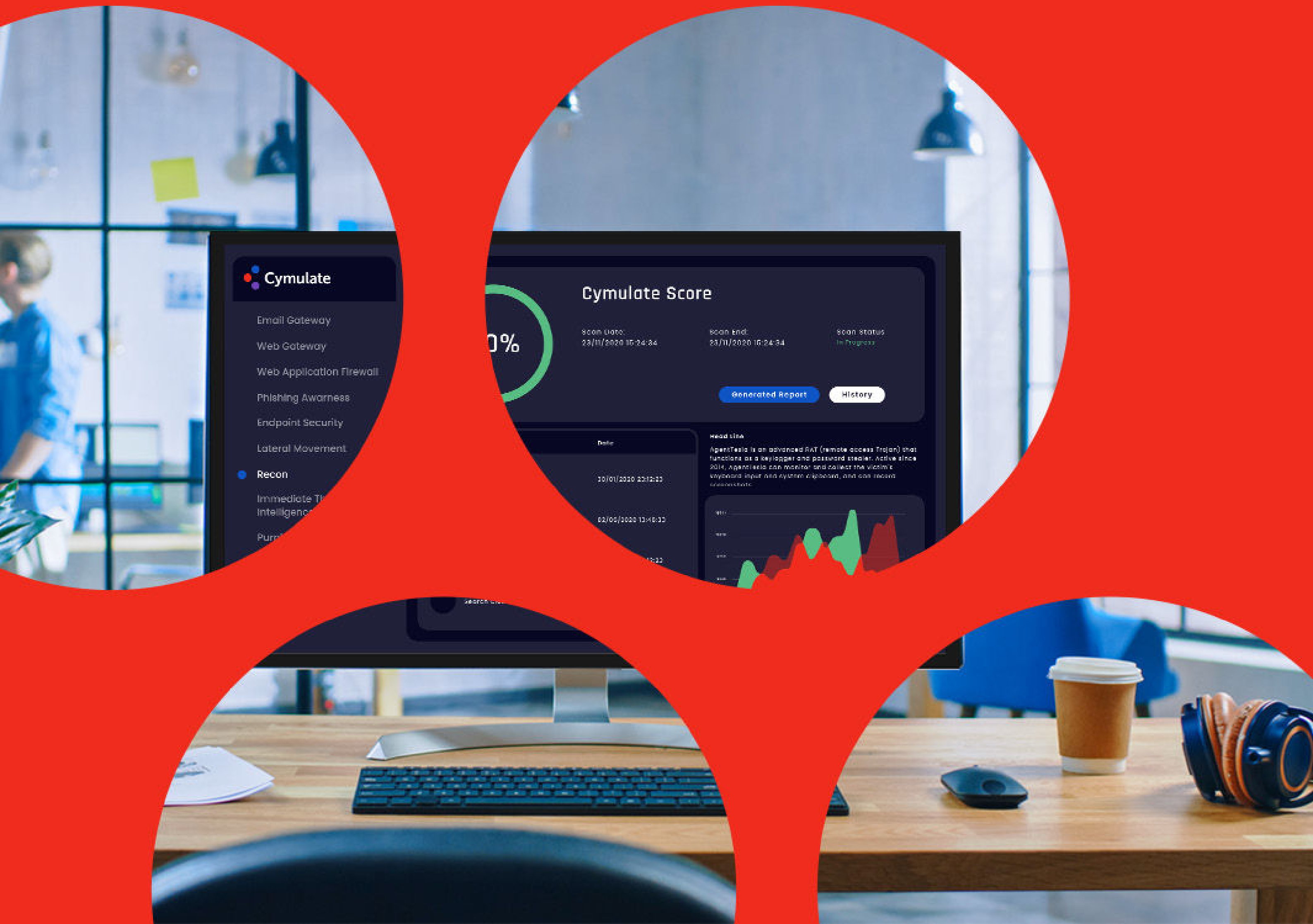
Cymulate
Extended Security Posture Management

The Benefits of Integrating Security Intelligence with Security Validation



01 Introduction

Continuous security validation automates security testing by launching attack simulations that are safe to run in the production environment. Implementations vary in the extent of coverage across the kill chain. This paper, intended for security, risk and compliance managers, will describe the benefits of integrating security intelligence with security validation, and the value of extending the coverage of automated testing to the MITRE pre-attack phase; the reconnaissance a threat actor performs prior to launching an attack.

> “If you know your enemy and yourself, you need not fear the result of a hundred battles.
> If you know yourself but not the enemy, for every victory gained you will suffer a defeat.
> If you know neither the enemy not yourself, you will succumb in every battle.”
>
> -Sun Tzu, The Art of War

In cyber security context, Sun Tzu’s quote can be interpreted to knowing your organization’s strengths and weaknesses, seeing them through the eyes of an adversary and knowing their tactics and techniques. There are various security programs that allow you to **know yourself**; programs that reveal your organization’s vulnerabilities and help you evaluate how your security operations prevent, detect, and respond to a breach. These programs include vulnerability management, security control validation, security auditing, penetration testing, red team exercises and employee security awareness programs.

Threat intelligence programs allow you to **know your enemy** by providing information on the evolving threat landscape and deception technology. By far, the most common approach of threat intelligence programs is black box penetration testing. This emulates an adversary and attempts to penetrate the network, providing insights on the tactics, techniques, and procedures (TTPs) that were successful. However, black box penetration testing is limited because:

- The scope is typically restricted so it doesn’t disrupt business operations.
- The outcome relies on the skill level of the tester.
- It provides only a periodic (typically yearly) snapshot in time.

A relatively new set of services has emerged that provide a detailed view of an organization’s attack surface as seen from the outside. These services perform reconnaissance of an organization’s web and IT infrastructure and of their connected third parties. Where reconnaissance performed by attackers and penetration testers will look for a limited number of conduits into the organization, these automated services continuously assess a much broader attack surface for all potential entry points. They provide an organization with valuable information by uncovering attackable weaknesses. It is when such weaknesses are put into attack context - and when the methodologies of successful simulated attacks are brought to light - that they enable defenders to know their enemy.

This paper will discuss the importance of incorporating a hacker’s reconnaissance (recon) findings with continuous security validation. By connecting the adversarial steps of the full kill chain and providing insights to threat actor TTPs, security teams can know their enemy and become significantly better defenders.

02 | Security Intelligence and its Impact on Cyber Risk

In its simplest form, cyber risk is a measurement of cyber exposure: the probability of a breach, adjusted for the potential loss and damage associated with such a breach.
The possibility of a successful breach is based on the combined capabilities of your people, technology, and processes, compounded by the skill, tactics, techniques, and technology of your opponent.
When defining potential loss and damage, each organization must define what the potential impact might be. For example, the impact of a breach will be wildly different for an organization that is tasked with acquiring and obtaining highly privileged data, compared to an organization that only holds publicly available data.

The key takeaway is that the impact of a breach cannot be ignored simply because it is difficult to quantify. An organization can manage risk more effectively by knowing its cyber strengths and weaknesses, measured up to the enemy's TTPs, and when they are fully aware of the overall impact a breach or disruption can cause.

The intelligence that adversaries gather prior to initiating an actual attack (recon) has an impact on the probability of an attack succeeding and its overall outcome before the attack even takes place. Recon provides attackers with information that serves to their advantage, but it can also become a deterrent. For example, if the information gathered by an adversary does not reveal significant weaknesses and it paints a picture of a meticulous IT operation with strong defenses, it may put them off, preventing the attack from taking place.

In a physical conflict the enemy is usually known the physical attack comes with clearly identified physical attackers. In digital attacks we don't know much about the adversaries or how many there are, but we do know their tactics and techniques.
By looking at your organization from the outside, through adversarial eyes, you can assess cyber risk levels in three steps:

Information Gathering
Discover what an adversary can learn about you.

Weakness Identification
Identify your perceived weaknesses from the perspective of the adversary.

Test Weaknesses to Assess
Evaluate what is actually at risk, and if the weaknesses can be exploited.

By taking this approach, security teams get to know their enemy better; protections can be optimized, and risk mitigation efforts can be prioritized. Large and multi-disciplined security teams are more likely to perform full recon and in-depth testing, however, companies with smaller teams will find this approach more challenging to scale and achieve.

03 Information Gathering and Weakness Identification

There are different types of information that can be collected on a target during the recon phase. These include both technical information related to applications and infrastructure exposed to the internet, and information about the organization and its people.
The information can be categorized as following:

Finding Category	Findings	Outcomes
Application	Application and platform vulnerabilities and weaknesses used to breach web applications.	Identifying application vulnerabilities, outdated software versions, and CVE’s can lead to client-side exploitation attacks. The risk level of the aggregated findings indicates the susceptibility to a web application breach.
Human Factor	Information used in social engineering attacks, including: • Contact information • Account information • Hacked emails • Compromised passwords	The risk level of this category is determined by the quantity and severity of the findings. It indicates the susceptibility of an organization to a targeted social engineering attack.
Counterintelligence	Corporate related information circulated by hackers and indicators of malicious intent, including: • Email addresses flagged with malicious activity • Similar domain names that may be used in phishing attacks • Darknet mentions	The risk level of this category is determined by the quantity of findings and their severity. It indicates a level of malicious intent.
Network and IT	Network and IT security weaknesses and vulnerabilities, used to breach IT infrastructure including: • Sensitive open ports • Blacklisted hosts • Defaced hosts • Open cloud storage buckets	The risk level of this category indicates the susceptibility to a network security breach.

The data collected by recon provides four perspectives for a security team to address:

The Attack Surface

The attack surface is a fragmented landscape which can contain many unknowns to the security team. One part of the attack surface includes digital assets owned by the organization, which are hosted on third party uncontrolled platforms, and managed by different business groups or teams.
Another part of the attack surface includes shadow IT services, testing, or staging deployments on-prem or in cloud environments, and unsanctioned SaaS based services. Knowing what is exposed to the outside world is key to improving your security and identifying weaknesses that an adversary can take advantage of.

IT Hygiene

IT hygiene is the high-level view of the attack surface. Use of up-to-date software and infrastructure; timely certificate updates; and shutting down unused domains, environments, and applications are some common attributes of high IT hygiene. Large enterprises will have many externally accessible assets, and not all of them may be maintained and up to date, or even protected by more recent security controls. These are indicators of potential and actual weaknesses and will attract adversaries to investigate further.

Technical Weaknesses

Technical weaknesses include all the underlying misconfigurations, application and web infrastructure vulnerabilities, and known vulnerable systems that can be found after discovering and fingerprinting the externally accessible assets of an organization. Leaked credentials, tokens, and weak or compromised passwords and password hashes also represent potential weaknesses. Testing can determine if these weaknesses are exploitable by an adversary, and associate a risk level to help prioritize remediation efforts.

Indicators of Malicious Intent

The attack surface is a fragmented landscape which can contain many unknowns to the security team. One part of the attack surface includes digital assets owned by the organization, which are hosted on third party uncontrolled platforms, and managed by different business groups or teams. Another part of the attack surface includes shadow IT services, testing, or staging deployments on-prem or in cloud environments, and unsanctioned SaaS based services. Knowing what is exposed to the outside world is key to improving your security and identifying weaknesses that an adversary can take advantage of.

04 Integrating Recon and Continuous Security Validation

> We welcome the addition of recon to Cymulate, it helps us measure, track and improve the security performance of our company and business ecosystem, it helps us assess and manage 3rd party risk which is a significant concern.
>
> -James LEE, Managing Director at Vertex Growth Fund

Recon sheds light on the attack surface, discovers information that is useful for an adversary, and identifies weaknesses for security teams to remediate. Incorporating recon into an organization's security validation program will increase its value dramatically.

While penetration testers will perform reconnaissance to find one way into a network, automated recon integrated with security validation will search for all potential information and points of entry; and simulate attacks (and/or use the discovered data to fine-tune attacks) to assess specific risks for prioritized remediation. Making it harder for adversaries to get in across all the potential points of entry, and blocking visible and discoverable weaknesses, makes your organization a less-enticing target and reduces the chances of an adversary's success if they do try to digitally attack. Breach and Attack Simulation (BAS) platforms that perform automated recon enable security teams to perform continuous security validation from the pre-attack phase and connect the dots between weaknesses and the risk they pose in the context of an attack. This allows security teams to quantifiably prioritize remediation goals based on the likelihood of attack and the risk associated with these varied attack points. Similar to BAS integration with Vulnerability Management systems, recon integration correlates attacks to vulnerabilities, without exploiting the vulnerability for non-disruptive testing in the production environment.

The result of a simulated attack on a system, correlated to vulnerabilities in that system, produces a much more complete picture of cyber risk. Weaknesses discovered by automated recon can be tested to determine:

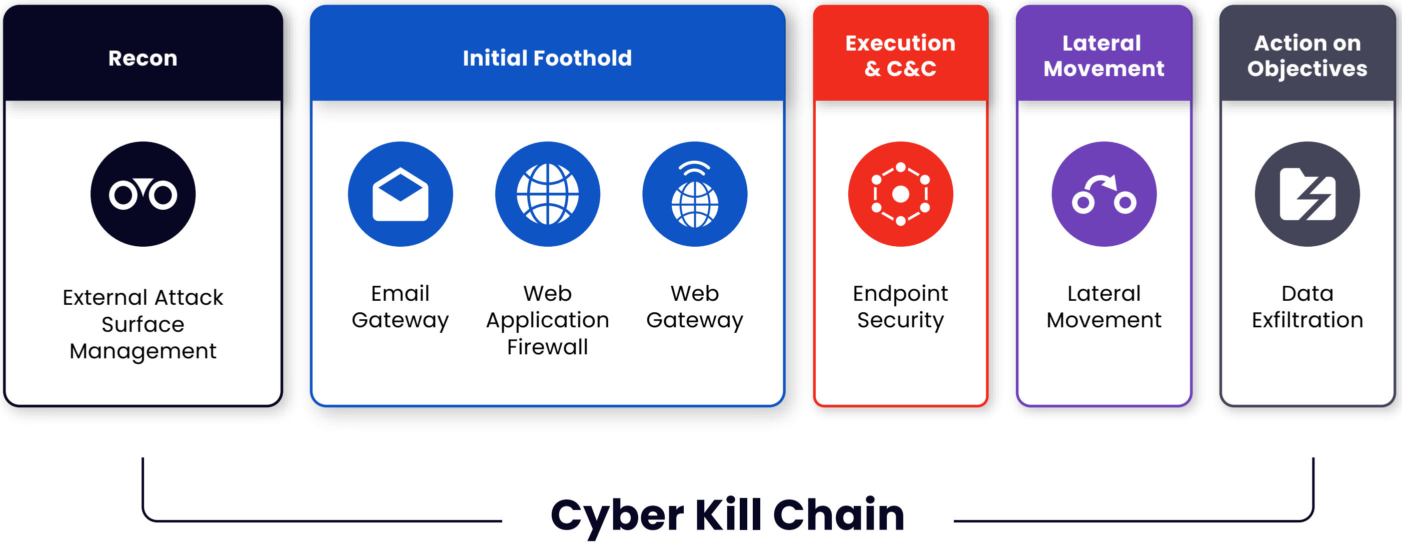
- If the weakness is exploitable
- What is at risk if it is exploited
- A risk score based on the severity of the weakness and the test result

For example, a vulnerability present in a specific web infrastructure component can be tested to determine if it is effectively protected by a Web Application Firewall (WAF) - a theory known as compensating security controls. While the vulnerability still exists in the web infrastructure, it cannot be exploited at present as the WAF compensates by blocking access to the vulnerability. As such, while the vulnerability will still need to be addressed, its priority should be lower than a similar vulnerability that is not currently defended by the WAF and is therefore immediately exploitable by an adversary. The exploitability of any given weakness combined with the potential cost of disruption or exfiltration of data, serve to quantify the cyber risk level and to prioritize risk mitigation efforts. Without this, prioritization becomes a subjective matter which can lead to significant risks being labeled as less important and leaving the organization in a high-risk state.

Continuous and automated, recon together with BAS have the additional benefit of assessing risk after every change that may inadvertently introduce a new security gap, whether they are routine administrative changes or in response to an event. Combined they make end-to-end security validation accessible and achievable even for security teams with limited resources.

05 Summary

Reconnaissance is key for an adversary working to select their targets and improve their chances of a successful attack, so much so that security frameworks such as the MITRE ATT&CK Framework dedicate entire sections to it. Security teams should integrate recon with their security testing and validation programs for a complete end-to-end simulation of the threats their organization faces. Adding recon to security analysis methodologies will uncover potential points of entry, improve testing procedures, and assess risk more completely. By assigning a risk score to recon findings security teams can prioritize remediation activity, optimize individual security controls, and mitigate infrastructure weaknesses in addition to validating their overall security architecture. By connecting the dots of the full kill-chain, security teams can get to know their enemy better and become better defenders.



About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data.
Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Contact us for a live demo, or get started with a free trial

Start Your Free Trial