

LEARNING MADE EASY

D3 Security Special Edition

MITRE ATT&CK™

for
dummies®
A Wiley Brand



Increase visibility
of cyber threats

—
Bridge gaps in
security coverage

—
Stay a step ahead
of adversaries

Brought to
you by

D3 SECURITY

Gordon Benoit
Min Lu

About D3 Security

D3 Security's Next-Generation SOAR Platform combines security orchestration and automation with the proactive analysis capabilities of the MITRE ATT&CK framework. Trusted around the world and by 100+ of the Fortune 500, D3 Security solutions help SOC and CSIRT teams increase the speed and quality of investigations, automate incident response workflows, and dramatically reduce false positives and MTTR. D3 Security integrates with hundreds of solutions, offering thousands of actions including fully automated MITRE ATT&CK analysis that can predict malicious behavior by correlating security events with the world's largest knowledgebase of cyberattack techniques and tactics. For more information, please visit <https://D3Security.com>.



MITRE ATT&CK™

D3 Security Special Edition

**by Gordon Benoit
and Min Lu**

**for
dummies®**
A Wiley Brand

MITRE ATT&CK™ For Dummies®, D3 Security Special Edition

Published by

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

Copyright © 2020 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. D3 Security and the D3 Security logo are registered trademarks of D3 Security. 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: 978-1-119-70313-6 (pbk); ISBN: 978-1-119-70311-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

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

Project Editor:

Carrie Burchfield-Leighton

Acquisitions Editor: Steve Hayes

Editorial Manager: Rev Mingle

Business Development Representative:

Molly Daugherty

- » Finding out where ATT&CK came from
- » Creating a common framework for naming in cybersecurity
- » Classifying the tactics and techniques of cyber attackers
- » Defining patterns of adversary behavior

Chapter 1

Defining MITRE ATT&CK

MITRE ATT&CK. It looks like two acronyms, but technically only one part is an acronym, and there's also an ampersand in there for some reason. It's a mouthful to say the least. So, we start off this chapter by breaking down the terminology:

- » **MITRE ATT&CK is pronounced *might-er-ah-tack*.**
- » **MITRE is the name of the company.** The name dates back to 1958, when it was apparently chosen by a board member because it didn't mean anything but had a nice feel to it (the 1950s were a simpler time). People often assume it's an acronym, but it isn't. MITRE is a not-for-profit organization that supports American governments at the federal, state, and local level and also works with academia and various industries. MITRE works in many domains, with a focus on technology.
- » **ATT&CK is an acronym that stands for Adversarial Tactics, Techniques, & Common Knowledge.** ATT&CK is a framework developed by MITRE for documenting common behaviors exhibited by cyber attackers, or adversaries, in real-world security incidents. There are ATT&CK matrices for enterprise, mobile, industrial control systems, and "Pre-ATT&CK"; however, for the purposes of this book, we refer exclusively to the ATT&CK Matrix for Enterprise, which comprises — at the time of writing — 12 tactics and approximately 300 techniques.

- » **Some names are used interchangeably.** When we use the word MITRE, we refer to the organization. When we use MITRE ATT&CK, or just ATT&CK, we refer to the framework and its matrix of tactics and techniques.

Tracing the Origins of ATT&CK

ATT&CK was created in 2013 as part of a MITRE research project about post-compromise detection in enterprise networks. The researchers found that they needed a framework for documenting adversary tactics, techniques, and procedures (TTPs) that

- » Drew from real-world incidents
- » Went beyond conventional indicators of compromise (IOCs)
- » Was more actionable than existing kill chain and life cycle models

ATT&CK was developed for MITRE's internal use but proved so useful that the company decided to release it publicly in 2015.

Looking at the Value of a Naming Framework

One of the ways ATT&CK provides value is by creating a common framework for naming adversaries and their behaviors, which may not seem that important, but the absence of such a structure has been a source of contention and confusion in the information security community for years.

As early as the 1990s, the advent of viruses, worms, and other malicious software prompted a rush by security researchers, and eventually security firms, to coin names for each new threat, resulting in a tangle of names to describe common phenomena. For example

- » The ubiquitous *Conficker* malware is also known as *Downup*, *Downadup*, and *Kido*.

- » The *Carbanak* threat group is also known as *Anunak* and *Carbon Spider*, depending on who's doing the talking.

Beyond just being annoying, inconsistencies of this sort make it hard to quickly classify threats and coordinate response.

Observing Tactics and Techniques

The core of the ATT&CK framework is a vast matrix of observed adversary tactics and techniques. The current iteration of the ATT&CK Matrix for Enterprise contains 12 tactics:

- » Initial Access
- » Execution
- » Persistence
- » Privilege Escalation
- » Defense Evasion
- » Credential Access
- » Discovery
- » Lateral Movement
- » Collection
- » Command and Control
- » Exfiltration
- » Impact

These tactics represent what an adversary is trying to accomplish at that stage of an incident. As you can see, the order of the 12 tactics reflects the path adversaries may follow in pursuit of their goals. This makes ATT&CK a variation on the “cyber kill chain” model.



Lockheed Martin created the cyber kill chain model to define the sequence of a typical attack. Understanding the sequence gives security teams a better chance to anticipate an attacker's next step and disrupt it, thereby breaking the “chain.”

Each tactic has between 11 and 70 associated techniques. *Techniques* represent the specific behaviors an adversary may use to try to achieve the goal of the associated tactic. Many techniques are

associated with more than one tactic. For example, Access Token Manipulation may be used by an adversary to achieve either the tactic of Privilege Escalation or Defense Evasion.

ATT&CK provides deeper information on each technique, including the applicable platforms (Windows, for example), on the data sources that could be used for detection, on the permissions one would need to execute the technique, and on some potential controls for mitigation.

Profiling Adversary Groups

Another significant component of ATT&CK is the behavior profiles that track the techniques known to be used by advanced persistent threat (APT) groups. These profiles aren't exhaustive, but they're an important part of the framework. They help distill some of the most prolific threat groups into constituent tactics and tools. Security teams can use this information for everything from incident response to modeling of security strategy to informing security investments.

For example, consider TA505, a prolific hacking group that has been observed since 2014. TA505 has been associated with the use of Dridex and TrickBot banking malware, a wide range of Trojan horse programs, and ransomware like Locky.

TA505 is known to be financially motivated with a history of targeting banks and financial services firms. Is your organization in the crosshairs of a group like TA505? The ATT&CK framework can help your security team answer that question by highlighting TA505's preferred techniques. Among them, the use of Code Signing (classified as technique T1116 in the ATT&CK matrix) of malicious payloads, including with certificates issued by Thawte and Sectigo. They also frequently use scripting in PowerShell, VBS, and JavaScript for Code Execution (T1064), including obfuscated commands like PowerShell commands encoded in base64 (T1027). TA505 often leverages rundll32.exe to execute malicious DLLs on compromised systems as well.

Any of these techniques, alone, may not arouse the attention of your security group. However, ATT&CK's group profiles can help your team recognize a constellation of otherwise unremarkable techniques like these as the work of a single sophisticated threat actor and move quickly to limit the damage of a compromise.

- » Using ATT&CK for assessment and analysis
- » Putting ATT&CK to work in intelligence and investigations
- » Evaluating detection and response with ATT&CK

Chapter 2

Exploring Use Cases for MITRE ATT&CK

ATT&CK provides so much information that the prospect of putting it into action can seem overwhelming. In this chapter, you discover three ways to start using ATT&CK in your security operations center (SOC).

Assessment and Analysis

In this section, you find out how you can use ATT&CK to assess your current level of coverage and compare it to the threats you're facing.

Assessing your coverage

One of the first things you can do to put ATT&CK into action is assess which ATT&CK techniques your current security tools and processes cover. Mapping your coverage across the entire ATT&CK matrix all at once is going to be out of scope for most organizations, so begin by assessing your coverage of one technique at a time, starting with the most important.



Determine the most important techniques by interviewing your security team, or use the threat modeling technique we describe in the section “Intelligence and Investigation.”

The ATT&CK website lists data sources and detection information for each technique, which you can use to assess coverage. Take the technique you’ve decided to start with, and check the listed data sources. If the sources are in place, move on to detection. Compare what’s listed in ATT&CK to the analytics you have, such as active rules in your security information and event management (SIEM) or endpoint detection and response (EDR) tool.

For example, sophisticated adversaries who are “living off the land” within a compromised environment may use the Windows Task Scheduler or utilities like `schtasks` to run malicious programs to maintain persistence. An organization that wanted to know if it was properly monitoring for such behavior could look up the Scheduled Task technique (classified as technique T1053 in the ATT&CK matrix). ATT&CK’s list of data sources needed to detect this technique includes Windows event logs, file monitoring, process monitoring, and process command-line parameter monitoring. With some luck, you’re already monitoring these data sources and have detections in place, even if you weren’t classifying the behavior as an ATT&CK technique. If you haven’t been monitoring the data sources, you now know this gap should be closed. If you have the data sources, but not the detections, create a new analytic or leverage an existing open-source analytic. Check out “Detection and Response” for more info.

Mapping coverage to ATT&CK

By assessing more techniques, you can begin to build a map of coverage. To broaden your understanding of your coverage, start by taking an inventory of your data sources. Some data sources, such as File Monitoring, Process Monitoring, and Process Command Line, are especially valuable because they’re involved in the detection of many different techniques. As you progress with your assessments, you can track the results of your assessments in the ATT&CK Navigator — a useful tool that we cover more in the section “Intelligence and Investigation.” Add more detail by tagging each technique with your level of confidence in the coverage. You won’t be able to create a full map overnight, but at the end of the process, you’ll have a clear picture of your vulnerabilities.

Evaluating tools

ATT&CK is also a useful framework for evaluating new tools. If a tool doesn't help you close gaps and cover relevant techniques, it isn't worth your money. For example, imagine a company in the oil and gas industry that's weighing investments in various security tools. Say the company has facilities and operations in the Middle East. A review of the ATT&CK framework identifies groups like MuddyWater (classified as group G0069 in ATT&CK) as well as the Iranian APT 33 (G0064) groups as active in that region with a history of targeting oil and gas companies.

The techniques used by those groups includes phishing emails with malicious Microsoft Word documents or HTML applications (T1204); the use of PowerShell for execution of malicious payloads (T1086); and the harvesting of credentials from web browser caches and files using tools like LaZagne and MimiKatz (T1003). However, neither group is associated with dedicated denial of service (DDoS) attacks.

Based on this analysis, DDoS protection isn't the highest priority. Web application firewall capabilities could address some attack vectors but aren't suited to groups that favor malicious email payloads. The most relevant tools are UBA technology to detect malicious activity on compromised endpoints or threat intelligence services that alert you to the activities of known advanced persistent threat (APT) groups.

Intelligence and Investigation

ATT&CK can standardize how you assess threat intelligence, model risk from APT groups, and investigate incidents in your environment. In this section, we explain using ATT&CK in your SOC to pinpoint your most pressing vulnerabilities.

Modeling threats

On the ATT&CK website, APT groups are catalogued with the industries they're known to have targeted. You can look up the major threats to your industry and see which techniques those APT groups use most frequently. For example, a quick search in ATT&CK for the APT group known as "Carbanak" or "Anunak" reveals that it relies heavily on Remote Access Tools (T1219) like AmmyAdmin and Team Viewer to conduct remote command and control of infected systems.



TIP

Map the techniques by using the ATT&CK Navigator, a web app from MITRE, available for free on GitHub. You can manipulate the ATT&CK matrix to create heat maps, add notes, and more. Find ATT&CK Navigator at <https://mitre-attack.github.io/attack-navigator/enterprise>.

By using Navigator, you then map the techniques onto the ATT&CK Matrix. If you've already done analysis of what techniques you have coverage for (we cover this in the section "Assessment and Analysis"), map your coverage as a layer to compare against the threats posed by APT groups. This action immediately highlights high-risk gaps and vulnerabilities in your detection and response capabilities. ATT&CK includes descriptions of each technique, as well as detection and mitigation recommendations, so even if you're starting from scratch, you have an idea of your next steps.

Mapping threat intelligence

Some threat intelligence providers now map reports to ATT&CK themselves, which is a huge time-saver, but security teams can also do it manually. For example, operators reviewing a published report that makes mention of ransomware gangs "setting a startup item in the SYSVOL share" on a domain controller could use the MITRE ATT&CK website to search for "SYSVOL." That would bring them to ATT&CK Technique 1003 (T1003) for "Credential Access" or "Credential Dumping," which they could map to ATT&CK using Navigator.

If that sounds like way too much work, MITRE now offers a web-based tool (currently available in beta) called the Threat Report ATT&CK Mapper (TRAM) to make it easier to extract tactics, techniques, and procedures (TTPs) from reports. You can find it at <https://github.com/mitre-attack/tram>.

Mining past incidents

Just like parsing a threat intelligence report for ATT&CK techniques, you can parse internal reports of security incidents to model threats. Mapping an incident to ATT&CK should become part of your standard postmortem process, so you can do it when the incident is still top of mind and the data is easily accessible. This process also has the unique benefit of showing you where your security coverage is effective during real incidents (for example, what techniques did the adversary fail to execute) and where the gaps are that need to be closed.

USING SOAR FOR INCIDENT INTELLIGENCE

Security Orchestration, Automation, and Response (SOAR) platforms integrate with the entire security stack to ingest alerts, enrich them with intelligence, and orchestrate response efforts. D3 Security has embedded ATT&CK into its SOAR platform, enabling it to analyze security events for indicators of techniques and automatically map them to ATT&CK. Using SOAR to turn past incidents into ATT&CK intelligence greatly reduces the time and expertise required to detect and map techniques. SOAR tools aggregate data from across the security infrastructure, so they capture a more complete picture of incidents than other tools, and also allow teams to sidestep the difficulty of developing a structure for storing and searching ATT&CK intelligence.

Detection and Response

ATT&CK can help you define your existing coverage, but chances are you're not just looking to understand where you're at; you want to make improvements. In this section, we describe ways you can increase your capacity to detect, mitigate, and respond to adversary TTPs in your environment.

Developing analytics

Analytics, in this context, are search queries that can be run from a tool (generally a SIEM) across collected log and event data to detect the behaviors associated with an ATT&CK technique. If, like most security teams, you don't have the detailed understanding of ATT&CK techniques required to write detection analytics from scratch, you can leverage existing ATT&CK analytics, including those created by MITRE. These open-source analytics provide pseudocode that can be run in a SIEM as a search query. If the code doesn't match the SIEM your organization uses, tools, such as Sigma, can translate the query for different platforms. After you're running analytics and receiving results in your SIEM, analyze the results for false positives and make changes to filter them out. When an analytic works properly, you can use it to trigger an alert in your SIEM or SOAR platform.

Mitigations

Just as every technique in the matrix contains data source and detection information, it also has mitigations, which may be policies, tools, or security controls, such as Multi-Factor Authentication (classified as mitigation M1032 in ATT&CK), Network Segmentation (M1030), and SSL/TLS Inspection (M1020). To check where you have this level of coverage, look up mitigations on the ATT&CK page for each technique, or start by looking up a mitigation you know you have in place and see all the techniques it can be used against.

Testing coverage

Test your defenses with adversary emulation, an exercise where a red team replicates the behaviors of a known adversary. One simple way to start, even if you don't have a red team, is to use a collection of existing open-source scripts, such as Atomic Red Team, that replicate ATT&CK techniques. This approach may look like this:

- 1. Pick an APT group, list its known techniques, and compare those techniques to your map of existing detections or mitigations.**
- 2. Run an Atomic Red Team script for each adversary technique, and compare what your security tools detect and mitigate to what you expected based on your coverage assessments.**

Find Atomic Red Team at <https://atomicredteam.io>.

Using security tools to correlate events with ATT&CK

A lot of security vendors are working the ATT&CK framework into their products. For example, some EDR tools will tag events with ATT&CK techniques when they match MITRE's criteria. Some of these tools provide a map of the techniques that they can capture, saving you from having to assess your coverage of those techniques manually.

- » Standardizing your language of threats
- » Staying a step ahead of adversaries
- » Improving SOC of any maturity

Chapter 3

Ten Reasons to Use MITRE ATT&CK

You're probably reading this book to decide whether MITRE ATT&CK is something you should be using in your organization. So in this chapter, we cut to the chase and give you ten things that make ATT&CK a valuable asset for security teams, along with the first step to put each thing into action.

Standardize Your Language of Threats

At its most basic level, ATT&CK brings value by providing a tangible and consistent framework for assessing and discussing security in a way that reflects real-world adversary behaviors.



TIP

To put this into action, establish ATT&CK as your internal framework for evaluating security coverage and threats. Taking this step helps security teams communicate what they're doing — and what they need — to stakeholders that may not be well versed in security.

See Chapter 1 for more about how ATT&CK standardizes the language of security.

Join an Industry-Wide Movement

ATT&CK isn't just a standardized way to talk internally about security. It also gives you the benefits of sharing a standard framework with other security teams, researchers, and vendors around the world. This means there are numerous open-source projects that support the implementation of ATT&CK through scripts for detections, tools for adversary emulation, and more.

Take advantage by leveraging a few free resources:

- » **ATT&CK Navigator:** <https://mitre-attack.github.io/attack-navigator/enterprise>
- » **Atomic Red Team:** <https://atomicredteam.io>
- » **Threat Report ATT&CK Mapper (TRAM):** <https://github.com/mitre-attack/tram>.

See Chapter 2 for more details on each of these resources.

Stay a Step Ahead of Adversaries

ATT&CK is more than just a matrix of tactics, techniques, and procedures (TTPs). MITRE has also studied the known behaviors of prominent adversary groups, which you can map onto the matrix to model threats. Security teams can use these maps, create their own, or copy open-source models and drop them into ATT&CK Navigator.

Get started by mapping the techniques used by the most prominent advanced persistent threat (APT) group in your industry. See Chapter 2 for how to model the threats posed by APT groups.

Decipher Complex TI Reports

In a mature SOC, you may be proactively analyzing threat intelligence (TI) reports that are relevant to your organization. Even for security pros, these reports can be an overwhelming deluge of granular information. Using ATT&CK as your model for dissecting

TI can focus your efforts on the indicators that represent high-risk TTPs.



TIP

Start by uploading a TI report to TRAM and mapping the detected techniques in Navigator. See Chapter 2 for more about using ATT&CK to make sense of threat intelligence.

Improve Incident Postmortems

Using ATT&CK TTPs to describe what happened in an incident makes for a clear, actionable, and repeatable postmortem process. Start by selecting one past incident. Go through the data collected in security tools — for example, security information and event management (SIEM) or security orchestration, automation, and response (SOAR) — and interview the rest of the security team to determine the techniques used by the adversary. Then map those techniques to the ATT&CK matrix to visualize what the adversary did, and what it tried to do.

Head to Chapter 2 for more information about mapping incidents to the ATT&CK matrix.

Apply Behavior-Based Security

ATT&CK provides a framework for implementing behavior-based security by giving you the tools to search for the actions adversaries are known to take, even when those actions aren't obviously malicious on their own. Put this into action by implementing a detection analytic for a behavior that may slip past signature-based systems.

Flip to Chapter 2 for more on detection analytics.

Go beyond the Kill Chain

Like the cyber kill chain, ATT&CK tactics are ordered in the sequence that an adversary is likely to follow. However, ATT&CK is a more actionable model than the kill chain because it provides granular information about each behavior.

Leverage the kill chain model by mapping the techniques used in a past incident to ATT&CK. This helps you visualize the path of the adversary, where it was successful, and where you may disrupt a similar attack in the future.

Chapter 2 has more information about mapping techniques to the ATT&CK matrix.

Create Rules Using MITRE's Data

MITRE provides detailed technical information about each technique, which you can turn into effective actions. Get started by picking an important technique and creating a rule in your SIEM to detect it, and read Chapter 2 for more on using SIEM rules to detect techniques.

Test Your Defenses

Whether or not you have a dedicated red team, ATT&CK provides a great playbook for adversary emulation exercises. Run a simple exercise by picking one of the APT group profiles included in ATT&CK and use Atomic Red Team's prebuilt scripts to replicate that group's methods of attack.

In Chapter 2, we give you more info about adversary emulation.

Improve SOC's of Any Maturity

Because ATT&CK is free, it's accessible to organizations of any size, and it can help improve the effectiveness of SOC's of different maturity levels. In advanced SOC, you could start by building a detailed map of your coverage across the matrix. In a less mature SOC, you could start by implementing open-source analytics to detect the most frequently used techniques in your industry.

For information on how to build a map of existing coverage, head to Chapter 2.



IMPROVE THE SPEED AND QUALITY OF SECURITY OPERATIONS WITH THE ONLY PLATFORM THAT COMBINES SOAR WITH MITRE ATT&CK™

- ✓ Automatic correlation and response
- ✓ ATT&CK-based guided workflows
- ✓ TTP dashboards and gap reporting

Learn more at D3Security.com

Leverage a powerful cybersecurity framework

The MITRE ATT&CK Matrix for Enterprise is the world's largest database of cyber adversary tactics, techniques, and procedures. In fact, it's so comprehensive that it can be hard to know where to start using it in your security operations. In this book, you discover what exactly MITRE ATT&CK is and how to get value from it by modeling threats, assessing your security coverage, creating detection analytics, and much more.

Inside...

- Define the security value of ATT&CK
- Profile dangerous adversary groups
- Study valuable use cases for ATT&CK
- Get actionable threat-detection rules
- Find out about must-have free tools
- See ideas for improving SOC maturity
- Learn to turn SOAR data to ATT&CK TTPs



Gordon Benoit is D3 Security's President and **Min Lu** is Vice - President of Development and D3 Labs. Together, they bring 40 years of cybersecurity experience.

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

ISBN: 978-1-119-70313-6

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.