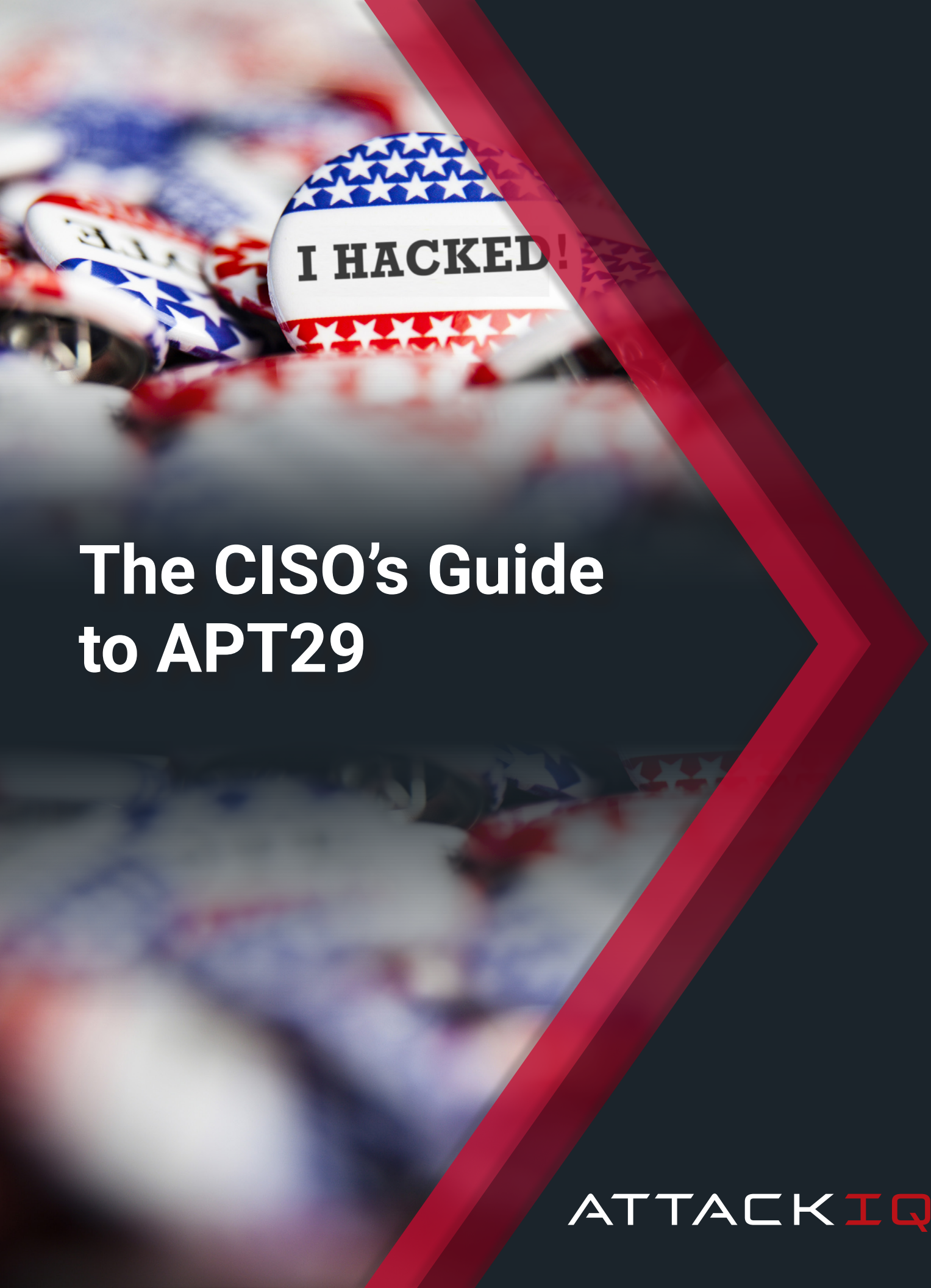



# The CISO's Guide to APT29

ATTACKIQ®

# Contents

**Notice** ..... **3**

**An Introduction to APT29** ..... **4**

**Objectively Assess Your APT29 Defenses by Using Breach and Attack Simulation** ..... **5**

The MITRE ATT&CK Framework ..... 6
MITRE ATT&CK's benefits include: ..... 7
Breach and Attack Simulation (BAS) Platforms ..... 8

**Emulating APT29 with Breach and Attack Simulation** ..... **9**

The APT29 Assessment Template ..... 9
Configuring the Assessment Template ..... 10
Analyze the Results - Take Decisive Action ..... 12

**Improve and Repeat** ..... **14**

**Recommendations** ..... **15**

A CISOs Guide to MITRE ATT&CK ..... 15
A CISOs Guide to Breach and Attack Simulation ..... 15

**References** ..... **15**

## Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Any additional developments or research since the date of publication will not be reflected in this report.


## An Introduction to APT29

APT29 (aka Cozy Bear, CozyDuke, the Dukes, or PowerDukes) is a threat group that has shown strong ties to the Russian government since approximately 2008. APT29 is best known for its compromise of the Democratic National Committee starting in mid-2015 in advance of the U.S. presidential election the following year.

Following the 2016 U.S. presidential election, APT29 was responsible for a series of spear-phishing campaigns that focused on U.S.-based "think tanks" and other non-governmental organizations. The attackers utilized a mix of Google Gmail accounts as well as stolen credentials that enabled them to send email from Harvard's Faculty of Arts and Sciences. These emails were sent to many individuals in national defense, international affairs, and public policy. Some of these emails even pretended to come from the Clinton Foundation to share analysis on the election. APT29 has continued to evolve and shows the use of new tactics, techniques, and procedures (TTPs).

APT29 has many custom-developed tools which it continually improves on as new information is published in security communities. This toolset is mainly focused on providing persistent access to the victim's machine (backdoors) as well as gathering information, files, credentials, etc. and exfiltrating them.

APT29 has used a wide range of different programming languages to develop its malware, from pure assembly (found in some components of MiniDuke) to C++ (CozyDuke) and from .NET (HammerDuke and RegDuke) to Python (SeaDuke). The group's creativity goes even beyond that, as over the time it has tried different technologies, infection vectors, infrastructure, and more.

In summary, APT29 presents a dangerous advanced persistent threat. Its team is highly technically skilled and capable of adapting to the defenses of the targets it chooses. It often uses techniques and tools that have been identified in previous attacks. The "fingerprints" of its attack activity are becoming well documented and the subject of considerable ongoing analysis.

## Objectively Assess Your APT29 Defenses by Using Breach and Attack Simulation

Some of the toughest board of director questions a CISO will ever receive are the ones along the lines of "I just read about APT29. Are we protected against APT29? What is our risk of a successful breach by the APT29 threat actors? How do we know?"

There are two new defensive tools which enable CISOs and their teams to best answer these difficult questions correctly and accurately. They give you everything you need to know to stand tall in assessing the relative risk of APT29, or any other new "threat du jour," against your enterprise's cyber defenses.

MITRE ATT&CK™ Framework. The first of these important additions to your defensive toolkit is the MITRE ATT&CK cybersecurity framework. MITRE ATT&CK takes the view of the attacker and frames the likely activity of APT29 in terms of very specific attacker tactics, techniques, and procedures.

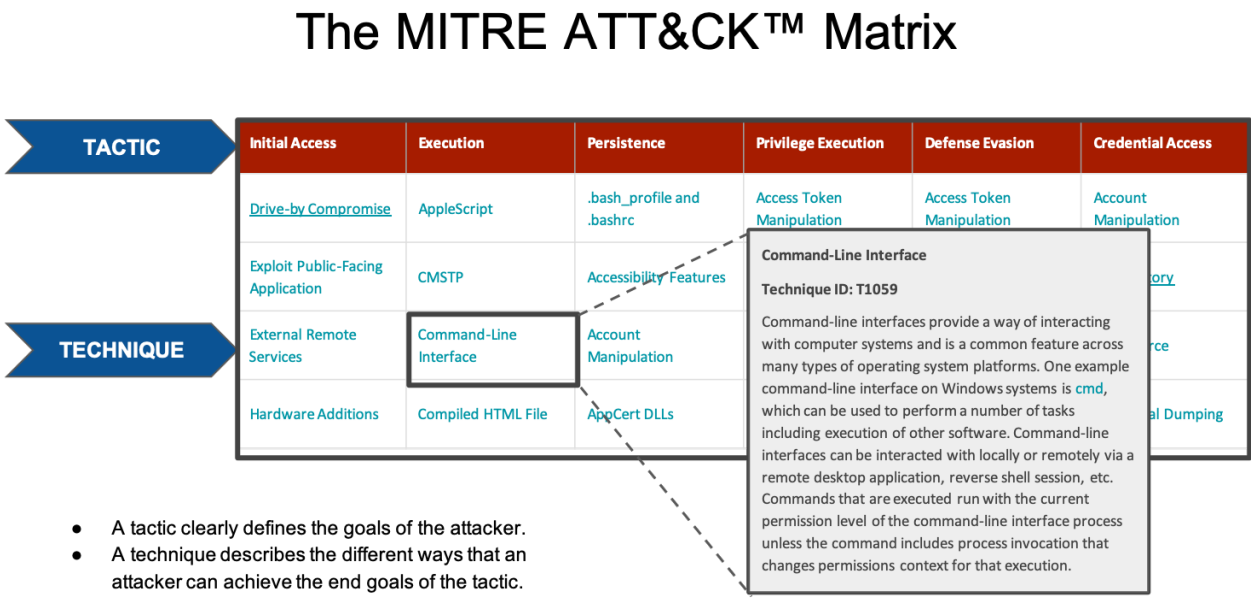
AttackIQ Breach and Attack Simulation (BAS) Platform. The second important addition to your defensive toolkit is the AttackIQ breach and attack simulation platform. AttackIQ allows you to operationalize MITRE ATT&CK and build out scenarios that simulate exactly the tactics, techniques, and procedures that the APT29 attack group might use based upon known threat intelligence and industry data.

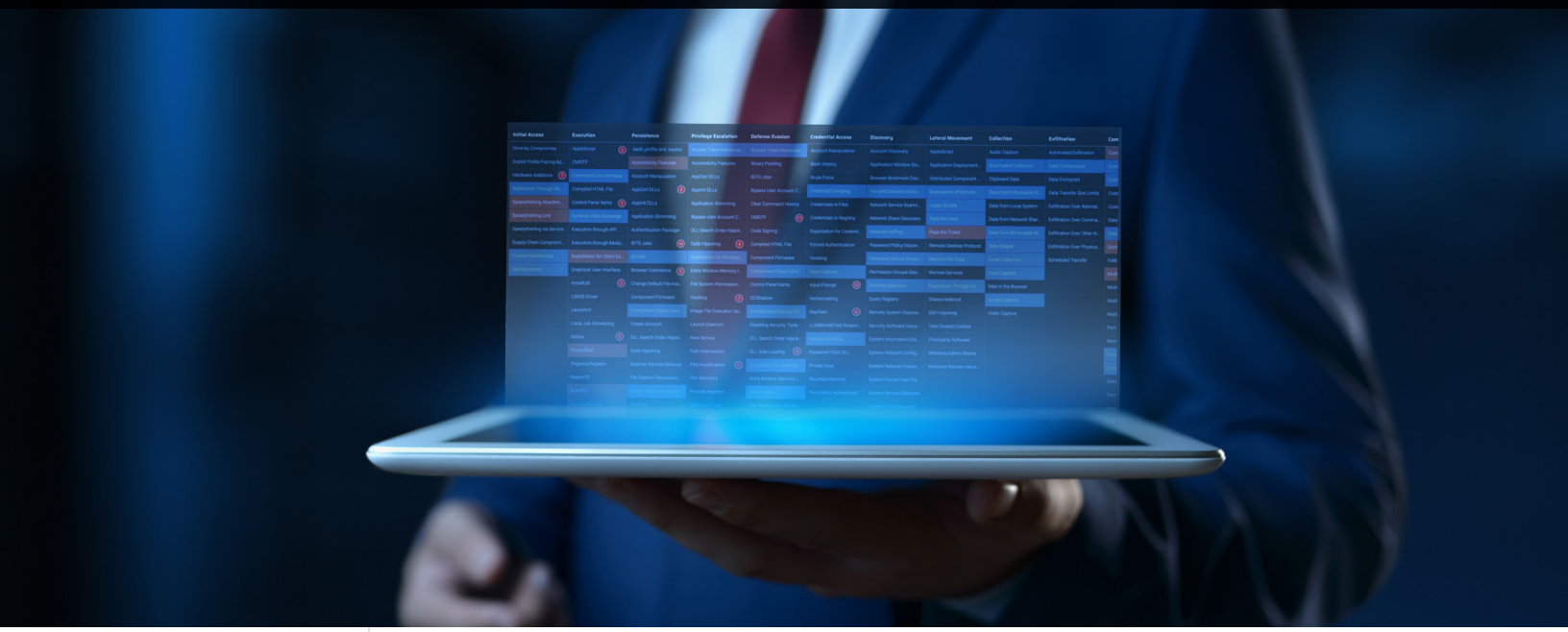
Let's take a closer look at these important and powerful defensive tools.

## The MITRE ATT&CK Framework

MITRE ATT&CK is, in both depth and breadth, the largest cyber attack knowledge base, providing suggested mitigation techniques, detection procedures, and other important technical information. MITRE has expanded the traditional Kill Chain to include the widest variety of tactics that are then supported by detailed techniques. This organized approach enables you to methodically select and analyze attacks and to compare them to the capabilities of your security controls so that you can understand the gaps. Once understood, you can then rationally expand your security controls and adjust your budgets. MITRE's stature in the cyber community and the independence of its intellectual property in the ATT&CK matrix make it the ideal platform from which security operations management, executive staff, and the board of directors can objectively evaluate and measure cybersecurity controls' performance, risk, and capability.

The MITRE ATT&CK enterprise matrix provides a tabular view of all attacker tactics and techniques that might leverage Windows, Mac, and Linux environments. Across the top are headings listing the 12 tactics defined by MITRE ATT&CK. Listed below each of the 12 tactics is a column that shows nine to 67 techniques that might be used to implement a particular tactic. It is often that case that several techniques are used in one or more tactics. A tactic clearly defines the goals of the attacker. A technique describes the different ways that a cyber attacker can achieve the end goals of the tactic.





## MITRE ATT&CK's benefits include:

A Common Lexicon. MITRE ATT&CK has brought a well-matured taxonomy of the tactics and techniques that may be leveraged by any prospective attacker. This provides, for the first time, a common lexicon that enables business stakeholders, cyber defenders, and vendors to clearly communicate on the exact nature of a threat and the objective assessment of the cyber defense plan that can defeat it.

The Largest Database of Documented Attacker TTPs. MITRE ATT&CK includes detailed information about the APT29 attack group scenarios with suggested mitigation techniques, detection procedures, and more. MITRE has expanded the kill chain to include the widest variety of tactics that are then supported by detailed techniques. This organized approach enables you to methodically select the attack you need to validate your security controls and to understand the gaps so you can rationally expand your security controls set.

Use the Tactics, Techniques, and Procedures of APT29. MITRE ATT&CK lets you take on the mindset of the APT29 attacker. Imagine that one or more cyber attackers are working full time, with no other goal in mind than to break, enter, and compromise your intellectual property, damaging or destroying your information technology infrastructure. MITRE ATT&CK helps bring that attack to life so that you can understand the techniques they might use and position the defense you need to best defend your enterprise.

## Breach and Attack Simulation (BAS) Platforms

The next step is to automate security control validation and performance measurement using a breach and attack simulation platform that operationalizes the MITRE ATT&CK framework. With automation, this new infrastructure will continuously validate your cybersecurity controls in your production environments.

Breach and attack simulation platforms allow enterprises to automatically simulate the full attack and expanded kill chain used by cyber attackers against enterprise infrastructure using software test points that allow testing across roaming laptops, user desktops, virtual machines, or cloud infrastructure. The result is detailed reports of the status and performance of your security controls and processes as well as the personnel that support them. Once BAS allows you to find the performance gaps, you can strengthen your security posture and improve your incident response capabilities. BAS can validate that your enterprise security systems are performing against known attacker behaviors.

Lets review how these work and how they help fill the gaps so you can accurately and completely answer the challenging questions in front of us. Breach and attack simulation platforms allow enterprises to automatically simulate the full attack and expanded kill chain used by cyber attackers against enterprise infrastructure using software test points that allow testing across roaming laptops, user desktops, virtual machines, or cloud infrastructure. The result is detailed reports of the status and performance of your security controls and processes as well as the personnel that support them. Once BAS allows you to find the performance gaps, you can strengthen your security posture and improve your incident response capabilities. BAS can validate that your enterprise security systems are performing against known attacker behaviors.

Most important, BAS platforms provide automation that enables the platforms to work autonomously and to scale to support the largest global enterprise. Support for live production environments enables you to see in real time how changes to configurations or administration can open new vulnerabilities in your cyber defense.

AttackIQ's BAS platform provides the setup of scenarios that are used to test your technology controls, validate your security posture, and instrument your environment. Scenarios will mimic malware and attack vectors so that you can confirm that your security controls are working as expected. The fast path to productivity is to test your existing security controls to validate they are performing as you expect.

# Emulating APT29 with Breach and Attack Simulation

As the security posture of a company becomes more mature, providing the ability to have advanced insight into how security controls and the teams behind them would respond to a full attack chain of a known malicious threat actor becomes increasingly valuable.

At AttackIQ, we certainly want to help our customers do that, so we started developing a new assessment template with that goal in mind. Today we are happy to announce that we have completed the new APT29 Assessment Template: a group of scenarios that emulate the known tactics, techniques, and procedures (TTPs) of the APT29 threat group.

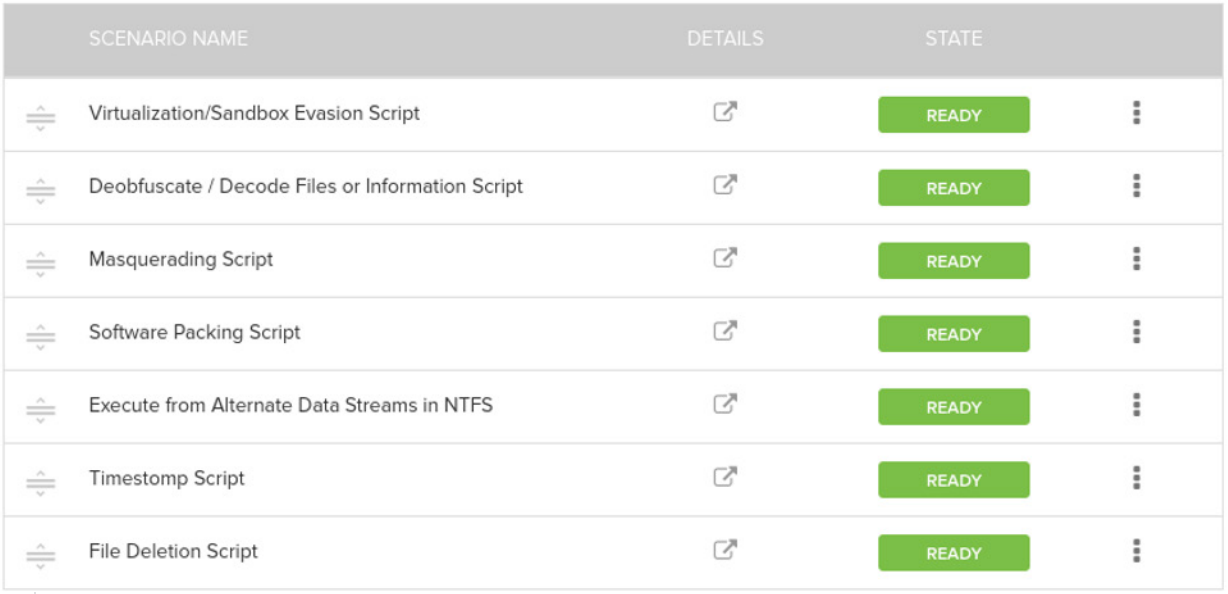
## The APT29 Assessment Template

The AttackIQ assessment template is designed to simulate the behavior of APT29, selecting and configuring the necessary scenarios to cover the entire post-exploitation attack chain of this threat group: from the first stage after compromising a machine to the later stages of communication with a Command and Control server and the exfiltration of sensitive information. In total, this assessment template contains 45 scenarios covering 56 MITRE ATT&CK techniques. We based this selection of techniques on the one done by MITRE for its new round of evaluations, which will have APT29 as the simulated attacker.

But how are these scenarios organized and why? We decided to group them into nine different tests according to their MITRE ATT&CK tactic, except for the last test, in which we decided to group the scenarios belonging to either Command and Control or Exfiltration tactics. In our case, the order of the tests corresponds to their position inside the MITRE ATT&CK matrix which, roughly speaking, corresponds to the depth of the intrusion after the initial breach.

| TEST NAME | ASSETS | SCENARIOS | SCENARIO STATUS |
|---|---|---|---|
| 1 - Execution | 4 | 4 | READY (4) |
| 2 - Persistence | 4 | 4 | READY (4) |
| 3 - Privilege Escalation | 4 | 4 | READY (4) |
| 4 - Defense Evasion | 4 | 7 | READY (7) |
| 5 - Credential Access | 4 | 2 | READY (2) |
| 6 - Discovery | 4 | 10 | READY (10) |
| 7 - Lateral Movement | 4 | 4 | READY (4) |
| 8 - Collection | 4 | 7 | READY (7) |
| 9 - Command and Control | 4 | 3 | READY (3) |

Similarly, inside each test the scenarios are ordered taking into account the usual course of actions as well as the level of sophistication of the attacks (executing the most simple or common first).

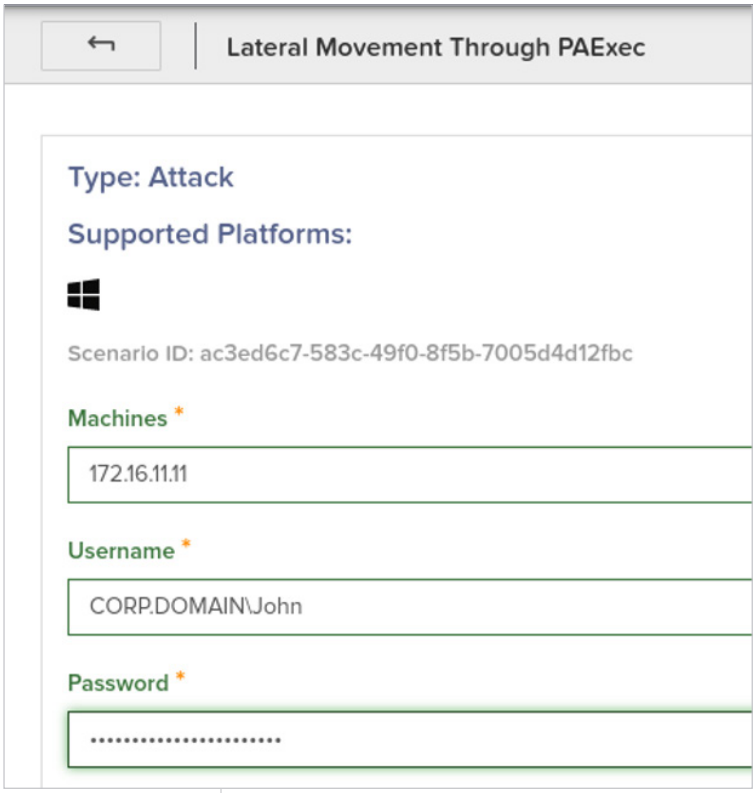



This ordering is intended to emulate as closely as possible the actions that APT29 would take once a network is compromised, but also has other advantages. For example, separating the scenarios by MITRE ATT&CK tactic allows identifying the blind spots and strengths of the defenses at each stage of an attack. This can help to prioritize actions, locate sources of forensic information that might be useful in a real incident, build custom rules, detect misconfigurations, and more. This information can be used to later design or improve a defense in depth strategy. Similarly, in emulating a whole kill chain, this assessment can also be used to test and improve incident response plans or perform threat-hunting exercises with an incident response team.

## Configuring the Assessment Template

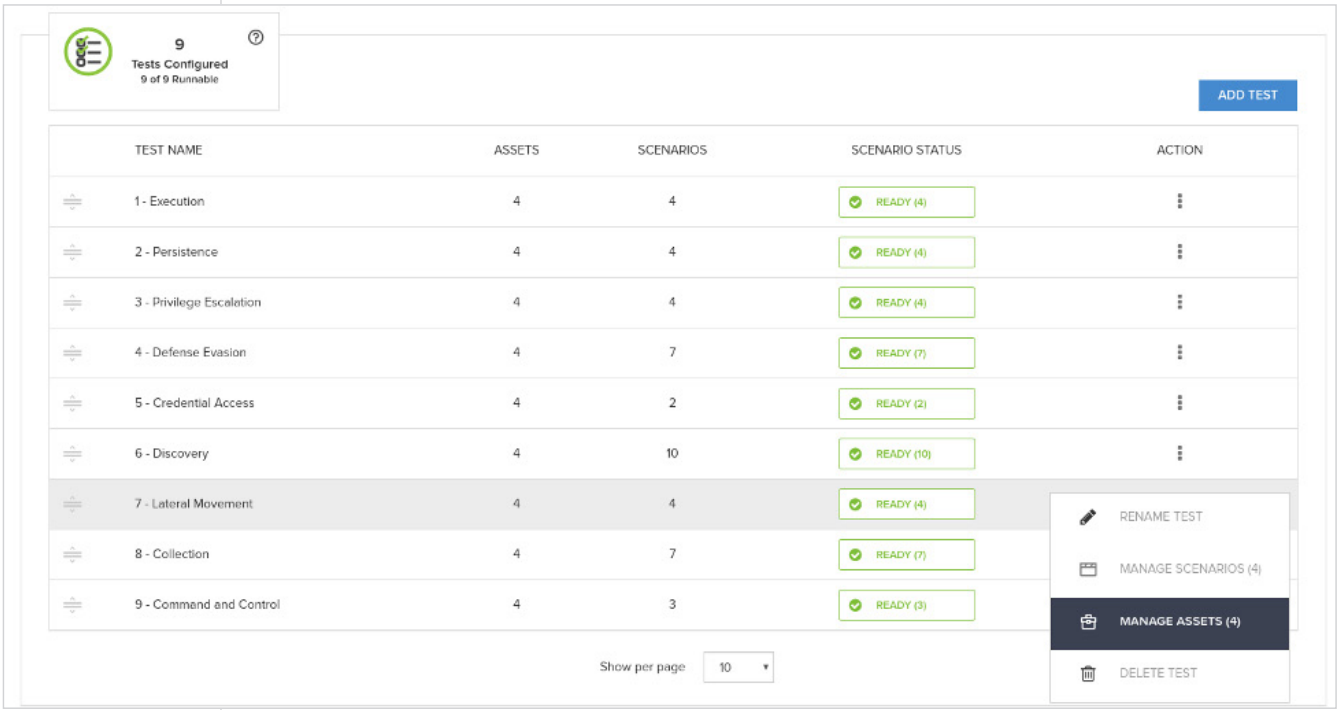
This assessment is designed to run almost out-of-the-box, from the commands that certain scenarios will execute to the file types that the Collection scenarios will search and from the credential dumping tools that will be used to the Command and Control servers (controlled by AttackIQ), to which some information will be exfiltrated. However, there are minor configuration options that the user will have to specify since they highly depend on the environment where the assessment is run.

One such example is the Lateral Movement test, specifically the scenarios "Lateral Movement through PAExec" and "Lateral Movement through WinRM." The first scenario will need a list of target machines, as well as valid credentials for these machines, to effectively perform the lateral movement. A similar case is the Lateral Movement through WinRM. Although it does not need the list of target machines since by default it will do a network scan to determine the possible targets, we recommend giving specific internet protocol (IP) addresses to avoid waiting the time that this network scan needs to complete across that target network. This scenario will also need valid credentials for the target machines to be specified.



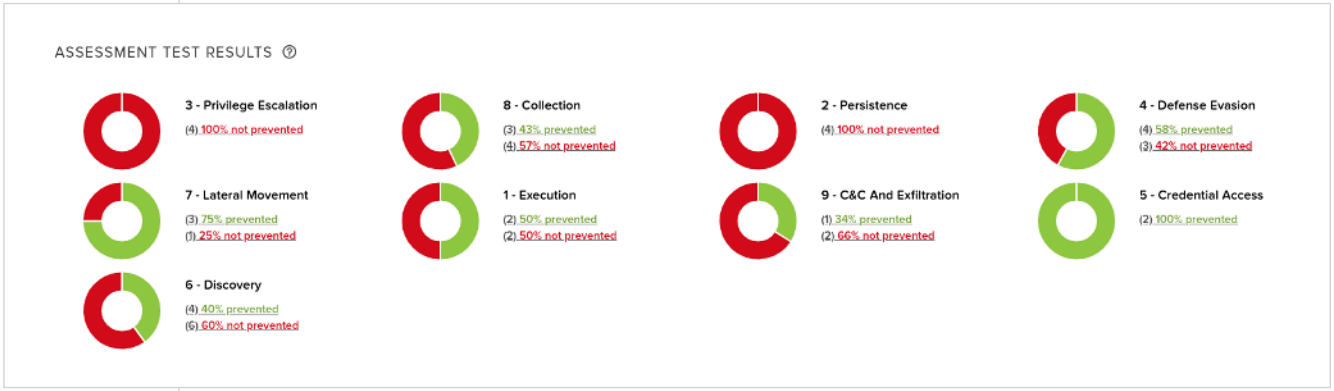

The other option that we leave for the user is deciding in what assets every test will be run. One option would be to run all tests in all assets, but in most cases it makes more sense to restrict some tests to "low-value" assets (those that might be easily accessed but that have less valuable information) and some other tests to the "high-value" assets.

For instance, it would make sense to execute the Lateral Movement test only in low-value assets (from which an attacker would try to access more protected assets from that source), while the Collection, Command and Control, and Exfiltration tests would be best run on high-value assets due to the likelihood of being targeted for their content. To configure the assets for a test, you only have to click on the three dots on the right side of it, and a dropdown will be displayed with the "Manage Assets" option:



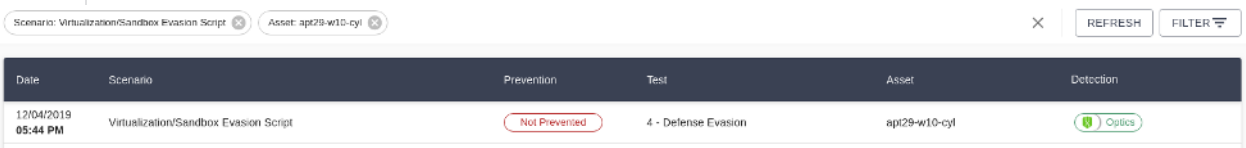
## Analyze the Results - Take Decisive Action

After running the assessment, it's time to analyze the results and take decisive action. From inside the assessment, navigate to the Findings section, where you will be able to find different visualizations of the outcome of the assessment. For instance, you will see a breakdown of the prevention results by test:



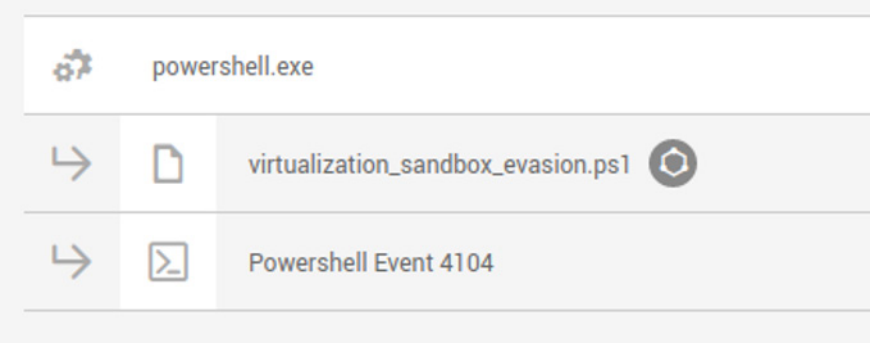

You can also go to the Mitre ATT&CK Heatmap, where with a simple look you will grasp in what MITRE ATT&CK tactics and techniques your defenses are the strongest or need to be improved. We can also select to display the detection results instead of prevention:


If you want a closer look to determine what worked as expected and what did not, it's time to go to the Results section. There you will find the prevention and detection outcomes broken down for each scenario and asset. Be sure to check out the filtering options to only display the results for a specific asset (or group of assets, like the high- or low-value assets), test, or scenario that you are interested in. For instance, in the following screenshot, we filtered the results by the Virtualization/Sandbox Evasion Script scenario for a particular asset, and we see that it is detected by CylanceOPTICS:



Clicking on the scenario will take you to a detailed view where you will find the different actions that have been taken in the scenario, mitigation recommendations, and Indicators of Compromise (IOCs).

Finally, we can check the CylanceOPTICS console directly to see all the data that has been captured by the EDR related to this scenario. For instance, we can see the process tree that triggered this alert:




Digging further within the console, we can also show the command line arguments of the PowerShell command, or we could even show the contents of the PowerShell script by clicking on the PowerShell Event above.


## Leverage all this information to improve your defenses!

## Improve and Repeat

After this process, you will be able to determine how your tools and team respond to a full attack chain from a real-world threat actor. Take your time to analyze all the results, determine improvements, and take proper actions. Once you are done, we would suggest repeating this exercise and measure how you evolve over time. In the end, achieving a mature security posture is a matter of time, analysis, and having the right data to assess the areas of improvement.

AttackIQ is excited to offer the APT29 Assessment Template precisely to help you and your team meet that goal.

# Recommendations

To learn more, please go to our website resource section and consider downloading these additional publications:

## A CISOs Guide to MITRE ATT&CK

**https://go.attackiq.com/CISOS-GUIDE-TO-MITRE-ATTACK_LP-Website-Organic.html**

Getting Started with MITRE ATTACK https://go.attackiq.com/WF-19Q1-MITRE-ATTCK-WP_Registered-Website-Organic.html

## A CISOs Guide to Breach and Attack Simulation

**https://go.attackiq.com/CISO-GUIDE_LP-Website-Organic.html**

To view a demonstration or participate in a free trial of the AttackIQ award winning BAS platform, please reach out to **info@attackiq.com** or visit us at **www.attackiq.com**.

# References

**The Dukes: 7 years of espionage (F-Secure).** **https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf**

**Operation Ghost. The Dukes aren't back - they never left (ESET).** **https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf**

**Threat Group Cards: A Threat Actor Encyclopedia (ThaiCERT).** **https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf**

**Who Is COZY BEAR (APT 29)? (Crowdstrike)** **https://www.crowdstrike.com/blog/who-is-cozy-bear/**

**Bears in the Midst: Intrusion into the Democratic National Committee (Crowdstrike).** **https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/**

**MITRE ATT&CK Evals: Round 2 Technique Scope** **https://attackevals.mitre.org/methodology/round2/scope.html**

ATTACKIQ
U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com

AttackIQ, a leader in the emerging market of breach and attack simulation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ® supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying that defenses work as expected. AttackIQ's platform is trusted by leading companies around the world. For more information visit **www.attackiq.com**. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.