posture — making the world a safer place for compute. We're glad to do our part to spread knowledge about MITRE ATT&CK through this book and also through AttackIQ Academy's free courses on threat-informed defense, breach and attack simulation, and MITRE ATT&CK. For more on MITRE ATT&CK and AttackIQ Academy, visit attack.mitre.org and academy.attackiq.com.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Table of Contents

FOREWORD v

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

CHAPTER 1: **Understanding MITRE ATT&CK and Cybersecurity** 3
Identifying What MITRE ATT&CK Is 4
Using Threat Intelligence and MITRE ATT&CK 6
Deploying a Threat-Informed Defense and ATT&CK 8

CHAPTER 2: **Using Threat Intelligence and Threat-Informed Defense** 9
Level 1: Using CTI with Limited Resources 10
Level 2: Working with a More Developed Team 10
Level 3: CTI with an Advanced Team 12

CHAPTER 3: **Building Detection and Analytics** 13
Level 1: Limited Resources 13
Understanding analytics 14
Incorporating analytics into your SIEM 14
Level 2: Using Analytics on a More Developed Team 16
Level 3: Using Analytics on an Advanced Team 16

CHAPTER 4: **Conducting Emulations and Purple Teaming** 19
Level 1: Adversary Emulation with Limited Resources 19
Level 2: Adversary Emulation with Moderate Resources 21
Level 3: Adversary Emulation on an Advanced Team 22

CHAPTER 5: **Developing Assessments and Engineering** 25
Level 1: Conducting Assessments with Limited Resources 26
Level 2: More Advanced Analytics and Engineering 27
Level 3: Advanced Analytics and Engineering 29

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

CHAPTER 6: **Making MITRE ATT&CK Operational** 31
Moving from Threat Intelligence to Threat-Informed Defense 31
Mapping Success across the Organization 32

CHAPTER 7: **Looking at a Use Case: Leveraging MITRE ATT&CK in the Financial Sector** 35
Meeting the Firm 35
Defining the Threats 36
Understanding Your Adversaries 36
Making ATT&CK Useful 37
Seeing the End Result 38

CHAPTER 8: **Ten Ways to Apply the MITRE ATT&CK Framework** 39
Cyberthreat Intelligence 39
Automated Testing and Auditing 40
Security Risk Management and Strategy 40
Regulatory and Compliance Mapping 40
Security Control Rationalization 41
Analyst Training and Exercises 41
Threat Hunting 41
Commercial Security Solutions Evaluations 41
Security Pipeline Validation 42
Business Enablement 42

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Foreword

When I arrived at MITRE in the summer of 2017, it was clear that MITRE's ATT&CK framework was already a big deal and on its way to being a game changer. But as impressive and useful as ATT&CK was (and is), what really struck me was the global community that sprung up around the framework. This organic movement, spurred by innovative security professionals who understand the importance of having a common foundation, was something that *everyone* can freely use and reference. The other thing that became increasingly clear was that this community was evolving a set of practices that took the knowledge on adversary tradecraft in ATT&CK and used it to improve their organization's defenses. Like the community itself, this evolution takes place in the daily course of individuals and organizations discovering what works (and what doesn't) and sharing that with others in the community.

But in spite of all the individual efforts we were seeing, there wasn't a succinct way to talk about the set of related activities and practices that were being shaped and refined by the people on the front lines of cyberdefense. Whether it was using ATT&CK as a lens to view and assess an organization's security posture, or building detections based on an adversary's *behaviors* rather than indicators, or taking the adversary's own playbook and using that to test whether its defenses would hold, the talented individuals evolving these approaches were, as I saw it, all shaping a new discipline.

That's the thinking behind a new discipline — *threat-informed defense*. This book helps you take the first steps in your own journey of using ATT&CK and implementing a threat-informed defense, which is your best chance to change the rules of the game on the adversary.

Richard Struse

Director, Center for Threat-Informed Defense at MITRE Engenuity

Washington, DC; November 2020

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

How can you ensure that your cybersecurity capabilities are working to defend your organization's data as best they can? Even after decades of investment in people, processes, and technology, this question haunts chief information security officers and security leaders at organizations all over the world. Despite billions of dollars spent, intruders still break through, security controls falter, and defenses fail to prevent data theft and destruction from occurring. How can security teams change the story to improve their cybersecurity effectiveness? Instead of simply trying to close every vulnerability, meet every security standard, or buy the "best" commercial technology, defenders can change the game by focusing their defenses on probable, known threats that are most likely to attack the organization.

The way to begin is with MITRE ATT&CK.

About This Book

Welcome to *MITRE ATT&CK For Dummies*, AttackIQ Special Edition. The purpose of this book is to help you take practical steps for deploying ATT&CK as a framework to maximize your security effectiveness. Each chapter helps you deploy MITRE ATT&CK into your security program at various stages of maturity, whether you're a small security team with limited resources or a more mature security program within a large enterprise. This book has an overarching mission in mind to make the most of scarce budgetary resources, drive down complexity for security leaders, and increase security effectiveness and efficiency. From there, the content is structured around a number of key initiatives for implementing MITRE ATT&CK.

Icons Used in This Book

Throughout this book, special icons alert you to important information. Here's what to expect:

This icon highlights information that's important to know. Tips can help you do things quicker or easier.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

This icon calls out information that's helpful to remember.

WARNING

Information contained here points out struggles you want to avoid in deploying MITRE ATT&CK.

TECHNICAL STUFF

If you like to know the technical details about a topic, watch out for this icon. It provides you with all the specialized, juicy details.

Beyond the Book

We can only pack so much information into the short 48 pages of this book, so in this section, we've given you some additional resources to peruse for more information. Discover more information on MITRE ATT&CK and how to deliver a threat-informed defense at the following:

- **`https://academy.attackiq.com/`:** Free training in how to operationalize MITRE ATT&CK, use breach and attack simulation, and run purple team operations
- **`attackiq.com/solutions`:** Automated security control validation solutions
- **`attack.mitre.org`:** Info on the full MITRE ATT&CK framework
- **`mitre-engenuity.org/center-for-threat-informed-defense`:** Key resources for deploying an effective threat-informed defense
- **`attack.mitre.org/mitigations/enterprise`:** Tools to deploy to defend yourself
- **`academy.attackiq.com/courses/intro-to-fin6-emulation-plans`:** Building an adversary emulation plan with MITRE's FIN6 emulation plan

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Defining MITRE ATT&CK
- Using threat intelligence and MITRE ATT&CK
- Understanding threat-informed defense and ATT&CK

Chapter 1
Understanding MITRE ATT&CK and Cybersecurity

Cybersecurity matters for the health and safety of our societies. Software underpins everything from your smartphones to the cars you drive to the global financial system. Dependence on cyberspace for daily life is matched only by the vulnerability it brings: Computer code has turned every part of civilization into a potential target. Adversaries across the globe, from nation-states to criminal organizations, hold your businesses, democracy, and society at risk through cyberspace. They steal intellectual property and financial resources, disrupt critical infrastructure operations from energy systems to weapons platforms, and manipulate socio-political narratives to provoke mistrust in democratic processes and institutions.

The world hasn't stood by flat-footed as cyber threats have increased against your interests. In recent years, the cybersecurity community has matured its approach to understanding adversary

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

behavior to better defend the networks and data of cyberspace. Traditionally, network defenders focus their defensive strategies on meeting baseline cybersecurity best practices, which are correcting misconfigurations, administering patches, and deploying best-in-class commercial products. This approach tends to focus on meeting standards and, for detecting and remediating attacks, on finding intelligence and analysis-driven indicators of compromise, which is information in the code that indicated the presence of an adversary inside a network. This fortress mentality focuses on two aspects: building better walls to keep the enemy out and on understanding signs of adversary intrusion. Both are valuable. Both are necessary. Yet they're insufficient for an effective cyberdefense strategy.

In this chapter, you discover the basics around MITRE ATT&CK and how you get started using threat intelligence and MITRE ATT&CK and deploying a threat-informed defense and ATT&CK.

Identifying What MITRE ATT&CK Is

Today, the cybersecurity community is evolving from the fortress mentality to a threat-informed defense approach, and MITRE ATT&CK is at the center of this transition. A threat-informed defense strategy applies a thorough understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyberattacks. From nation-states to criminal groups, ATT&CK directs teams to focus on

- A library of known adversary tactics — the adversary's technical goals
- Techniques — how those goals are achieved
- Procedures — specific implementations of the techniques

With the knowledge ATT&CK provides, teams can shift from an ad hoc approach of meeting cybersecurity regulations to countering known, dangerous threats.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

WHAT MAKES THE ATT&CK FRAMEWORK SO IMPORTANT?

Prior to MITRE releasing ATT&CK, there was no single, holistic repository of adversary TTPs. Elite and national security operators were largely focused on forensic, historical attributes of adversary intrusions, such as code that proved the adversary had already been inside the network; the nature of these signatures and indicators of compromise meant that organizations were constrained by needing to protect their intelligence sources and methods, and that made it harder for them to share information broadly.

The "kill-chain" methodology, first developed by Lockheed Martin in 2011, maps out the specific phases that an adversary follows, step-by-step, as it approaches an asset to attack, from reconnaissance to weapons deployment to command and control to actions on the objective. By understanding the kill-chain (a term originally coined in the military), defenders can better position their security controls to mount an effective defense.

While Lockheed Martin pioneered the kill-chain methodology, MITRE studied adversary TTPs in depth and built out the framework for the broader public to help defenders focus on the threats that matter most. Since then, the framework has gained significant momentum in the public and private sectors as a globally vetted, all-source repository of adversary threat behaviors.

ATT&CK has been received tremendously well by the public and private sectors. As one indicator, in the summer of 2020, the office of the Prime Minister of Australia referenced the importance of the ATT&CK framework in the face of escalating nation-state attacks against Australian infrastructure by highlighting the Australian government's ATT&CK-focused approach. This public statement by a head of state reflects the broad adoption of the framework as a global standard. In the private sector, customers derive deep value from the ATT&CK framework. One AttackIQ customer said ATT&CK gave it the ideal framework to meet its target use cases, and it could continually validate the performance of its production system security controls in real time.

ATT&CK transforms organizations from taking an ad hoc approach to security operations to adopting a data-driven, threat-informed approach — and it has caught on globally.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TECHNICAL STUFF

The MITRE Corporation, a federally, funded, non-profit research and development organization working in the public interest, built the ATT&CK framework to help defenders all over the world to pivot away from a passive defense and to focus on the threats and threat behaviors that mattered most. Launched in 2015, ATT&CK provides a clear framework for defenders to use cyberthreat intelligence (CTI) about known actors, to deploy adversary behaviors against their defenses to test and validate their effectiveness, and to make changes to fix misconfigurations or fill defensive gaps. ATT&CK is a globally available, *free,* open framework of known adversary tactics, techniques, and procedures (TTPs). ATT&CK helps the public focus on known TTPs to better defend their data.

Using Threat Intelligence and MITRE ATT&CK

The foundation of the work hinges on CTI provided by the ATT&CK framework and the CTI your team develops, either from its own forensic work or from external sources available either from vendors or open-source intelligence.

ATT&CK is a framework outlining the probable tactics that adversaries use to deploy against your enterprise. To use threat intelligence and MITRE ATT&CK, you must first understand the adversary by studying its behaviors. After that, you focus on which adversaries target *your* sectors and the TTPs they use. From there, you can build threat intelligence to prepare your defenses against adversary TTPs.

After you understand how to use CTI, you begin the process of integrating analytics. Within your enterprise, you have event logs, scripts, and cybersecurity capabilities that track adversary behavior. You can collect the information about adversary TTPs into your security information and event management (SIEM) tool to then run analysis about adversary tactics and assess results about the adversary's behavior. This process requires that you write detections, revise to filter out false positives, and ensure search detections. It takes work, but, step by step, you build your analysis and detection capabilities.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Train your teams on how to detect and analyze adversaries, how adversary tactics can impact your team, and how your defense operations respond to incoming threats. It's not enough just to know what adversaries will do; you need to build data about the adversaries' behaviors into your cyberdefense platform.

To improve your organization's security posture, you create teams to tackle different threats. These teams are as follows:

- **Blue teams:** Historically, blue teams are defensively focused teams that concentrate on securing a network and its associated data. Often working inside a security operations center (SOC), blue teams track security incidents, manage security technologies, and administer security controls for the organization, among other defensive responsibilities.
- **Red teams:** Red teams, or *penetration teams,* adopt an adversarial approach to test the blue team's defenses. Red team testing is episodic, and the coverage delivered is vastly smaller than the scale of the blue team's defenses. Blue teams are larger and cost more than red teams.
- **Purple teams:** In a purple team, the functions of the red and blue teams are tightly coupled and execute in a coordinated fashion to provide immediate and continuous improvement to the overall security program. Purple teams adopt a combined red/blue approach, thinking like an adversary and testing defensive technologies continuously from an adversary perspective.

Over time, you can run adversary emulations using ATT&CK as a base and direct different teams to assess your security performance against adversarial TTPs. You can integrate blue and red teams to run combined operations in a purple team with ATT&CK as a base. This process follows these steps:

1. **Select an adversary technique from ATT&CK or your own library of threat intelligence.**
2. **Choose a test of the technique.**
3. **Exercise the test procedure.**
4. **Analyze how your detections perform.**
5. **Improve your defenses on the basis of performance.**

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

This process requires that you assess how your defenses perform, identify your gaps in coverage, determine how to close the gaps, and then modify your defenses accordingly. Blue and red teams work closely together in the process and work across the security operations center to detect and prevent attacks from succeeding.

Deploying a Threat-Informed Defense and ATT&CK

You can operationalize ATT&CK by using a breach-and-attack simulation platform for continuous, automated security control validation safely, in production environments, and at scale across your enterprise. Security controls are the people, processes, and technologies that defend your network against intrusions, and these controls often fail for two reasons: user error and misconfiguration.

TECHNICAL STUFF

Even after decades of cybersecurity investment, 82 percent of enterprise breaches should've been stopped by existing security controls but weren't.

The only way to know if security controls are working at any point in time is to test them. To solve this problem, in the past, security teams used red teams (penetration teams) to test their defenses, but they were sporadic and unable to scale across the enterprise. A penetration test conducted six months ago against less than one-tenth of your enterprise's total security controls tells you nothing about the effectiveness of your cybersecurity platform *today*.

With ATT&CK as a foundation, you can direct your security teams to focus their security controls on the most probable methods of adversary attack. Continuous, automated testing allows teams to ensure that security controls are focused on what matters most and to verify that they are effective. Automation generates real performance data from across your enterprise that your security teams can use to improve your overall effectiveness.

For a deeper dive into automated adversary emulations and threat-informed defense operations, visit MITRE Engenuity's Center for Threat-Informed Defense at `mitre-engenuity.org/center-for-threat-informed-defense`.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

» Identifying known and unknown threats

» Developing threat intelligence

Chapter 2
Using Threat Intelligence and Threat-Informed Defense

The ATT&CK framework can be useful for any organization that wants to move toward a threat-informed defense strategy.

TIP

You can benefit from threat intelligence and MITRE ATT&CK in the following ways:

- Identify key hostile actors, using a globally vetted framework.
- Gain insight into adversaries' operational behavior to analyze how that impacts your cyberdefenses.
- Deepen your approach by comparing your results to other analysts.
- Strengthen your defense teams by focusing on countering known hostile actors.

In this chapter, we share ideas for how to start using cyberthreat intelligence (CTI) for a team of any sophistication.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

DEVELOPING THREAT INTELLIGENCE

The point of intelligence is to make information actionable for security practitioners. So how do you do it? You start by finding a group that has targeted your sector and against whom you want to be able to defend yourself. Then you share it with your defenders. Check out the ATT&CK website (`attack.mitre.org`) for ideas to get you started with detection and mitigation of techniques.

Level 1: Using CTI with Limited Resources

CTI is about what your adversaries do and using that information to improve your security program's effectiveness against known threats and threat behaviors. For an organization with only a few analysts that wants to start using ATT&CK for CTI, one way to start is by taking a single group of threat actors and looking at its behaviors as they're structured in ATT&CK. You might choose a group from those on MITRE's website, based on organizations previously targeted. Alternatively, many threat intelligence subscription providers also map to ATT&CK, so you could use their information as a reference.

If you visit `attack.mitre.org`, you can find the threat actor you're concerned about and look at the techniques it has used (based solely on open-source reporting that MITRE has mapped) to learn more. If you need more information on the technique, it can be found on the ATT&CK website. You can repeat this for each of the samples MITRE has mapped for the group, which MITRE tracks at `attack.mitre.org/software`.

Level 2: Working with a More Developed Team

If you have a team of threat analysts who regularly review information about adversaries, you can elevate your use of ATT&CK to the next level. You can map intelligence to ATT&CK yourself

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

rather than using what others have already mapped. If you have a report about an incident on which your organization has worked and generated intelligence, this can be a great internal source to map to ATT&CK. You can also use external reports, like a blog post.

TIP

We realize mapping to ATT&CK can be intimidating when you don't know all the hundreds of techniques available. The following steps can help you:

1. **Understand ATT&CK.**

   Familiarize yourself with the overall structure of ATT&CK: tactics, techniques, and procedures (TTPs). Take a look at available online resources.

2. **Find the behavior.**

   Think about the adversary's action more broadly than just the atomic indicator (like an IP address) used.

3. **Research the behavior.**

   If you're not familiar with the behavior, you may need to do more research. There's a wealth of knowledge available about adversary behaviors through the cybersecurity-threat research community.

4. **Translate the behavior into a tactic.**

   Consider the adversary's technical goal for the behavior and choose a tactic that fits. Good news: Enterprise ATT&CK contains just a handful of tactics. If you pick a SOCKS5 connection as an example, establishing a connection to later communicate would fall under the Command and Control tactic.

5. **Determine what technique applies to a behavior.**

   This step can be tricky, but you can do it by using your own analysis and the ATT&CK website (`attack.mitre.org`). If you search ATT&CK's website for SOCKS, the technique Standard Non-Application Layer Protocol (T1095) pops up. You can find this behavior by looking at the technique description. If searching the keyword fails to help, you can focus on the techniques ATT&CK shows for the tactics you identified in Step 4 to see where the behavior matches.

6. **Compare your results that of analysts.**

   You may have a different interpretation of an adversary's behavior than another analyst. This is normal, and we recommend comparing your ATT&CK mapping to others' and discussing any differences.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

For the CTI teams that have a few analysts, mapping information to ATT&CK can be a good way to ensure you're getting information to meet your organization's requirements. From there, you can pass the ATT&CK-mapped adversary information to your defenders to inform their defense.

Level 3: CTI with an Advanced Team

If you have an advanced cyberintelligence team, you can start to map more information to ATT&CK to prioritize your enterprise defense. You can map both internal and external information to ATT&CK, including incident response data, open-source intelligence (OSINT), intelligence subscriptions, real-time alerts, and your organization's information.

After you've mapped this data, you can compare groups and prioritize commonly used techniques. Use the MITRE framework Navigator function and substitute the groups and techniques you care about based on your organization's top threats. You can then aggregate the information to determine commonly used techniques, which can help defenders prioritize actions for detection and mitigation. After the defenders have conducted an assessment of what they can detect, you can overlay that information onto the information you know about threats. This is a good place to focus your resources: It reveals defensive gaps against known threats, and known threat behaviors to align resources against.

On the basis of adversary known techniques, you can develop a heatmap of known adversary tactics that shows the most important techniques in a color-coded fashion on the ATT&CK Navigator. MITRE experts developed a "top 20" list of techniques. Your team could create your own top 20.

REMEMBER

This practice of cybersecurity is both an art and a science. This process of mapping ATT&CK techniques to your defenses isn't perfect, but it can still help you gain a clearer picture of what adversaries will likely do to target your enterprise. For an advanced team seeking to use ATT&CK for CTI, mapping sources to ATT&CK can help you build a deep understanding of adversary behavior and build a threat-informed defense.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Understanding analytics
- Incorporating outside analytics into your SIEM
- Analyzing your security effectiveness

Chapter 3
Building Detection and Analytics

Building analytics to detect ATT&CK techniques may be different from detection. Rather than identifying things that are known to be bad and then blocking them, ATT&CK-based analytics involves collecting log and event data about the things happening on your systems and using that data to identify suspicious behaviors described in ATT&CK.

In this chapter, we talk about how to build detections for adversary behavior. We break this down by levels. This chapter builds on Chapter 2 to show you not only that you can understand what the adversary can do via cyberthreat intelligence (CTI) but also that you can use that intelligence to build analytics to detect those techniques.

Level 1: Limited Resources

This section helps you to understand how to analyze threat intelligence in relation to your defensive capabilities to adjust your defenses and achieve security effectiveness.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Understanding analytics

The first step to creating and using ATT&CK analytics is to understand the data and search capabilities you already have. To find suspicious behaviors, you need to be able to see what's happening on your systems. One way to do this is to look at the data sources listed for each ATT&CK technique. They describe the types of data that give you visibility into the technique; they give you a starting point for what to collect.

If you look through the sources, several can help you detect a number of the following techniques:

- **Process and command line monitoring:** Often collected by Sysmon, Windows Event Logs, and many endpoint detection and response (EDR) platforms
- **File and registry monitoring:** Also often collected by Sysmon, Windows Event Logs, and many EDR platforms
- **Authentication logs:** Collected from the domain controller via Windows Event Logs
- **Packet capture:** Includes east/west capture such as that collected between hosts and enclaves in your network by sensors such as Zeek

Incorporating analytics into your SIEM

After you know the data you have, you need to collect that data into some kind of search platform — a process known as *Security Information and Event Management*, or SIEM — so you can run analytics against it. You may already have this as part of your IT or security operations, or it may be something new you need to build. Don't underestimate the steps in this process; tuning your data collection is often the hardest part.

TIP

Need access to a good enterprise dataset for testing? Check out the Boss of the SOC (security operations center) dataset from Splunk (`github.com/splunk/botsv2`) or the BRAWL dataset from MITRE (`github.com/mitre/brawl-public-game-001`). Both are available as JavaScript Object Notation (JSON), a standard text-based format for representing structured data based on JavaScript object syntax. It also can be loaded into Splunk, ELK, and other SIEMs. BOTS is

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

extensive and contains real noise, while BRAWL is much more constrained and focuses only on the red team activity.

After you have data loaded in your SIEM, you're ready to try some analytics. One starting point is to look at analytics created by others and run them against your data. Try these:

- **Cyber Analytic Repository (CAR):** MITRE's repository of analytics at `car.mitre.org/analytics`
- **ThreatHunter Playbook:** A repository of strategies to look for ATT&CK techniques in log data at `threathunterplaybook.com/introduction.html`
- **Detection Lab:** A set of scripts to set up a simple lab to test analytics at `github.com/clong/DetectionLab`
- **BOTS:** Splunk's Boss of the SOC dataset with background noise and red team attacks at `github.com/splunk/botsv2`
- **BRAWL Public Game:** MITRE's red team dataset at `github.com/mitre/brawl-public-game-001`
- **ATT&CK Navigator:** A tool to visualize data on the ATT&CK matrix, including analytic coverage at `github.com/mitre-attack/attack-navigator`

REMEMBER

Make sure you read and understand the description in each analytic to identify its target, but the pseudocode at the bottom of the chart is the important part. Translate that pseudocode into a search for whatever SIEM you're using (making sure the field names in your data are correct), and you can run it to get results. *Note:* If you're not comfortable translating the pseudocode, you can also use an open-source tool called Sigma and its repository of rules to translate to your target. Look through each result and figure out whether it's malicious. If you're looking at your own enterprise data, it's hopefully benign or known red team data — but if not, it's time to figure out what you have going on.

TIP

After you have the basic search function returning data and you feel like you understand the results, try to filter out the false positives in your environment so you don't get overwhelmed. Your goal is to reduce false positives as much as possible while ensuring that you can catch malicious behavior; your goal isn't to get to zero false positives. After you've configured the analytic to a low false-positive rate, you can have it automatically create a ticket in your SOC each time the analytic fires, or you can use it from the library for manual threat hunting.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Level 2: Using Analytics on a More Developed Team

After you're enabled by analytics that other people wrote for their operations, you can start expanding your threat coverage by writing your *own* analytics. This process is complicated and requires understanding how attacks work and how they're reflected in the data. To start, you can look up the technique description from ATT&CK and the threat intelligence reports.

After you look at how adversaries use the technique, figure out how to run it yourself so you can see it in your own logs. To do that, follow these steps:

1. **Use an open-source tool for atomic tests that include red team content aligned to ATT&CK.**

   If you're already doing red teaming, feel free to run the attacks you know yourself on systems where you have permission and try to develop analytics for them.

2. **After you've run the attack, look inside your SIEM to see what log data was generated.**

   At this stage, you're looking for things that make this malicious event look distinctive. A general pattern to follow is to write the search to detect malicious behavior; revise it to filter out false positives; make sure it detects the malicious behavior; and repeat the filter to reduce other kinds of false positives.

Level 3: Using Analytics on an Advanced Team

The red team is responsible for *adversary emulation* — essentially, trying to evade your blue team analytics by executing the types of attacks and evasions you know from threat intelligence that adversaries use in the real world. You can supplement or replace your red teams with automated adversary emulation plans deployed through breach-and-attack simulation platforms.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

The back and forth between a blue team and a red team around an adversary emulation is known as *purple teaming.* This practice is a great way to rapidly improve the quality of your analytics because it measures your ability to detect the attacks that adversaries actually use. After you get to a stage where you're purple teaming all your analytics, you can automate the process to make sure you don't have any regressions and are catching new variants of attacks.

In the real world, adversaries don't just carry out cookie-cutter attacks copied and pasted from a book. They adapt and try to evade your defenses — including your analytics; that's why there's a defense evasion tactic in ATT&CK. The best way to ensure that your analytics are prepared against evasion is to have a red team deploy against your blue teams. Check out Chapter 1 for details on the kinds of teams.

If you feel confident that you're cranking out quality analytics to detect attacks, it's time to test that confidence and improve your defenses by doing some purple team operations. In practice, adversary emulations work like this:

1. **You have an analytic designed to, say, detect credential dumping.**

   Maybe you write an analytic to detect *mimikatz.exe* on the command line or *Invoke-Mimikatz* via PowerShell.

2. **To conduct a purple team operation against it, give that analytic to your red team.**

   The team can then find and execute an attack to evade your defensive analytic. In this case, the executable may be renamed to *mimidogz.exe.*

3. **Update your analytic to look for different artifacts and behaviors that won't rely on the exact naming.**

   Perhaps you look for the specific *GrantedAccess bitmask* from when *mimikatz* accesses *lsass.exe* (don't worry about the exact details; this is just an example).

4. **Give this example to your red team.**

   The teams execute an evasion that, for example, adds an additional access so your GrantedAccess bitmask no longer detects it. Or you can deploy an automated breach-and-attack simulation tool against your defenses.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

After you're this advanced and are building out analytics, use ATT&CK, either through the ATT&CK Navigator or your own tools, to track what you can and can't cover.

TIP

To track your analytics, you can use a *heatmap*, which is a kind of periodic table of tactics, techniques, and procedures (TTPs), highlighting each TTP in color to determine the degree of defensive coverage you have deployed against the adversary behavior. For an image of a heatmap and instruction on how to use Navigator, visit `www.attackiq.com/mitre-attack`.

You can use a heatmap in the following ways:

- **With single analytics:** As you continue your purple team operations, you can integrate specific analytics from CAR and color them to indicate your coverage. A single analytic is unlikely to provide sufficient coverage for any given technique, but you want to track them.
- **With comprehensive CAR analytics:** Refine the analytics from the preceding bullet and add more from CAR to improve your coverage against those techniques. Eventually, maybe you feel comfortable enough with your detection that you color some of the tactics green. Keep in mind that you will never be 100 percent sure of catching every usage of a given technique, so green will never mean done; it will just mean "okay for now."
- **With CAR and custom developed analytics:** Over time, you'll want to expand the scope of the things you care about and add your own externally or internally provided analytics to deepen your analysis. (Check out Chapter 1 on prioritizing threat actors.) In the end, you want to develop a comprehensive set of detections so you can detect more adversary behaviors; ATT&CK gives you the scorecard to do so.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Conducting adversary emulation at the basic level
- Building on the basics with moderate resources
- Creating a plan with an advanced team

Chapter 4 Conducting Emulations and Purple Teaming

Adversary emulation is a type of red or purple team (we cover this in Chapter 1) engagement that mimics a known threat by deploying known threat intelligence and adversary tactics, techniques, and procedures (TTPs) to test your team's cyberdefense capabilities. Adversary emulation is different from penetration testing and other forms of red teaming. Adversary emulators construct a scenario and the red team (or the automated emulation) follows the scenario while operating on a target network to test how its defenses fare against the emulated adversary. Because ATT&CK is a large knowledge base of real-world adversary behaviors, red teams and platforms use it to build scenarios and adversary emulations. In this chapter, we cover adversary emulations with ATT&CK to demonstrate how you can test the analytics in Chapter 3.

Level 1: Adversary Emulation with Limited Resources

Small teams and those mainly focused on defense can benefit significantly from adversary emulation even if they lack a red team. Many resources are available to help jump-start testing your

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

defenses with techniques aligned to ATT&CK. You can dip your toe into adversary emulation by trying simple tests.

Breach-and-attack simulation companies provide scripts that can be used to test how you detect certain techniques and procedures mapped to ATT&CK techniques. Adversary emulations can be used to test individual techniques and procedures to verify that your behavioral analytics and monitoring capabilities work as expected. A good repository has a directory dedicated to an ATT&CK technique. You can view MITRE's scenario repository in the ATT&CK Matrix (`attack.mitre.org/matrices/enterprise`) and MITRE Engenuity's adversary emulation library here: `github.com/center-for-threat-informed-defense/adversary_emulation_library`.

You start the testing process by selecting the T1135 page to see the details and different types of tests available. Each contains information about the technique, platforms supported, and test execution. After you've executed your first test, look to see if what you expected to detect was what you actually detected. For example, maybe you had a behavioral analytic in your SIEM tool that should have alerted, but you find that it didn't fire, and you determine that the logs weren't correctly exported from your host. You troubleshoot and fix the problem, and now you've made a measurable improvement to improve your chances of catching an adversary using this procedure in the future. Figure 4-1 shows the process.

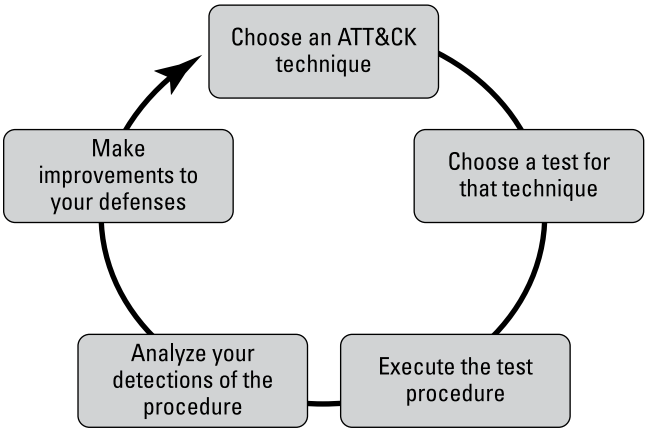

FIGURE 4-1: Adversary emulation and security control validation.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

These tests allow for a laser focus on individual ATT&CK techniques, which makes building ATT&CK-based defensive coverage easier to approach. You can start with a single test for a single technique and expand from there.

Level 2: Adversary Emulation with Moderate Resources

If you already have a red team, you can benefit by integrating ATT&CK with your existing engagements. Mapping red team engagement techniques to ATT&CK provides a common framework for writing reports and discussing mitigations. To get started, take an existing planned operation or tool you use and map it to ATT&CK. Mapping red team procedures to ATT&CK is similar to mapping threat intelligence to ATT&CK, so you may want to check out the recommendations we outline in Chapter 1.

Sometimes mapping techniques can be as simple as searching the command used on the ATT&CK website. For example, the "whoami" command is used in both Unix and in Windows Operating Systems. It displays the name of the current user when executed. If you've used the "whoami" command in your red team operation, two techniques apply:

- System Owner/User Discovery (T1033)
- Command-Line Interface (T1059)

You can map command-by-command actions to techniques with these two examples. To help you do this, MITRE Engenuity's Center for Threat-Informed Defense (`mitre-engenuity.org/ctid`) is building a comprehensive library of adversary emulation plans to empower organizations to test their defenses based on real-world TTPs. MITRE Engenuity is building this library with support from AttackIQ and other industry participants. The scenario library can be found at `github.com/center-for-threat-informed-defense/adversary_emulation_library`. To automate this approach, use an adversary emulation program with deep alignment to MITRE ATT&CK. Armed with your individual commands, scripts, and tools mapped to ATT&CK, you can now plan your engagement.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

WARNING

Some red teams have their tried-and-true toolkits and methods of operation. They know what works because it works all the time. They may not know how their methods overlap with real threat behaviors, however, and that leads to a gap in understanding how well the defenses stack up to what you're actually trying to defend against — the real adversaries targeting your environment.

TIP

Make sure you aren't just doing the techniques because your tool can perform them — emulate a real adversary you care about to provide more value. The analysis can show where opportunities exist to vary your red team's behaviors beyond what it typically employs down to the procedure level. Sometimes a technique is implemented in a particular way in the tools your red team uses, but an adversary isn't known to perform it in that way. ATT&CK helps your red team ensure that it's in line with known threat behaviors.

TIP

As you plan red team operations, you reap rewards by communicating to the blue team about the operation. If you map analytics, detections, and controls back to ATT&CK, you can easily communicate with the blue team in a common language about what you did and how the blue team was successful. Including an ATT&CK Navigator image in a report can help this process and your team to improve.

Level 3: Adversary Emulation on an Advanced Team

In an advanced stage, your red team is integrating ATT&CK into operations and finding value in communicating back to the blue team. To deepen effectiveness, the red and blue teams can work with the CTI team to tailor engagements toward a specific adversary using data they collect and by creating your own adversary emulation plan.

Creating your own adversary emulation plan draws on the greatest strength of combining red teaming with your own threat intelligence: The behaviors reflect the efforts of real-world adversaries targeting *you*. The red team can turn that intelligence into effective tests to show what defenses work well and where resources are needed to improve.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Your security team increases its overall effectiveness with increased visibility and by exposing security-control gaps through testing. Testing allows you to see where and how an adversary would likely succeed. Linking your CTI to adversary emulations increases the tailored effectiveness of your testing and the quality of the data you provide to senior leaders. Real data helps you optimize your security program.

MITRE recommends a five-step process to create an adversary emulation plan:

1. **Gather threat intel.**

   Select an adversary based on the threats to your organization and work with the CTI team to analyze intelligence about what the adversary has done. Combine what your organization knows to publicly available CTI to document adversary behaviors.

2. **Extract techniques.**

   Map the CTI you have to specific techniques in conjunction with your intel team. Point your CTI team to Chapter 1 to help it learn how to do this.

3. **Analyze and organize.**

   Diagram your information into its operational flow in a way that's easy to create specific plans. Check out Figure 4-2 for the phased plan.

4. **Develop tools and procedures.**

   After you know what you want your red team to do, figure out how to implement the behavior. Consider how the threat group used this technique, if the group varied what technique was used based on the environment context, and what tools you can use to replicate these TTPs.

5. **Emulate the adversary.**

   With a plan in place, the red team now has the ability to execute and perform an emulation engagement. The red team should closely work with the blue team to gain a deep understanding of the gaps in the blue team's visibility and why they exist.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

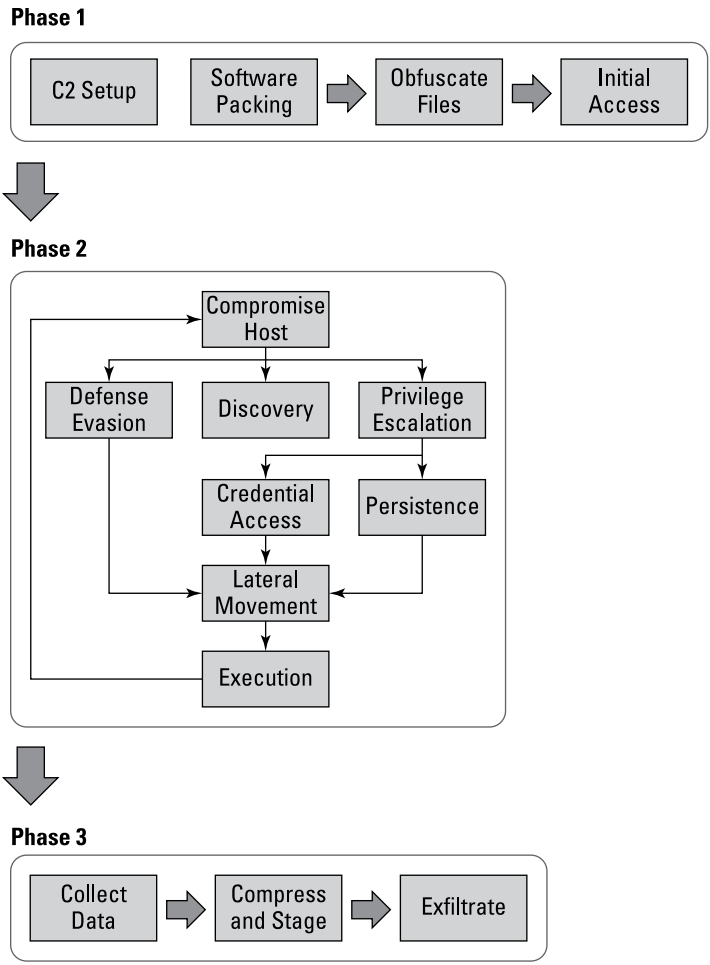

FIGURE 4-2: The APT3 operational flow phased plan.

After this process takes place, the red and blue teams can work with the CTI team to determine the next threat on which to repeat the process, creating a continuous cycle that tests defenses against real-world behaviors; it can be augmented through an automated breach-and-attack simulation platform.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Integrating analytics into threat-informed operations
- Performing continuous analysis and validation

Chapter 5
Developing Assessments and Engineering

What is an assessment? ATT&CK assessments are a part of a larger process to provide useful data to security engineers and architects to justify threat-based defense improvements. In this chapter, we show you how to use ATT&CK to conduct assessments and improve your cyberdefense effectiveness. Here are the three simple steps for running an assessment:

1. Assess how your defenses currently perform against techniques and adversaries in ATT&CK.
2. Identify the highest-priority gaps in your coverage.
3. Modify your defenses (or acquire new ones) to address those gaps.

REMEMBER

We break this chapter into three levels based on sophistication and resource availability; they're *cumulative* and build on each other. Even if you have an advanced team, we encourage you to start at Level 1 to ease into the process.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Level 1: Conducting Assessments with Limited Resources

If you work with a small, resource-constrained team, the idea of creating a color-coded heatmap (see Chapter 3) of the ATT&CK matrix that visualizes your coverage is appealing, but if you're a small team, the process may leave you burnt out on ATT&CK versus excited to use it.

TIP

Instead, start small: Select a single technique to focus on, determine your coverage for that technique, and make the engineering enhancements to start detecting it. Not sure where to start? Chapter 1 can help you choose a starting point.

After you've chosen a technique, figure out how well you have it covered. We suggest the following categories:

- Your existing analytics will likely detect the technique.
- Your analytics fail to detect the technique, but you're pulling in the right data sources to detect it.
- You lack the correct data sources for detection.

TIP

When starting out, keep your categories simple: Are you able to detect it or not? Look at your analytics to see what techniques they already cover. This can be time-consuming but is worth it: Many security operations centers (SOCs) already have rules and analytics that map back to ATT&CK. Often, you need to bring in other information about the technique, which you can get from ATT&CK's website, `attack.mitre.org` and then dropdown Techniques, or another external source.

As an example, suppose you're looking at Remote Desktop Protocol (T1076) and receive the following alerts:

- All network traffic over port 22
- All processes spawned by AcroRd32.exe
- Any processes named tscon.exe
- All internal network traffic over port 3389

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The third alert, "Any processes named tscon.exe," is a detection header. Port 3389 — specified by the fourth bullet — corresponds to the technique. If your analytics pick up the technique, great. Record your coverage and move to the next one. If it isn't picked up, look at the data sources to see if you're pulling in the right data to build a new analytic. If you are, then it's a question of building the analytic. If you aren't, this is where engineering comes into play. If you look at the data sources listed at `attack.mitre.org` and then dropdown Techniques, these sources can be a starting point to gauge the difficulty of collecting the data versus your ability to use the data sources effectively.

TIP

A frequently cited data source is Windows Event Logs, which provides visibility into ATT&CK techniques. Check out Malware Archaeology's Windows ATT&CK Logging Cheat Sheet to get started. Visit `tiny.cc/irjwsz` for more.

If you want to do more advanced analytics and engineering, run through this process several times and pick up new techniques with each tactic. To keep track of results, use ATT&CK Navigator to generate heatmaps of ATT&CK coverage. After you feel comfortable with the process, run a data-source analysis and build a heatmap of the techniques you can detect with the data sources you're pulling in. Helpful resources include Olaf Hartong's ATT&CK Datamap project (`github.com/olafhartong/ATTACKdatamap`), DeTT&CT (`github.com/rabobank-cdc/DeTTECT`), and ATT&CK scripts.

Level 2: More Advanced Analytics and Engineering

After you're familiar with the basics (see the preceding section) and have access to more resources, you can expand your analysis to a larger subset of the ATT&CK Matrix and use a more advanced coverage scheme to account for detection fidelity. We recommend bucketing your coverage into low, some, or high confidence that a tool or analytic in your SOC will alert you on the technique. Your chart should be a mix of yellow and green, indicating "high" and "some" confidence of detection. Don't worry about pinpoint accuracy when trying to assess your coverage; your goal is to understand if you have the engineering capabilities to generally detect techniques.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TIP

For each analytic, find what it focuses on and see how it maps back to ATT&CK. As an example, you may have an analytic that looks at a specific Windows event; to determine this analytic's coverage, look up the event ID in the Windows ATT&CK Logging Cheat Sheet or a similar repository.

Another important aspect to consider is the Group and Software examples listed along with a technique. These describe the procedures, or specific ways, an adversary has used a technique. They often represent variations of a technique that may not be covered by existing analytics and should be factored into a coverage assessment. In addition to your analytics, analyze your tools. Iterate through each tool, creating a heatmap per tool, with the following questions:

- Where does the tool run (for example, perimeter or endpoint)? The location may impact how well it performs versus a tactic.
- How does the tool detect? Is it using a static set of known indicators? Or is it doing something behavioral?
- What data sources does the tool monitor? Knowing the data sources helps you infer the techniques it may detect.

WARNING

Answering these questions can be hard. Try not to spend too much time getting bogged down in specifics; opt instead for broad strokes about general coverage patterns. To create a heatmap of coverage, aggregate all the heatmaps for your tools and analytics, recording the *highest* coverage over each technique. To improve coverage, we recommend a more advanced version of the analytic development process:

1. Create a list of high-priority techniques that you want to focus on in the short term.
2. Ensure you're pulling in the right data to start writing analytics for the techniques on which you focus.
3. Build analytics and start updating your coverage chart.

You may also want to start upgrading your tools. As you analyze documentation, keep track of any optional modules that you may be able to use to increase coverage. If you come across any, look at what it would take to enable it on your network. If you can't find any additional modules for your tools, you may be able to use them as alternative data sources.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Level 3: Advanced Analytics and Engineering

In advanced analytics and engineering, you introduce adversary emulation and, in particular, atomic testing (testing that is small and focused on a single technique) for specific controls. Each time you prototype a new analytic, run a matching atomic test and see if you caught it. If you did, great. If you didn't, see what you missed, and refine your analytics. For more on this process, visit `http://tiny.cc/trjwsz`.

For those with more advanced teams, you can include mitigations to ramp up your assessment. This moves your assessment away from looking only at tools and analytics and what they're detecting to studying your SOC as a whole. To see how you mitigate techniques, go through your SOC's policies, preventative tools, and security controls, map them to the ATT&CK techniques they may impact, and add those techniques to your coverage heatmap. MITRE's approach allows you to map techniques to mitigations. Some examples of techniques with mitigations include the following:

- Brute force can be mitigated with account lockout policies.
- Deploying Credential Guard on Windows 10 systems can make Credential Dumping more difficult.
- A hardened local administrator account can prevent Windows Admin Shares.
- Leveraging Microsoft EMET's Attack Surface Reduction rules can make it harder to use RunDLL32.

Another way to extend your assessments is to speak with others working in your SOC. A conversation can help you make better use of your capabilities. Start with key questions:

- What tools do you use most frequently?
- What are their strengths and weaknesses?
- What data sources do you want to see that you can't?
- What are your detection strengths and weaknesses?

Answers to these questions can help you augment your heatmaps. For example, if you previously found a tool with many

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

ATT&CK-related capabilities, but staff members only use it to monitor the Windows Registry, modify the heatmap to reflect how it's being used.

As you talk to your colleagues, look at the tool heatmaps you created. If you're still not satisfied with the coverage your tools provide, it may be time to evaluate new ones. Come up with a heatmap of coverage for each prospective new tool and see how adding it helps enhance your coverage.

TIP

If you're well-resourced, you can build a test environment to test the tool live, recording where it did well and where it didn't, and see how adding it can help improve your coverage.

Lastly, you may be able to decrease your reliance on tools and analytics by implementing more mitigations. Look at mitigations in ATT&CK to gauge if you can practically implement them. Consult your detection heatmap as part of this process; if there's a high-cost mitigation that prevents a technique that you're already managing relatively well on your own, it may not be worth investing in other tools. On the other hand, if there are low-cost mitigations you can implement for techniques for which you're struggling to write analytics, implementing them may be a good use of resources.

REMEMBER

Always weigh the potential loss of visibility when investigating removing detections in favor of mitigations. Make sure you have some visibility in cases where a mitigation or control may be bypassed so those events are less likely to be missed. Both detection and mitigation should be used as tools for effective coverage.

TIP

Assessing your defenses and guiding your engineering toward remediation can be a great way to get started with ATT&CK. Running an assessment helps you understand your current coverage, which you can augment with threat intelligence to prioritize gaps and then tune your existing defenses by writing analytics. You should keep a tab on your last assessment, update it every time you get new information, and periodically run adversary emulation exercises to check results. Over time, changes in the network and what's collected may have consequences that reduce the effectiveness of previously tested defenses. By leveraging ATT&CK to show how your defenses stack up to real threats, you can better understand your defensive posture and prioritize your improvements.

Automated continuous testing helps validate your security controls' effectiveness. See Chapter 6 for more information.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Moving from threat intelligence to threat-informed defense
- Mapping success across the organization

Chapter 6
Making MITRE ATT&CK Operational

This chapter focuses on helping organizations transition from using threat intelligence in a manual fashion to building a threat-informed defense strategy across the organization. It then pivots to using automated adversary emulations and assessments to improve your security effectiveness, and describes specific steps that you can take to use breach-and-attack simulation platforms to deploy ATT&CK scenarios to validate your security controls.

Moving from Threat Intelligence to Threat-Informed Defense

How can organizations make the most of the knowledge available in ATT&CK? Stemming from ATT&CK, breach and simulation adds two new concepts to improve an organization's cybersecurity: automation and security control validation. The goal is to move from point-in-time assessments to programmatic assessments that validate security controls at scale, in production, and continuously.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Why is this important? One core use for ATT&CK is for blue team defenders to use the information in ATT&CK to validate their security controls, building on the ATT&CK library with threat intelligence from the outside or that the team generates. The first goal is to focus on the threats that matter most. If defenses — people, processes, and technologies (PPTs) — aren't oriented toward the most important threats, those resources are wasted, and if they aren't tested actively against threats, security controls are likely to fail when challenged.

To validate security control effectiveness, past practice has been for organizations to turn to red team and "penetration testing," but such testing is often sporadic, under-resourced, and ineffective to validate security-control effectiveness continuously and at scale. You can use ATT&CK in combination with a breach-and-attack simulation platform for automated security control validation as opposed to relying on a sporadic manual process.

REMEMBER

An automated platform helps you be more efficient with ATT&CK; you can run automated testing and benefit from the rich performance data that scaled automation brings. You can run tests in a light, affordable way to drive up security effectiveness and efficiency and devote scarce resources to focus on other problems that demand attention.

When ATT&CK is used in this way, with blue and red teams together, it enables purple teaming. *Purple teaming* is a defensive method that focuses on collaborative communication between the red and blue teams, sharing threat information between them to understand adversary TTPs, close defensive gaps, and stop intrusions quickly. The combination of MITRE ATT&CK, breach and attack simulation, and purple teaming delivers a threat-informed defense across your organization.

Mapping Success across the Organization

You can deploy ATT&CK with a breach-and-attack simulation platform across your security organization in a maturing process. You begin with automated testing and end on a cyclical, comprehensive process of security optimization. Performance data stands at the center of this transformation. The initial goal is to achieve a pervasive and continuous testing program with the

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

means to find and close security gaps. A good breach-and-attack simulation program delivers

- Automated testing (using red, blue, and purple teams)
- Validation throughout the security pipeline, commercial vendors, and open-source solutions
- Assessments of managed security service providers (MSSPs) at the proof-of-concept stage of engagement and throughout the contract life cycle

You start deploying automated testing using MITRE ATT&CK to implement a threat-informed defense by following these steps:

1. **Orient yourself.**

   Set your security goals, identify stakeholders, and define rules of engagement across the organization to operationalize ATT&CK.

2. **Plan your work.**

   Set a scope for the work, assign responsibilities to security personnel, and identify scenarios to deploy against your security controls.

3. **Begin to execute the process.**

   Test your security controls using automated adversary emulations aligned to ATT&CK. Quantify your security controls, deploy the platform into your enterprise, and collect results by running adversary emulations against your assets.

4. **Analyze the data that the platform returns.**

   Interpret the data within the context of your operations and make decisions about the security controls that are underperforming or gaps that have been revealed.

5. **Remediate your security gaps.**

   Fix misconfigurations or user errors and identify gaps for investment.

6. **Validate your testing results.**

   Before making any further decisions, run tests again to validate that your remediation worked.

7. **Reflect and automate your operations.**

   Capture the lessons you learned in the first test process and implement a continuous validation strategy.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

As your company seeks to make your security program more effective and efficient with ATT&CK, you can develop granular performance data to drive improvements in your organization's security and technology governance with the following breach-and-attack-simulation-generated solutions:

- Threat emulation for security optimization
- Threat-informed technology operations to improve software security and architectural security
- Projections of software security development life cycle (SSDL) and modeling

In addition to performance data, automation helps you evolve toward a SecDevOps model, combining Security with Development and Operations in a continuous process to ensure software effectiveness and security. By using scenarios and emulation plans as a base, you gain a consistent, automated approach to project security oversight and control.

TIP

As you mature in this approach, with ATT&CK you can

- Continuously exercise your analysts against known threats to sharpen your defense capabilities.
- Streamline compliance by creating dashboards that map real data about your cybersecurity effectiveness against known threats to applicable regulatory requirements.
- Begin to benchmark your security return on investment by rationalizing your controls (overlaps and gaps) and your architectural strategy (for example, prevention-centric or detection-centric).

REMEMBER

Your goal is to mature into a fully actualized security program with ATT&CK as a foundation. A data-driven, threat-informed strategy gives the organization a shared understanding of threats and threat behavior, which makes security more granular and manageable. This change in security culture eliminates fear, uncertainty, and doubt. By using real performance data provided by continuous testing, you can prioritize the improvements that matter most for your security posture. Data-driven reporting leaves board members and senior leaders with deeper confidence in the security team's approach and overall effectiveness.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Introducing the case
- Looking at the threats
- Identifying your adversaries
- Putting ATT&CK to use
- Getting results

Chapter 7
Looking at a Use Case: Leveraging MITRE ATT&CK in the Financial Sector

MITRE ATT&CK can help organizations improve their cybersecurity effectiveness. To explore how one major company uses ATT&CK, we spoke to a leading chief information security officer in the financial sector about how it helps him achieve his mission of protecting his customers and the firm's most important data. We cover those lessons in this chapter, hoping to show how ATT&CK can help you.

Meeting the Firm

Dimensional Fund Advisors (DFA) is an investment management service that operates with over $550 billion in assets under management. Headquartered in Austin, Texas, the 38-year-old company has more than 1,700 employees and is run by a group of computational geniuses (or at least that's what the

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

head of cybersecurity calls them). As a global distributed firm with significant financial assets, the company faces significant cyberthreats to the firm's assets and personnel.

Defining the Threats

As the head of cybersecurity at DFA, Peter Luban watches out for a range of cybersecurity risks to his organization, and MITRE ATT&CK helps him set a strategic baseline for his team. A security professional with over 20 years of experience in cybersecurity and risk management, Luban refers to ATT&CK as the "Mother Brain" of cybersecurity planning and threat intelligence for his firm. The tool helps him align his entire security team around probable threats so he can achieve real security outcomes for his firm.

TIP

MITRE ATT&CK's focus on threat-informed defense helps DFA stay ahead of emerging threats. Over the last decade, adversaries have shifted their behavior and tactics, techniques, and procedures (TTPs) to exploit fissures in the security system. In the past, adversaries focused more on developing unique malware payloads to achieve specific effects. Today, adversaries have shifted their emphasis to social engineering and finding the weakest link in second- or third-party applications that could help them gain access to the institution's crown jewels.

Understanding Your Adversaries

So how does ATT&CK help cybersecurity professionals and companies like DFA understand the adversary and defend the firm? The principal value is that the ATT&CK framework codifies adversary capabilities into one simple and easy-to-use tool for security teams to access. It makes threat intelligence useful through its expanded view of the adversary and its capabilities. This is a historical advancement in the field of threat intelligence. It's like the advancement of video games. In the 1980s, characters were depicted through a series of single dots on a screen aligned in two dimensional space, but today video games have evolved into an immersive, three-dimensional experience where the user sees a complex environment where threats and other players move through a space.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The evolutionary analogy stands with ATT&CK. In the past, in conducting forensics and to understand their cybersecurity postures, defenders focused their sensors on indicators of compromise (often referred to as *signatures*), remnants in the computer code of an adversary's presence; this data providing only one small insight into the attacker. Moving far beyond signatures, the ATT&CK framework gives defenders a comprehensive view of the threat landscape; it allows defenders to see the attacker move along every step in the attack ladder. With years of threat research behind it, the framework provides unbiased, third-party analysis.

Making ATT&CK Useful

For DFA's security team, ATT&CK is useful in two principal ways:

- It serves as a purple team platform for a small security team. The security professionals on the DFA team are responsible for defending the entire DFA enterprise and all the firm's assets. This small team doesn't have a dedicated red or blue team to conduct malware forensics and reverse engineering; ATT&CK provides a recipe for purple teaming, and the security team can follow the framework left to right, using it as an intelligence resource for its defense operations. ATT&CK gives the firm a ready-made, industry-vetted, research-informed methodology by which it can validate its security effectiveness.
- ATT&CK provides the security team leverage with its infrastructure and technology teams across the company. It gives a common language of risk and, when used with a breach-and-attack simulation platform, allows the team to measure performance against threats, which results in real performance data the team can use to measure the organization's security effectiveness. If and when a new application is brought into the organization, the team and others in the company can use ATT&CK-based scenarios to validate that application's security.

These points are particularly useful when facing the demands imposed by governmental regulators, which are especially strict when it comes to financial governance. Regulations include the National Institute of Standards and Technology 853 family

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

of reports as well as regulations from the European Union, New York, and Singapore. Each regulation has subtle differences between it, yet the regulators and the DFA board can use ATT&CK to validate and display how security controls are working (or not). ATT&CK gives DFA an edge to be able to better prepare if and when a regulator were to ask for more data; the framework helps the team validate security-control effectiveness and provide regulators and the board with granular performance data.

There is another application. If the data indicates ineffectiveness, the security leader can turn to the security teams or the board and outline the steps required to solve the problem. ATT&CK provides accountability because there's tons of configuration drift, and many people have their hands in various pieces, which can turn into a security nightmare. ATT&CK allows the security team to focus on what matters from a threat standpoint and use ATT&CK as a tool to drive effectiveness.

Seeing the End Result

REMEMBER

The DFA security team gets real data with ATT&CK and realizes long-term value. ATT&CK is a unifying effort and something tangible to refer back to. That unifying component is the biggest benefit of the framework — at least to Peter Luban. ATT&CK provides the DFA security team with a clear process through which to understand threats and build intelligence about adversary behavior. It gives chief information security officers a way to think about risk effectively at the strategic and management level. The DFA team sees ATT&CK as a modern, adversary-focused approach and a valuable tool for security leaders.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Using ATT&CK for CTI
- Exercising your security team's capabilities
- Validating your detect and alarm capabilities

Chapter 8
Ten Ways to Apply the MITRE ATT&CK Framework

In this chapter, we give you ten ways to use the MITRE ATT&CK framework to achieve security optimization in your organization.

Cyberthreat Intelligence

Security teams can use ATT&CK as a platform for integrating, assessing, and focusing its cyberthreat intelligence (CTI) development process around key threats. The ATT&CK framework provides a baseline of available knowledge about key adversaries and the methods they use to attack data. CTI teams can take content from ATT&CK and build on it either by generating their own intelligence or through third-party intelligence providers. With ATT&CK as a foundation, security teams can build adversary emulations, deploy them against their cyberdefenses, and optimize their security programs.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Automated Testing and Auditing

Companies use MITRE ATT&CK with their red, blue, and purple teams in conjunction with an automated breach-and-attack simulation platform to test and audit their security controls. Blue and red teams use ATT&CK and adversary emulations to exercise and validate specific security controls, building on ATT&CK's existing content with new threat intelligence from the outside or their own intelligence. If you don't have a testing program in your company, you usually have an audit team, which performs many of the same benefits as a blue team. The audit team could be the blue team or an independent assessor. We cover the different types of teams in more detail in Chapter 4.

Security Risk Management and Strategy

Security leaders can use MITRE ATT&CK and automated adversary emulations to generate performance data about their security team, set a strategy for making adjustments, and decide whether to invest or divest in specific security areas. Security teams should select a security platform that provides a deep library of scenarios stemming from MITRE ATT&CK to objectively assess control performance against an adversary. The data you generate from MITRE ATT&CK and an emulation platform will help you determine the state of your assets, where you get value (or not), and what your business strategy should be to make the most of your investments.

REMEMBER

The only way to make these decisions is with an inventory and a data-driven assessment of how well the controls work.

Regulatory and Compliance Mapping

Cybersecurity compliance requirements are typically ambiguous, and regulators often look to the security team on how to achieve them. You can use MITRE ATT&CK to reduce compliance and regulatory burdens by mapping your regulatory and compliance controls, conducting continuous tests and mapping the data from those tests to your compliance framework, and training your auditors on how it works. The regulators want to see that

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

companies have a process, and they want to see documentation. This process provides proof.

Security Control Rationalization

Security teams can use MITRE ATT&CK and adversary emulation tools to assess the functioning of their controls and rationalize their use on the basis of their overall effectiveness and the organization's security posture requirements. This capability nests under the architecture team, which faces a series of choices through its strategy-rationalization narrative.

Analyst Training and Exercises

Beyond using ATT&CK to test analysts against specific certifications, you can tailor it under an adversary emulation platform to exercise your security team's capabilities — large or small scale — across the security organization or for a specific component of the team. ATT&CK makes exercises real by focusing the team against a true adversary, and, if you use a robust adversary emulation platform, it can do so in a real-world environment.

Threat Hunting

Security teams can use ATT&CK to anticipate, prepare, and hunt for threats that may affect the enterprise. In this scenario, the CTI team uses a new threat behavior that MITRE ATT&CK has just released or that a third party or your company has created. The security operations center (SOC) then uses ATT&CK to conduct a purple team exercise to test its capabilities to see how it performs against the new threat.

Commercial Security Solutions Evaluations

Your security technology team can use ATT&CK and a security optimization platform to assess competing security technologies and determine which one meets your enduring requirements.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Most technology companies allow potential customers to run a proof of concept before they do an enterprise-wide deployment of the technology. A robust platform can generate performance data about which technology performs best in meeting your security, regulatory, and compliance needs.

Security Pipeline Validation

In managing your security program, your security operations team needs confidence that it can see and respond to an event efficiently, effectively, and in a timely manner. If you're a member of a security operations team, you can use ATT&CK and an adversary emulation platform to assess all the security technology sensors within an enterprise, including the event logs, the network security controls, and the SIEM, to ensure that the technology works as it should.

TIP

Whether you're just starting to build your security program or choosing a new commercial security vendor for your security needs, you can use ATT&CK to assess competing security technologies and determine which one best meets your enduring requirements.

Business Enablement

Businesses can use ATT&CK in a range of stages for business enablement, from internal quality-assurance testing to pre-sales enablement to mergers and acquisitions. If you're a security vendor in the software development process, before the product enters the market, you can use ATT&CK and a security validation tool to validate that your capabilities detect and alarm as required. You can use it internally as a part of your product development and creation.

Security vendors can use ATT&CK in a pre-sales motion to show how their capabilities would work for the customer; in this way, when operationalized, ATT&CK performs an overwatch function with analysts during a proof-of-concept stage. Finally, security vendors can use ATT&CK in an adversary emulation platform to make sure that their capabilities perform effectively for customers and drive accountability within the organization. Sales teams want to be able to tell the truth about their products when they engage customers.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

ATTACKIQ

Better insights.
Better decisions.
Real security outcomes.

Increase efficiency and effectiveness across your security organization.

More isn't better. *Better is better.*

Learn more: www.attackiq.com

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Optimize your security program

How can you ensure that your cybersecurity capabilities defend your organization effectively? After decades of heavy investment in people, processes, and technology, this question still haunts security leaders. Intruders break through, security falters, and defenses fail against attacks. What should be done? Instead of trying to close every vulnerability, meet every standard, or buy the "best" technology, you can change the game by focusing your defenses on known threats. The way to begin is with MITRE ATT&CK.

Inside...

- Understand ATT&CK and cybersecurity
- Use threat intelligence effectively
- Learn detection and analysis methods
- Conduct purple team operations
- Make ATT&CK operational in an enterprise
- Learn from an ATT&CK case study
- Discern novel ways to apply ATT&CK

ATTACKIQ

Jonathan Reiber is Senior Director for Cybersecurity Strategy at AttackIQ and served as a Speechwriter and Chief Strategy Officer for Cyber Policy in the U.S. Defense Department. **Carl Wright** is Chief Commercial Officer at AttackIQ. A seasoned executive, he served as CISO for the U.S. Marine Corps.

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

ISBN: 978-1-119-74809-0
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.