Continuous Security Validation Against an Ever-Changing Landscape

Matt Bromiley

A SANS Product Review

Continuous Security Validation Against an Ever-Changing Landscape

Written by **Matt Bromiley**

February 2021

Sponsored by:

Cymulate

Protecting Your Security Investment

Many organizations have spent considerable time and resources building security programs to protect their users and data. Despite those best-laid plans, attackers still find ways to infiltrate systems, leaving personnel stunned to find that their security controls did not work as expected (if at all). This lands the organization in the unfortunate position of having to explain why controls failed while simultaneously responding to an incident. Far too often, incidents are disclosed and the organization ends up with a public relations nightmare to boot.

To bridge the gap between expectations and capabilities, consistent and thorough security control testing is required. This advice is not new, but it is often easier said than done. Due to complexities, penetration tests are scheduled as infrequently as possible and are narrowed in scope and impact—rules that threat actors do not care about when they set their sights on your organization. We think it is time to think of security control validation as a must-have, on-demand capability—one that is effective in highlighting the security weaknesses of an organization—so that security teams can prioritize remediation and implementation where necessary.

In this whitepaper, we examine a platform that aims to do exactly that: **Make security validation a standard, daily activity for your organization.** Cymulate Continuous Security Validation, or Cymulate, is a highly integrated, customizable platform built around testing the security controls of your organization—*whenever you see fit*. In addition, Cymulate recently took its platform to the next level, offering resources that allow you to craft your own purple team-style assessments of your enterprise. Furthermore, as a SaaS platform, it is extremely simple to deploy and can be fully operational within an hour.

Our favorite takeaways from working with this platform include the ability to do the following:

- Craft custom Purple Team assessments of our environment that align with the MITRE ATT&CK® Matrix.
- Pivot from to-the-minute intelligence reports to security control testing, offering a real-time answer to the question, "Are we defended against this?"
- Use Full Kill-Chain APT assessments to emulate a known threat actor from end-to-end and uncover APT weaknesses that an attacker could easily exploit.
- Gain executive-level insight into how the organization fared against various assessments by viewing Cymulate's reporting mechanisms.

Overall, we had a fun time working with Cymulate's platform. We believe that the customization of the various assessments situates this tool as a valuable resource for both blue and red teams, allowing them to create automated validations with subtle tweaks unique to their organization. As we worked our way through the platform, we quickly realized that this was more than just blue or red team testing. There are myriad use cases for a platform such as this. We will examine two of them, both relevant to the modern enterprise security posture.

Similarly, as you work your way through this paper, we encourage you to consider how your organization currently tests your security controls. Do you have validation in place, or are you simply hoping your tools will stop attacks? Furthermore, how does your security stack compare to the techniques attackers are using today, not yesterday? It is time to find out.

Cymulate offers 11 modules for attack simulation, covering the entire Cyber Kill Chain®. The Purple Team module, which we assess later in this paper, is perhaps the most powerful, combining red team and/or threat actors' attack techniques with blue team defenses and detections. The goal is for each side to get smarter and for the organization to be better protected.

Getting Familiar with the Platform

Our journey with Cymulate begins with the initial dashboard. This is where most analysts begin their validations and where management and stakeholders go to assess the current state of the organization. The initial screen provides an intuitive, albeit unique, perspective into the state of the environment. Figure 1 provides a snippet of the initial dashboard.

Figure 1. Cymulate Dashboard, Showing Real-Time Security Validation Status of an Organization

We found this initial dashboard both intuitive and informative, providing real-time insight into assessments that have been performed within the organization. They are appropriately aligned with key threat actor objectives, such as Initial Foothold, Execution and C&C, and Network Propagation. Each score is interactive and provides granular details, as shown in Figure 2. This granular information details baselines, organization trends and assessment time frames.

Cymulate also provides high-level statistics from a control, infrastructure, endpoint and full kill-chain perspective. We loved this view for one simple reason: It allowed us to log in—once—and get an overview of where the organization currently stands. Notice the largest score provided is the Overall score, a number the organization would obviously want to keep as low as possible.

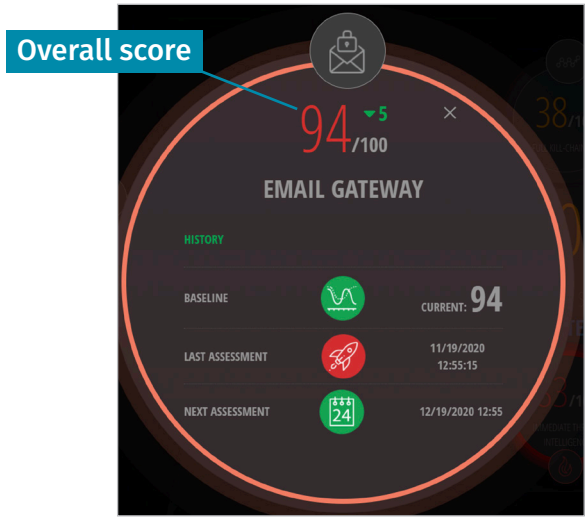

Figure 2. Email Gateway Assessments: Showing Overall Score and Granular Details

Equally useful is a preview of the Immediate Threats alerts, delivered via a sidebar in the dashboard (see Figure 3). Immediate threats are pulled from various threat intelligence sources and turned into rapid-fire assessments that you can run against your organization. (We will examine this capability in a subsequent section.)

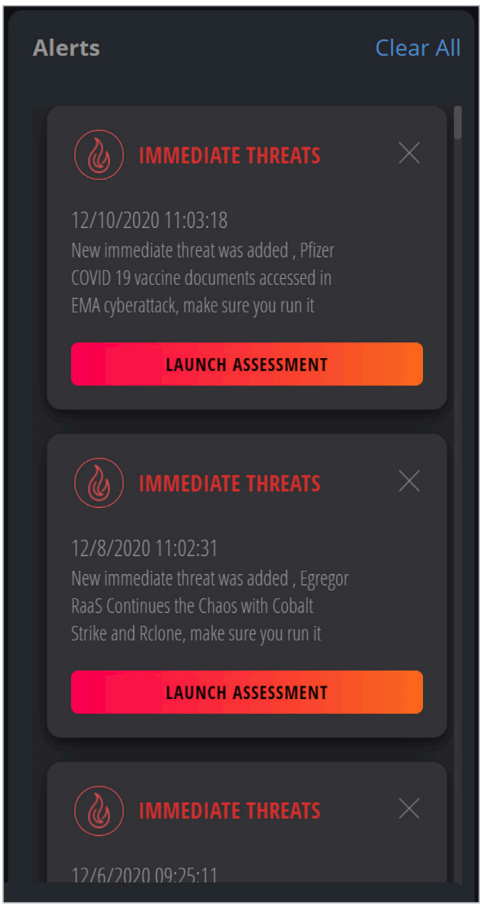

Figure 3. Immediate Threats Alerts

> One requirement for optimal use of Cymulate's platform is to reconsider how you characterize your environment. Rather than simply defining your environment in terms of *endpoint* or *network*, start thinking of your environment as *attack vectors* or *objectives*. Testing for lateral movement, for example, focuses on the success of the technique, much as an attacker would. Thinking of the environment from an attacker's perspective makes for better defenders.

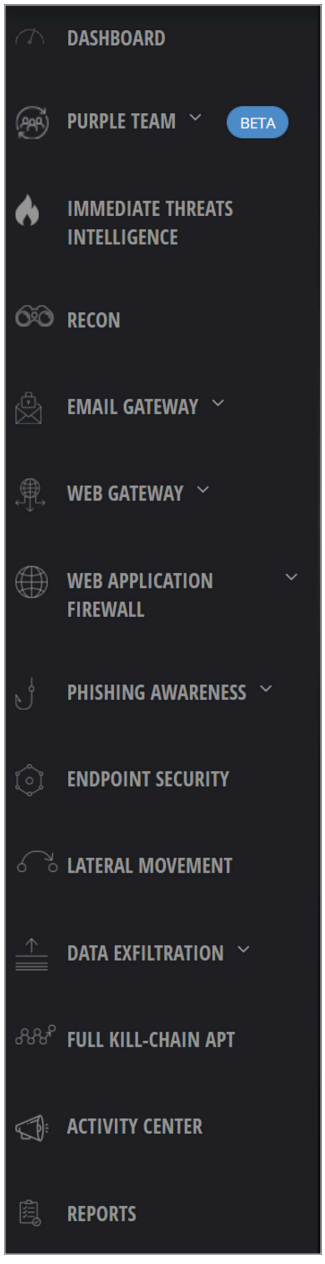

Figure 4. Assessment Options

As analysts delve deeper into the platform, Cymulate organizes the various assessments in the same manner in which they were scored. Thinking of the environment from an attacker's perspective—a necessity for success with Cymulate—helps navigate to assessment for Recon, Lateral Movement or Data Exfiltration (see Figure 4).

Cycling through each option presented in Figure 4 allows an analyst or security engineer to examine, schedule and conduct various assessments. The platform is comprehensive, covering the entire cyber kill chain from reconnaissance to impact. The Recon module provides visibility to manage the external attack surface; the vectors allow security teams to challenge and optimize individual layers of defense and infrastructure; and the Phishing vector tests employee security awareness.

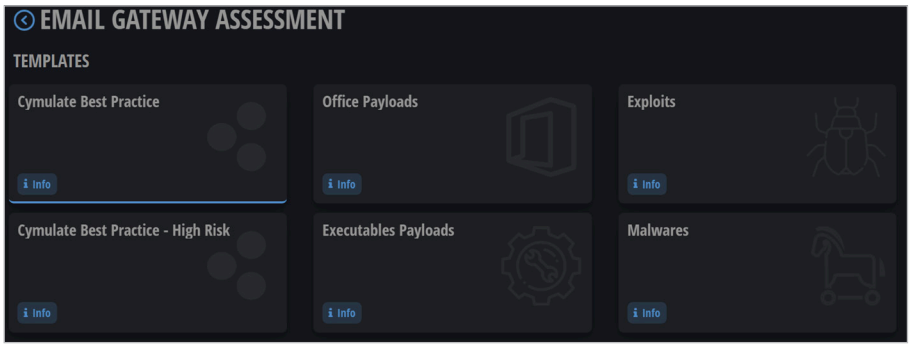

Figure 5. Email Gateway Assessments

Focusing on Email Gateway, for example, allows an organization to conduct various assessments via a variety of delivery mechanisms. As shown in Figure 5, an organization can launch assessments that test email gateways (and thus defense/detection/response capabilities) for exploits, office payloads, malware or executable payloads—to name

just a few among *many*. There are a multitude of assessments available, and Cymulate also allows for the creation of custom assessments to fit your unique environment. However, during our initial assessments, we were satisfied that nearly every email gateway we have encountered had thorough testing available out-of-the-box.

For further customization, your team can also upload its own payloads or utilize the standard ones that Cymulate offers (shown in Figure 6).

Figure 6. Payloads for Email Gateway Testing

The ease of this process speaks volumes to the engineering work that Cymulate has done behind the scenes. We found it incredibly simple to put together various assessments with different payloads and behaviors, reversing what is typically a complex VM- or lab-driven process involving multiple hours of work. It dawned on us: **Why aren't security controls tested with greater frequency?** The complexity of maintaining a test environment and emulating threat actor activities is an arduous one. Cymulate's platform has simplified, if not nearly eliminated, this process.

Advanced Enterprise Testing

Focused testing of the individual vectors, such as Email Gateway or Phishing Awareness, is extremely important to validate their efficacy and optimize their performance. However, threat actors rarely target one and only one piece of an enterprise environment. They typically utilize whatever systems and means are necessary to accomplish their objectives.

Immediate Threats Intelligence

One of our favorite features of Cymulate's platform is the Immediate Threats Intelligence capability. Shown in Figure 7, Immediate Threats Intelligence pulls from multiple sources and threat intelligence feeds to show organizations *what is happening in the threat landscape today*.

One of the most common scenarios in today's threat landscape is reading about a threat and immediately wondering whether your organization is defended against that very threat. Cymulate thought of this. It quickly turns news and/or intelligence sources into assessments you can run on demand. We love it!

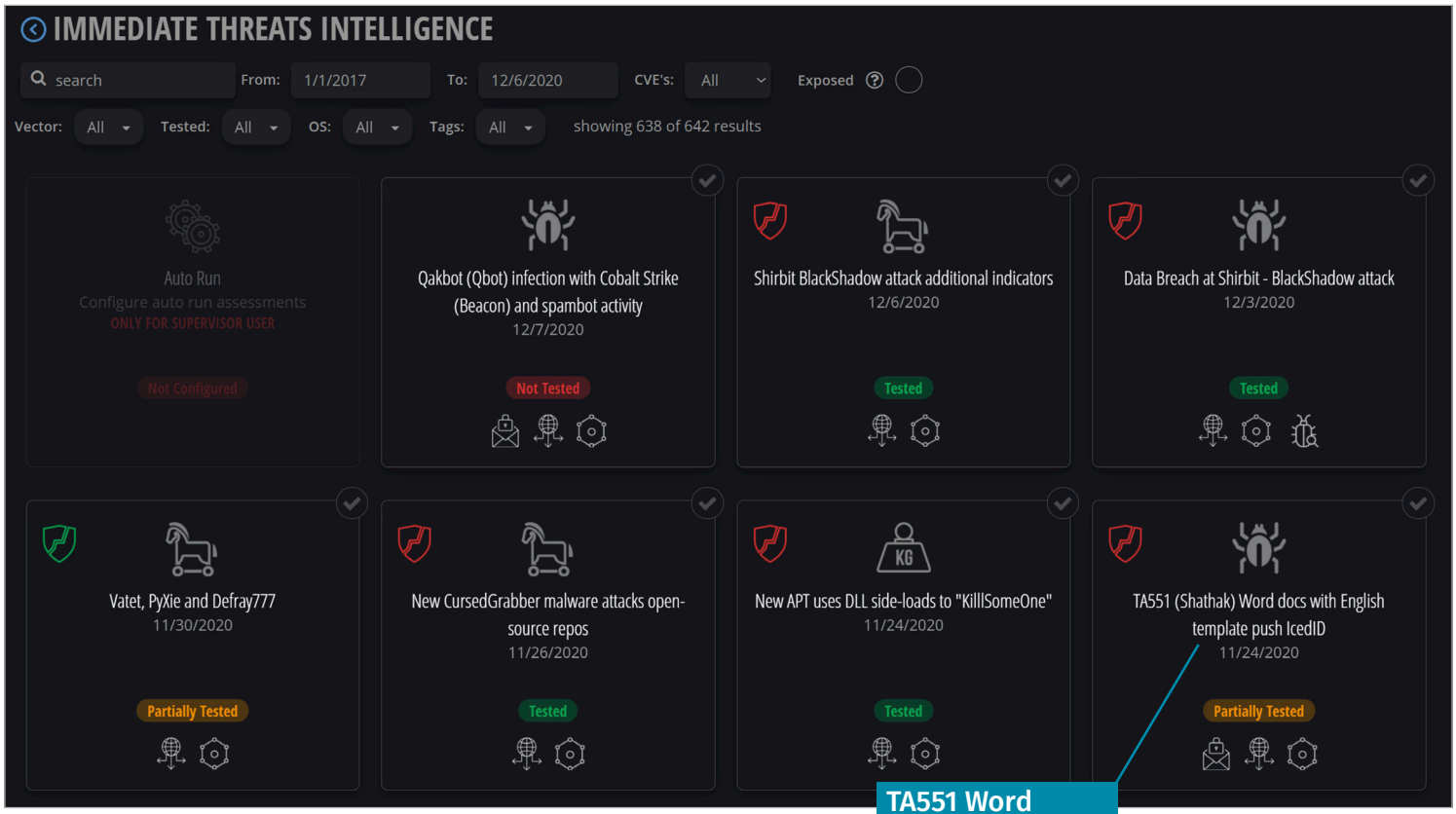

Figure 7. Immediate Threats Intelligence Feature

Not only can analysts see what threats are out there today, but they can also quickly pivot to testing their own environment. For example, as shown in in Figure 7, a report on 11/24/2020 showed the threat group TA551 utilizing Microsoft Word documents to spread **`IcedID`** malware.[1] The SANS InfoSec Handlers Diary Blog provides a rather extensive walkthrough of examining this email-based threat.

[1] "TA551 (Shathak) Word docs push IcedID (Bokbot)," Aug. 7, 2020, InfoSec Handlers Diary Blog https://isc.sans.edu/diary/TA551+%28Shathak%29+Word+docs+push+IcedID+%28Bokbot%29/26438

As an information security analyst, you want to know whether your organization is defended against this threat. Examining this threat further in Cymulate's platform (see Figure 8), you can see that this attack involves opportunities for email and web gateways, as well as endpoint security for detection and/or mitigation. Here is the best part: You can run one or all these assessments *straight from the console*. You can also set the assessments to run automatically, with email notifications sent upon completion.

It is hard to quantify how great this feature is, both in automation and the time saved by an analyst. The ability to read a source about a particular threat and then immediately test that threat against the environment is a huge benefit to security analysts. At the time of this paper, our platform had both Endpoint Security and the Web Gateway tested, allowing us to set and view a benchmark as we improve security controls.

It is worth noting that Cymulate also collects and provides the relevant indicators of compromise (IoCs) from each threat for the analyst (see Figure 9). However, this platform saved us the effort of collecting IoCs for the purpose of posterity. Knowing how your environment stands up against a threat is extremely valuable data.

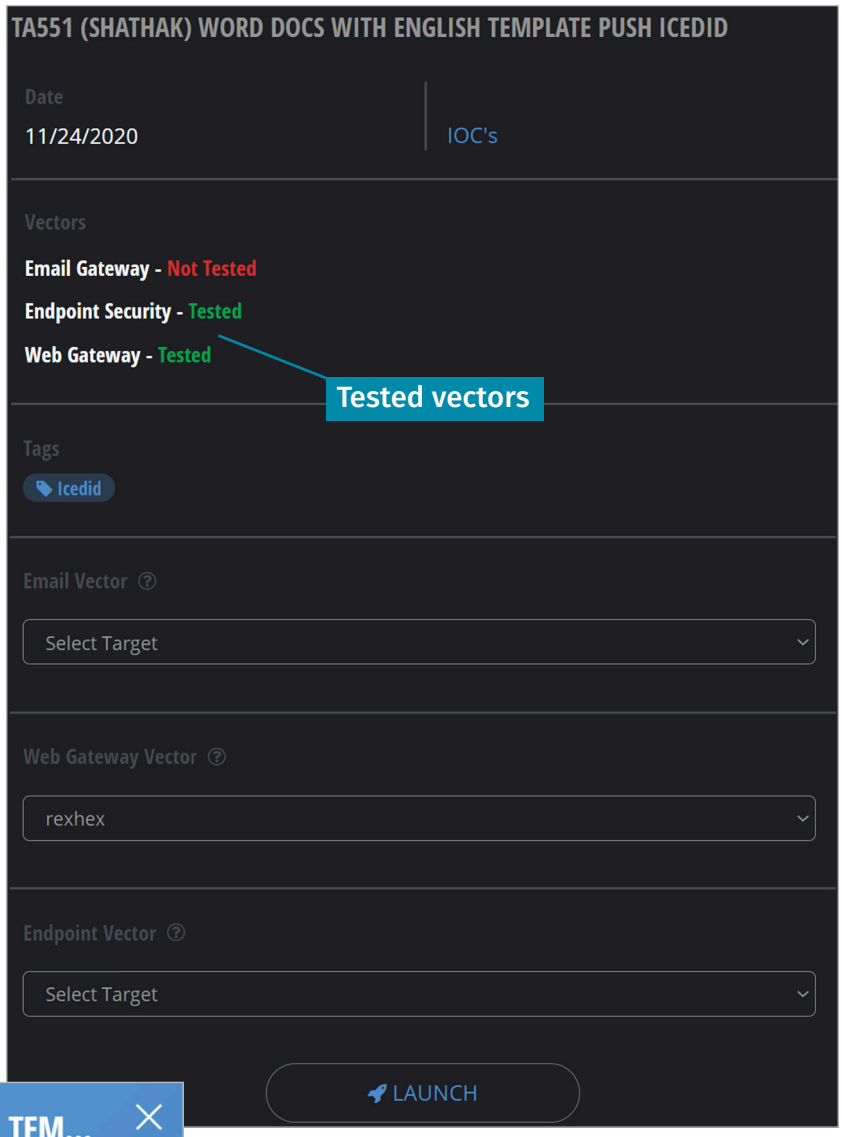

Figure 8. Immediate Threats Intelligence Dashboard: TA551 Word Document Threat

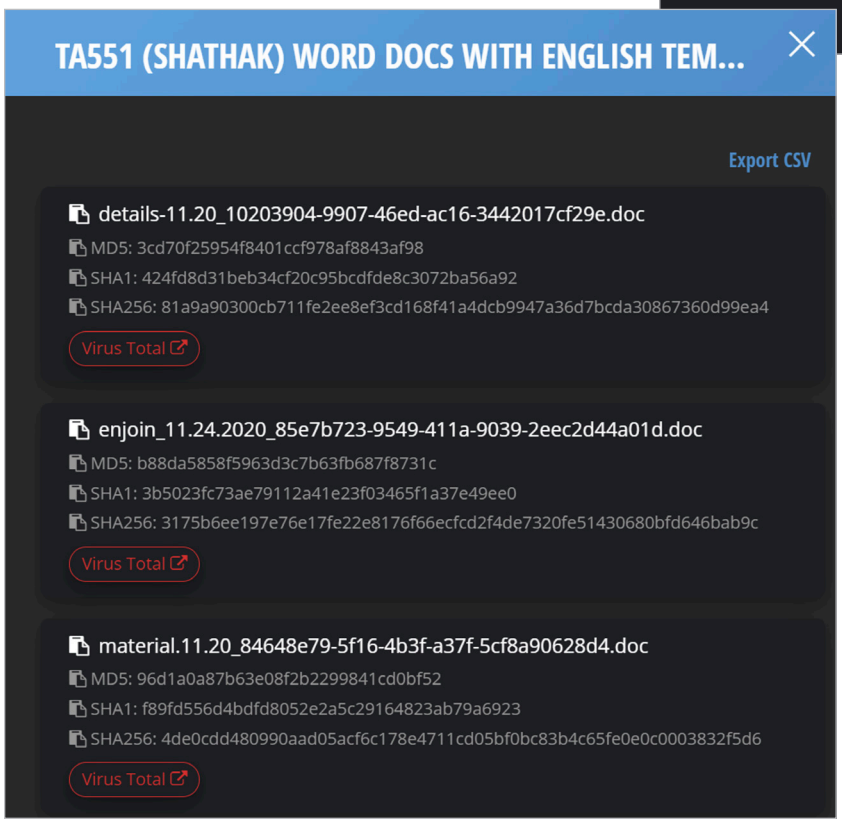

Figure 9. IoCs from an Immediate Threats Alert

As we mentioned in the previous section, alerts from Immediate Threats Intelligence are also streamed directly into the initial dashboard, allowing analysts to stay in front of what attackers are doing out in the wild.

With all assessments, knowing the outcome is just as important as being able to run the test. By quickly navigating to the Reports section, we can view how effective our environment was at defending against this TA551 threat (see Figure 10).

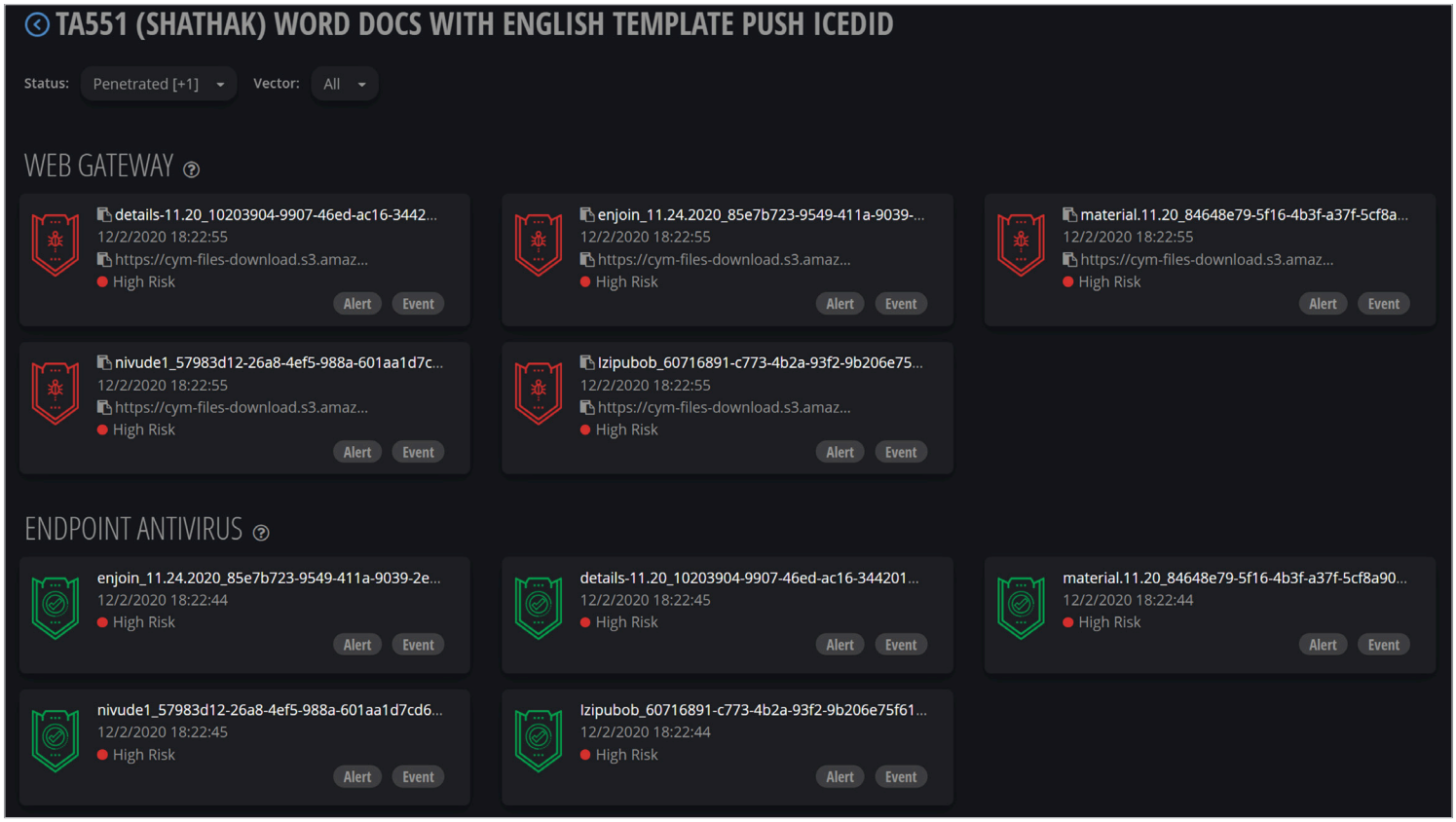

Figure 10. Assessment Results

Figure 10 shows that we potentially have a few holes in our security stack. While endpoint antivirus successfully detected and blocked the objects from this assessment, our web gateway failed to detect and/or alert on this content. This disparity gives our security team a chance to pause and address these concerns. In looking at these results, a few questions come to mind:

- Should our web gateway have detected this threat?
- Does the associated traffic pass through the gateway?
- Do we have any whitelists in place that, based on source, allowed malware into the environment? (Note in Figure 10 that the malware was hosted in an S3 bucket.)
- What steps do we need to take to rectify these results?

You should constantly be asking your security team questions about threats, but if they do not have a vehicle to answer them, you will forever be in doubt. These questions usually get asked during incident response. With Cymulate's platform, we were able to quickly assess a threat, test it against our environment and plan our fixes. All without suffering an actual incident.

It is imperative that organizations ask these kinds of questions *before an incident occurs*. Unfortunately, what happens is often the opposite. Incidents and data breaches tend to shine the most light on weaknesses within an environment, which is too late in the game.

Full Kill-Chain APT

On-demand testing against immediate threats is an impressive feature, one that we feel gives organizations the advantage over attackers. Via continuous testing, an analyst team can provide up-to-the-minute feedback on exploitations, mitigations, and remediations. However, established threat actors combine more than one technique. In fact, threat groups are typically a collection of techniques and tactics repeated in various incidents. Cymulate offers end-to-end testing as well, via its aptly named Full Kill-Chain APT module.

At a high level, many organizations may not see the value in testing for the full kill chain of a threat group. Let us hypothesize that your organization's early warning detection systems—web and email gateways, firewalls, and so on—detect a known threat group. Does this omit the need to implement security controls further on in the attack, to identify how a group may move laterally or exfiltrate data? *Of course not!* Determined, resourceful and capable threat actors will find ways around security controls; therefore, we must test as much of the kill chain as we can. That is the only way to build confidence that your early warning systems are effective enough.

Looking at a snippet of the Full Kill-Chain APT Assessment dashboard (see Figure 11), you can see that Cymulate has pre-populated multiple threat actors for quick testing in your environment.

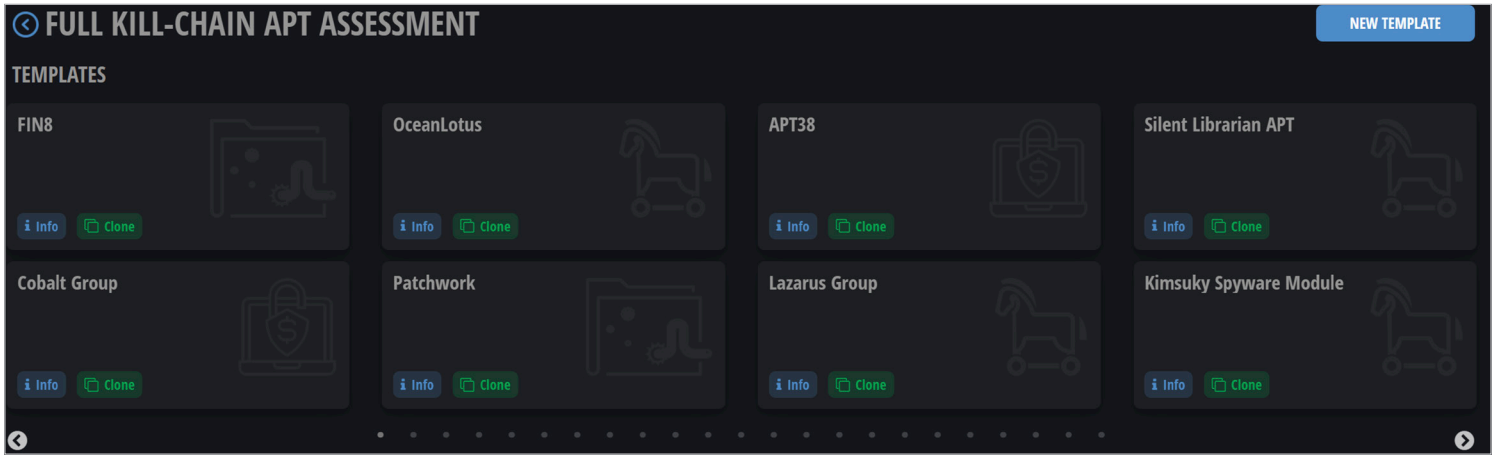

Figure 11. Full Kill-Chain APT Assessment Dashboard

These groups are classified via the public names they are associated with, such as FIN8 or OceanLotus. Security personnel can easily migrate from an article, blog or threat intelligence feed to their own platform and perform a correlative assessment. Output is viewed just as we did with Immediate Threats Intelligence—via insightful, detailed reports delivered via the Cymulate platform (see Figure 12 on the next page).

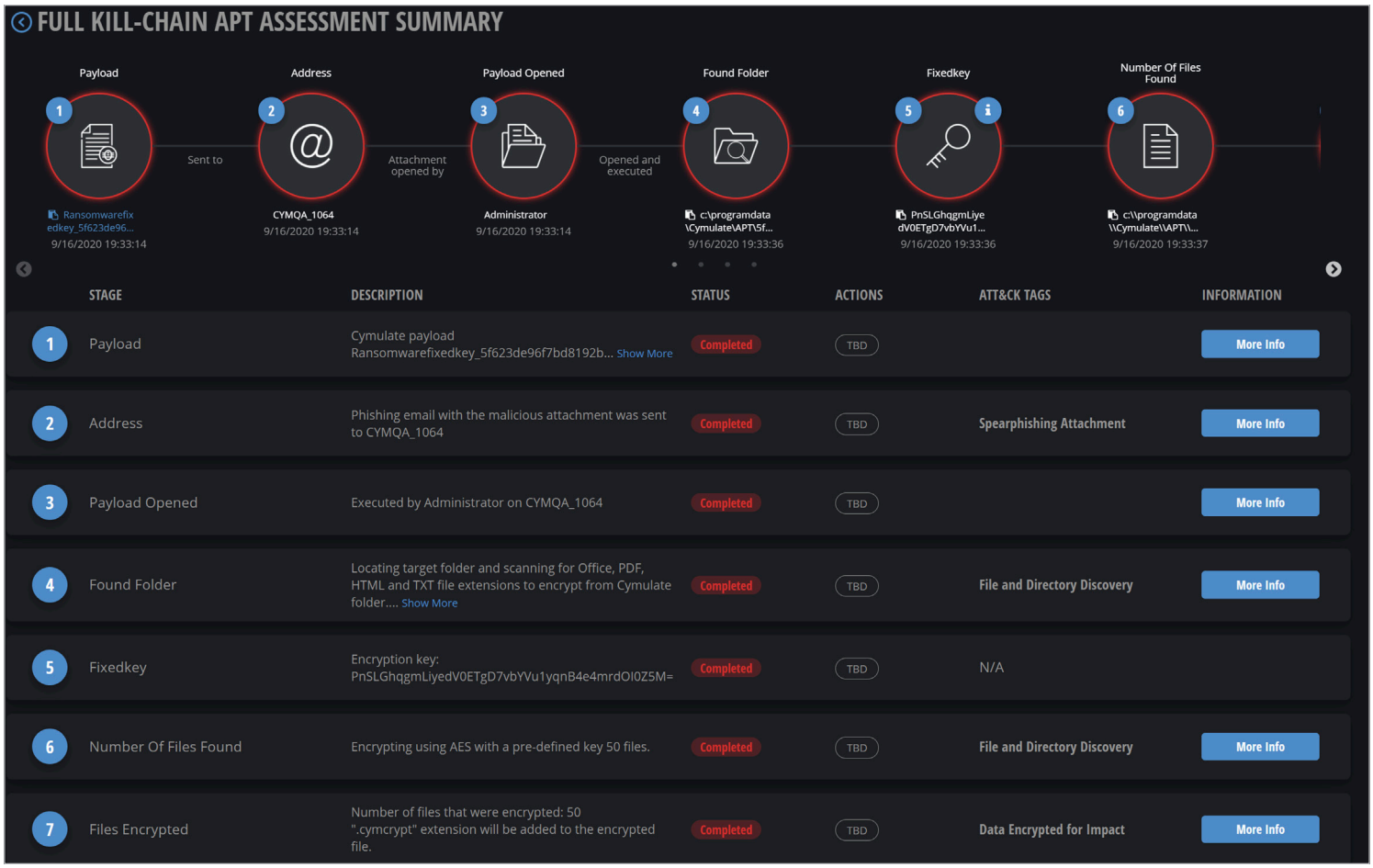

Figure 12. Full Kill-Chain Assessment of APT38

Figure 12 shows the results from an APT38[2] assessment. A North Korean-backed threat actor, APT38 has been known to deploy ransomware and impact data within victim environments. Cymulate's platform allowed for this process to be repeated and tested within our environment, showing us where our defenses were in protecting against the attack.

As you can see, we scored a perfect score on this environment—not a good sign. The assessment was able to successfully receive the spearphish, execute the payload, perform file and system discovery, and ultimately ransom the files on our test agent. Cymulate even provides a helpful play-by-play timeline showing the events as they took place (see Figure 13).

It is here we must pause and make sure readers understand the power of what just happened. We successfully emulated techniques used by a known, well-resourced threat actor and discovered where our weaknesses lie. Fortunately, we did not have to suffer an actual data breach to know that we need to tune our security stack. We love this outcome!

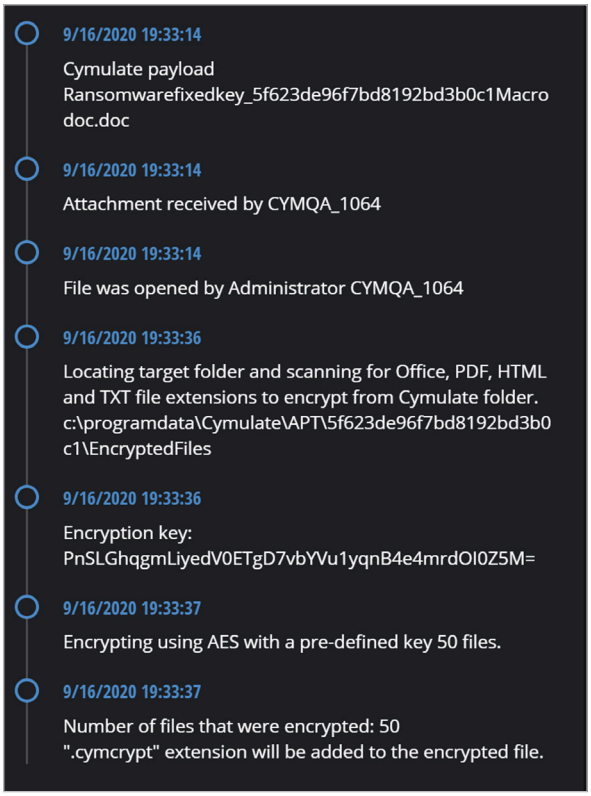

Figure 13. Timeline of APT38 Assessment

[2] "APT38," Mar. 30, 2020, https://attack.mitre.org/groups/G0082

The ability to know how your organization would compare against known techniques is invaluable knowledge that every defender should be armed with. You may have noticed that with this assessment, our email and endpoint defenses were tested—and failed. Based on this simple assessment, which took all of 23 seconds in our environment, we now know to focus our defense resources on tuning endpoint security and enhancing spearphishing detection. The chained attack pattern elevates our assessment capabilities above ad hoc testing, while still pinpointing where our organization needs to improve.

Purple Teaming

A brand-new feature, still in Beta at the writing of this paper, that we were excited to test during our product evaluation is the Purple Team functionality. This is perhaps the most powerful capability in Cymulate's platform, bringing together all the benefits of the Immediate Threats Intelligence and Full Kill-Chain APT features, while simultaneously providing a mechanism via which *red teams* can also deliver customized assessment services.

As we mentioned earlier, the benefits of Cymulate to the blue (defense) teams is quite apparent. While testing, in a few examples we came dangerously close to saying, "We may not need to run a penetration test again!" Of course, that is not the case. In fact, the Purple Team module does quite the opposite. It empowers red teamers to create custom assessments that allow them to utilize Cymulate's delivery mechanisms with their own techniques, creating a powerful, on-demand red team assessment vehicle.

The Purple Team module itself is broken down into a handful of capabilities. Whereas the other assessments we analyzed, such as Recon or Email Gateway, are simple-to-use assessments and resources (such as a payload or an email address), Purple Team is the opportunity to truly make Cymulate work for your environment.

The Purple Team navigation pane (see Figure 14) includes not only the overall dashboard, but also custom templates, assessments, assurance, resources and scheduling capabilities. There are powerful options inside of each.

The Purple Team dashboard begins with the ATT&CK Matrix, as shown in Figure 15 on the next page, compared to your organization. Based on Purple Team assessments that have been conducted, users can quickly see where they have failed and succeeded from an ATT&CK perspective. We cannot think of a more impactful statement than a screen that shows successes and failures from a technique perspective.

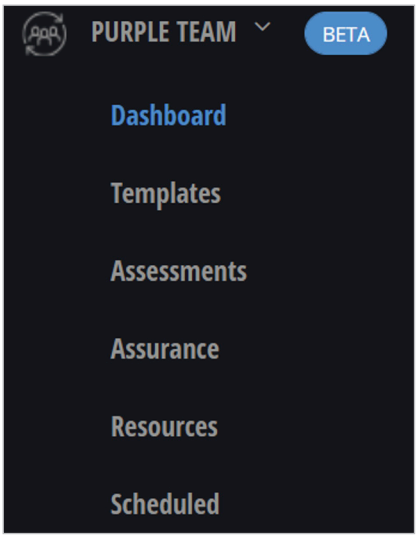

Figure 14. Purple Team Navigation Pane

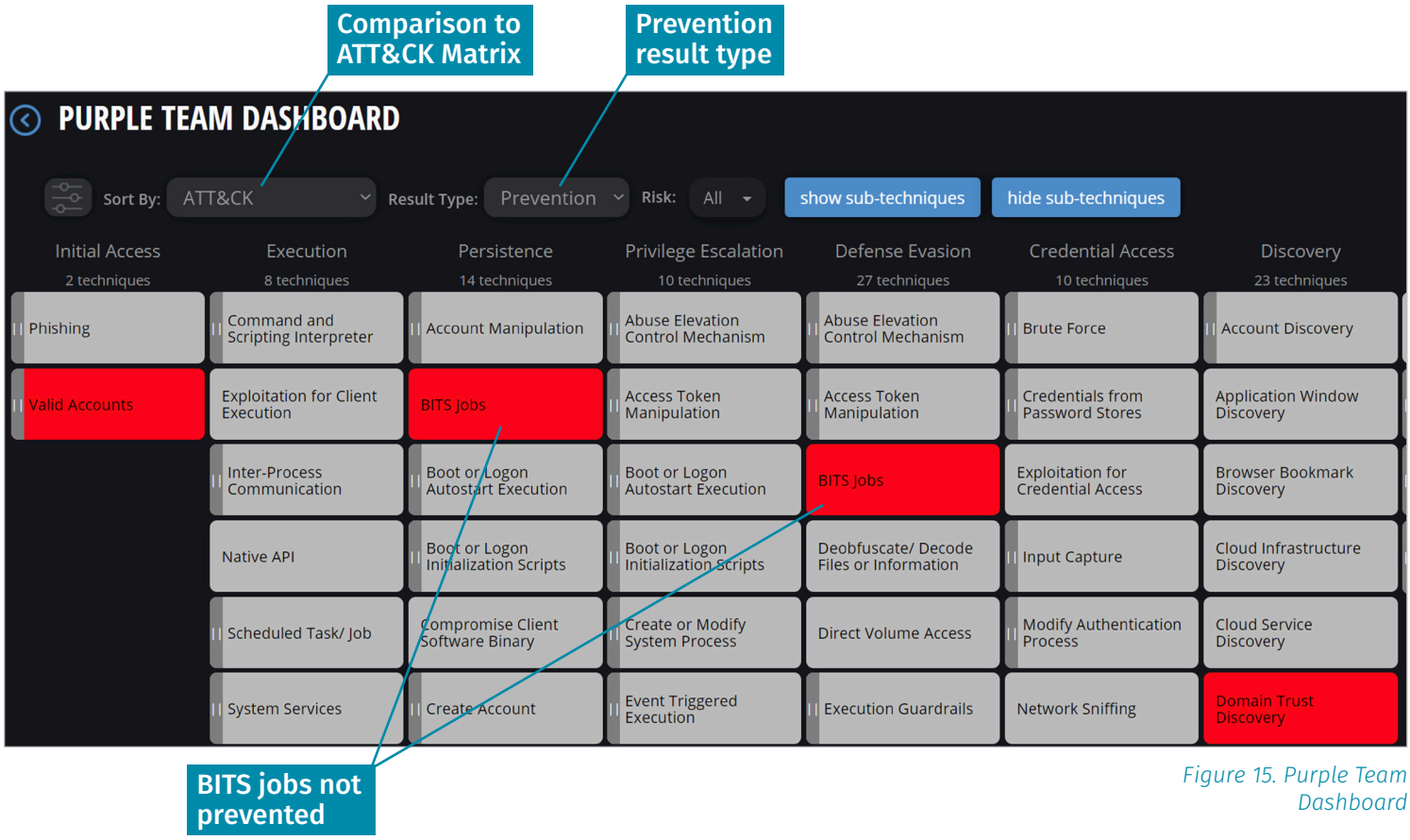

Figure 15. Purple Team Dashboard

For high-level users this is enough detail to start thinking about how to change security resource allocation. Based on Figure 15, it appears that our organization failed to prevent (notice the Prevention result type) BITS jobs from a recent assessment. This provides a novel opportunity to sit with the team, analyze this activity and determine the best course of action: Is this something we can even prevent, or do we need to accept the risk?

As technical analysts and red teamers, we can drill down into the various assessments offered. This is perhaps our favorite part of the Purple Team capability: constructing assessments that resemble attack patterns within an environment. Figure 16 provides a snippet of the pre-populated templates Cymulate provided during our assessment.

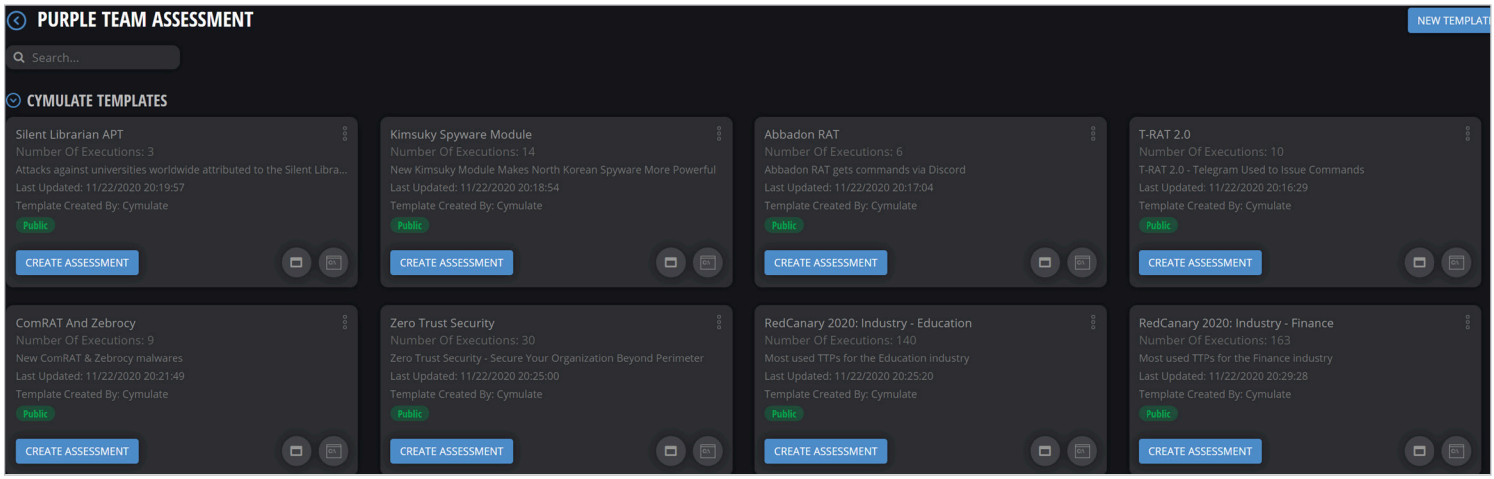

Figure 16. Purple Team Assessment Templates

We can use these powerful, pre-populated assessments on their own to test our environment. The difference in these assessments as opposed to those available in Full Kill-Chain APT, for example, is the ability to completely customize and modify our activities. Let's drill down deeper into one of these assessments, shown in Figure 17.

Initially, we can see that this assessment is a series of "scenarios" chained together to replicate a particular type of activity. (Think of a scenario as a single activity, such as running a script or creating a registry key.) In the example in Figure 17, we can see the assessment is designed to install and execute a service, modify a **`RunOnce`** registry key, and then establish logon scripts.

These are all mechanisms to establish persistence on a victim system, compiled into a single scenario. Here is the best part: We can drill down into the technical details of what *each scenario* is configured to do (see Figure 18). We can view the technical steps behind each scenario and examine the commands being executed. Furthermore, a red teamer or offensive tester can *modify each detail to their liking* (see Figure 19).

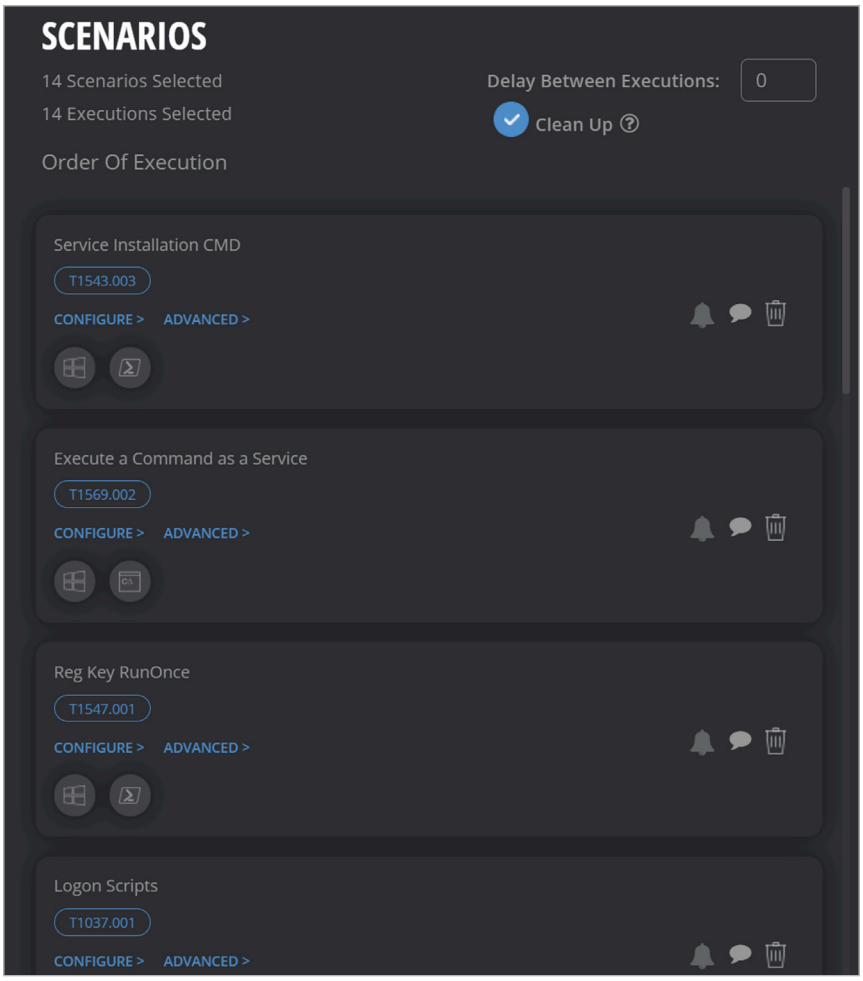

Figure 17. Scenarios from a Purple Team Assessment

Figure 18. Service Installation CMD, a Scenario from a Purple Team Assessment

Figure 19. Inputs and Success Indicator from a Custom Purple Team Scenario

These functionalities allow for red teamers to modify the various Purple Team assessments to their liking; customize commands, inputs, and outputs; and run assessments just as they would a normal offensive penetration test—all via the Cymulate platform in a repeatable, reportable fashion.

For even further customization, red teamers can either copy an existing template (all of which Cymulate makes freely available) or create their own from scratch. Cymulate makes assessment creation *incredibly easy and fun*, something we hope will encourage more security validation in the future. Figure 20 shows a snippet from a sample assessment that steals credentials via **`Mimikatz`** and then uses those credentials to use **`PsExec`** to move laterally throughout an environment.

Note that Cymulate offers both text- and graphical-based options for creating assessments (see Figure 20). We loved them both but were amazed at how easily the graphical version allowed us to create complex, chained scenarios. The entire interface is dynamic and data-aware, meaning it only displays chainable options for the actions that you have selected. For example, once we found stolen credentials from a system, we could chain together lateral movement or data exfiltration, among many other steps.

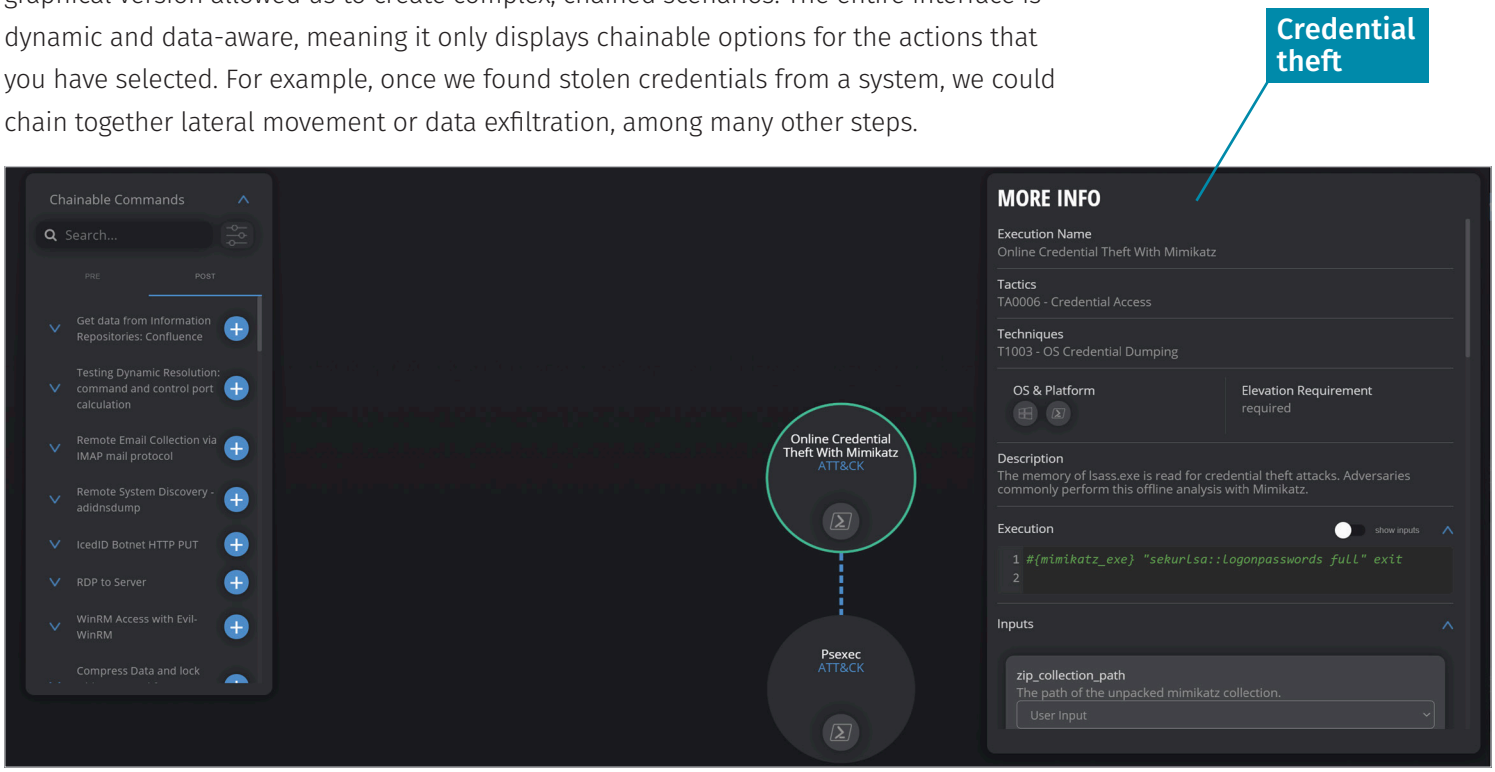

Figure 20. Custom Assessment Creation

The Purple Team module has so many capabilities, we spent a lot of time simply building multiple assessments to test various parts of our organization. We truly feel that this is a platform that can empower red teamers to create consistent, impactful assessments of their clients' or organization's environments and utilize the data output to laser focus where the organization needs to improve.

The platform also allows organizations to schedule purple team assessments, a huge benefit for taking advantage of maintenance windows, new software deployments and changes to the environment. The scheduling feature also means that teams can create assessments ahead of time and develop their own testing schedules, perhaps enabling continuous testing of the environment. We love it all!

Use Cases

Having on-demand security validation capabilities is much more than simply replicating penetration tests or attacker techniques within your environment. As we have examined, Cymulate allows for total customization and control over the testing of your controls. This allows your organization to prepare for a multitude of potential scenarios and use cases, including incident detection and response exercises, SOC validation, and even pre-purchase product evaluation. Furthermore, as your security landscape and posture change, Cymulate Continuous Security Validation will keep pace, changing with the needs of the organization and the security team. See the following two use cases for examples.

Use Case #1: Securing a Remote Workforce

Prior to 2020, organizations were already seeing an uptick in remote workforces, with more and more organizations allowing for flexible working plans. The COVID-19 pandemic only accelerated these numbers, with some organizations moving to 100% remote workforces. Unfortunately, while the enterprise landscape may have changed, the role of the security team did not.

The Problem

A virtual workforce often means relying on remote access solutions and cloud providers. Given a majority, if not all, staff members working remotely, how can you ensure that your security controls are protecting employees and data when they are not physically within the corporate network?

The Validation

Cymulate's platform can be tailored to focus on the impact of remote endpoint compromise, lateral movement through the corporate network and/or targeting of third-party cloud providers. Cymulate's Lateral Movement Assessment, for example, is a fantastic resource to identify the impact of stolen credentials from a corporate system (see Figure 21).

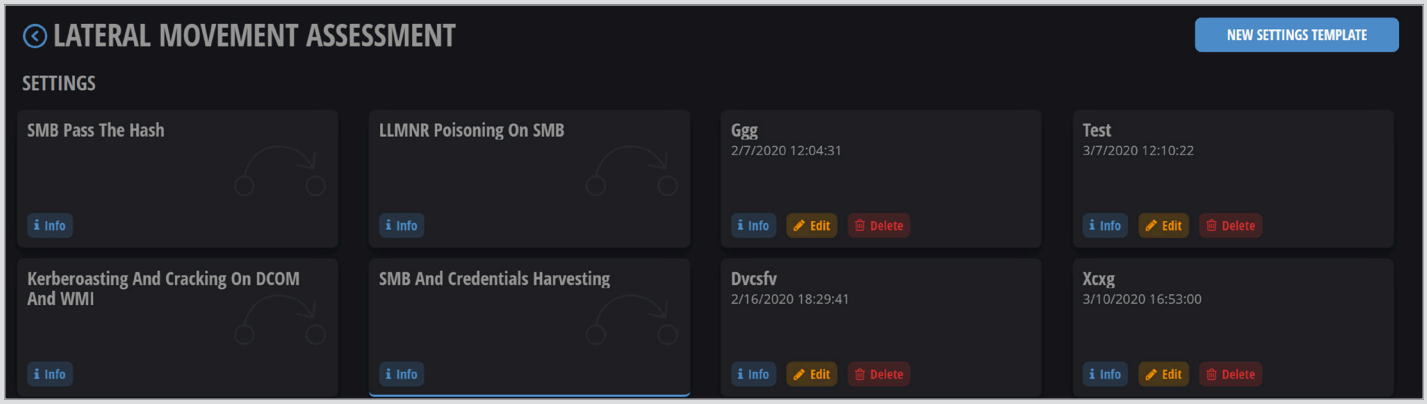

Figure 21. Lateral Movement Assessment Default Options

The platform also integrates with other tooling, such as a vulnerability management system, enabling security teams to identify weak systems within the environment and ways attackers may exploit those weaknesses.

Use Case #2: Protecting Against Third-Party Integrations and Supply Chain Attacks

The modern security enterprise is not an island of technology. Today, most networks include assets secured by the organization, as well as connections to third-party organizations that provide various services. Unfortunately, these third-party integrations often serve as the weakest link in the chain, providing an excellent entry vector for patient threat actors.

The Problem

Despite having connections into your environment, third-party providers often do not fall under your security purview. This creates a security paradox. Someone has access into your environment, but you do not secure their assets. How can you ensure that a third party doesn't get compromised and ultimately allow threat actors into your network?

The Validation

Cymulate's platform offers assessments for Recon, Web Application Firewall and/or Phishing Awareness, for example. It can also simulate lateral movement from an initial foothold, such as a third-party software or service. Security teams could use these assessments in conjunction with a third-party to perform a security assessment of their organization's environment. Figure 22 shows an example of lateral movement activity as simulated and detected by Cymulate, beginning from an initial foothold and expanding through the organization.

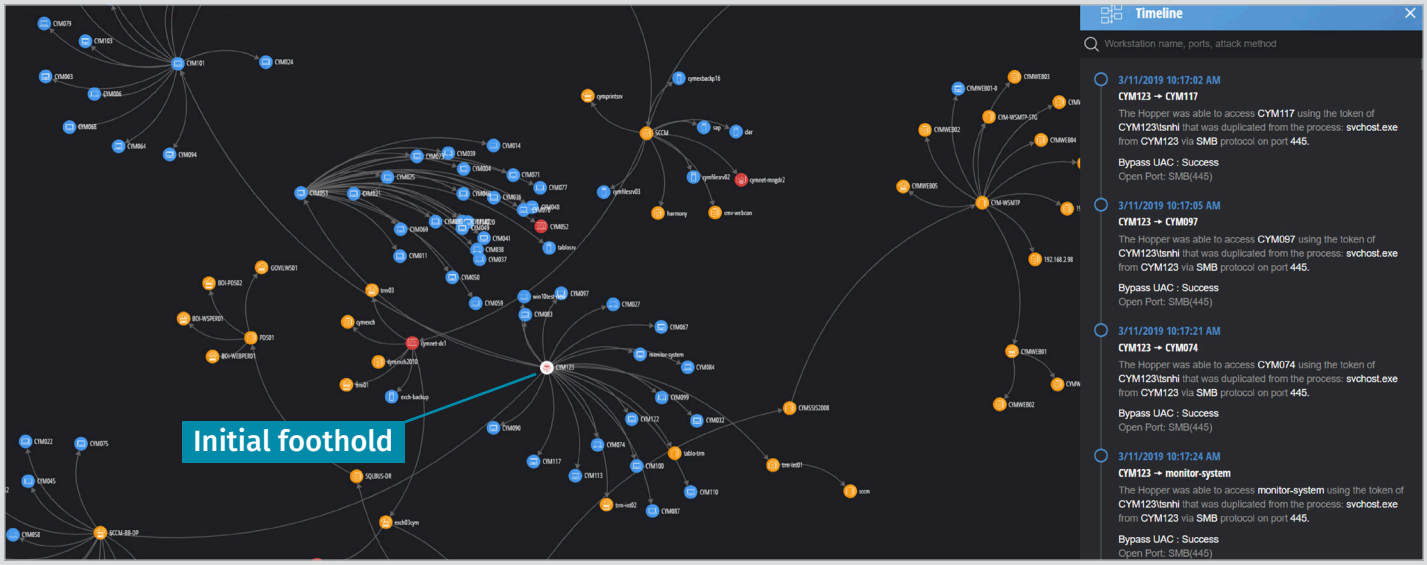

Figure 22. Lateral Movement: Attack Path Visualization from a Compromised Endpoint/Initial Foothold

Of course, your organization could also go full steam ahead and ask your third parties to conduct a Full Kill-Chain APT assessment, offering them the ability to find weaknesses throughout their entire organization and hopefully securing them—ultimately securing the link with your network as well.

Closing Thoughts

It is a difficult day when your organization suffers a data breach—made even more difficult when your top-notch security stack failed to prevent or detect the attack in time. Once you have deployed your various technologies, the question still lingers: Is this security investment going to protect my organization? Waiting for an attack to test your security controls is not acceptable. How can you be sure that your security program is working effectively?

In this SANS review, we examined Cymulate Continuous Security Validation—Cymulate's answer to these questions. As a validation and testing platform, Cymulate has brought together an extremely intuitive and easy-to-use platform that allows security teams to go as granular as testing a single exploit against a single control, all the way to running an entire APT group playbook against the environment. Furthermore, an integration with real-time threat intelligence feeds means that we can test our organization against the techniques and tactics being used *today*—not yesterday.

Organizations face too many complexities to ignore the benefits of continuously testing their controls. Cymulate packs a lot into its platform—and we found a lot of reasons for organizations to consider on-demand, or continuous, security validation. Threat actors gain momentum, skill sets and new tooling daily. It is time to stop allowing attackers to have the advantage in your environment.

About the Author

Matt Bromiley is a SANS digital forensics and incident response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and FOR572: (Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is a principal consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory and network forensics; incident management; threat intelligence; and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor: