SANS

Analyst Program

Whitepaper

The Advantages of Going Purple: How BAS Works and Why It Matters

Written by **Erik Van Buggenhout**

June 2022

PICUS

Introduction

In this whitepaper, we discuss the concept of breach and attack simulation (BAS) and the benefits of using such platforms. However, to understand the added value provided by BAS solutions, let's first consider the current state of affairs.

The Bad

Colonial Pipeline, Kaseya, SolarWinds, and Okta. All these companies have one thing in common: They became victims of cyberattacks (and not small ones). These high-profile attacks made the news due to the size of their fallout, which also affected the victims' customers and often resulted in not just cyber but also real-life or physical implications. Cyberattacks affect their immediate victims, but the consequences also ripple down to their customers, partners, and in many cases, society in general. In the case of Colonial Pipeline, for example, the attack resulted in six days of downtime, with several more days before operations returned to normal. Attackers stole gigabytes of data, and the pipeline shutdown caused fuel shortages as well as a state of emergency.[1]

When the news of another cyberattack hits, it would be short-sighted of us to assume the victim deserved it because of sloppy security. Victim blaming is pointless. Many of these companies have spent a significant cyber defense budget to prevent and detect possible attacks. However, the fact that they experienced compromises surely indicates something went wrong in their security control validation process. But what?

The Good

A boxer prepares for a fight by sparring. Companies can prepare for an attack by having a white-hat hacker target their systems and networks (technology) as well as their people and processes. Vulnerability assessments and penetration testing focus on the technical aspects to identify and exploit (in the case of an actual penetration test) as many possible issues on a fixed scope as possible. Red teaming adds people and processes to the equation, resulting in end-to-end attack simulations where a team of attackers tries to gain access to the target environment, followed by pivoting and accomplishing a specific set of objectives/flags. These types of tests are all useful in their own way. Combined, they serve different purposes, validating preventive controls and also assessing the blue team's detection and response capabilities.

That's right, the blue team or security operations center (SOC) is a key component in companies' cyber defenses. These unsung heroes hide behind multiple screens, whose duty it is to identify and investigate suspicious activity, triggering the incident response process to stop attackers in their tracks. To highlight the growing importance of this role, a job as information security analyst is at the number one spot of the U.S. News & World Report's list of best jobs for 2022.[2] In addition, the U.S. Bureau of Labor Statistics projects a 33.3% growth for information security analysts, with nearly 50,000 job openings by 2030.[3]

[1] "Colonial Pipeline Ransomware Attack," NATO Cooperative Cyber Defence Centre of Excellence, https://cyberlaw.ccdcoe.org/wiki/Colonial_Pipeline_ransomware_attack_(2021)

[2] "U.S. News Ranks the Best Jobs of 2022," U.S. News & World Report, https://money.usnews.com/careers/articles/u-s-news-ranks-the-best-jobs

[3] "U.S. Bureau of Labor Statistics," https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

If companies are aware that it is important to have a blue team looking out for attacks and to have a red team simulating attacks to validate prevention, detection, and response, why are adversaries successfully compromising (high profile) targets?

The Ugly

While companies are doing penetration testing and red teaming to validate their security controls, they often do it from a compliance-driven point of view. One-off exercises on a yearly basis to “check the box” result in underutilization of security controls. A clean vulnerability report at one point in time does not guarantee an absence of vulnerabilities one or six months later. The red team triggering an alert in your SOC during their exercise says nothing about the effectiveness of all the other detection rules. Neither does that alert test the same detection rule if attackers switch up their techniques or procedures. In addition, continuous execution of red team exercises is not the most cost-effective way to validate your security controls.

When the blue team spots an ongoing attack thanks to a detection triggering an alert, that is a victory, but it is a minor victory, making use of reactive measures that might come too late to implement any meaningful damage control. To prevent incidents, or at least detect them before attackers can inflict serious damage, blue teams need to proactively hunt for threats and create new detection cases based on relevant threat intelligence and gaps in their current detection capabilities. One-off exercises do not provide the view they need to implement such measures.

> **To prevent incidents, or at least detect them before serious damage can be done, blue teams need to proactively hunt for threats and create new detection cases based on relevant threat intelligence and gaps in their current detection capabilities.**

With continuous red teaming being cost-ineffective and defenders needing to proactively validate their security controls both in terms of prevention and detection, what options does an enterprise have to ensure its data stays safe?

Breach and Attack Simulation for Security Control Validation

Breach and attack simulation (BAS), a highly specialized area of cybersecurity, aims to help organizations automate security control validation. Some of the most basic properties of BAS solutions (shown in Figure 1) include the following:

- **Automated—**BAS provides the capability to automatically execute desired test cases against all endpoints and across networks.
- **Repeatable—**It should be possible to repeat a combination of test cases to revalidate previous results.
- **Continuous—**Automatable and repeatable, a BAS platform allows continuous validation of security controls by executing relevant attack cases consistently and rigorously.

Figure 1. Basic Properties and Enabler of a BAS System

A common denominator for most BAS platforms is the MITRE ATT&CK® framework, serving as an enabler to the aforementioned properties. Having become the de facto framework to model attack simulations and adversary behavior (in the form of tactics, techniques, and procedures, or TTPs), attackers and defenders alike use ATT&CK. MITRE ATT&CK enables BAS platforms to simulate realistic attacks by running a set of TTPs linked to a specific threat actor and validating whether a company's security controls prove effective against such an attack.

Environment-Specific Properties and Possible Pitfalls

The previous section presented the most basic requirements for a BAS platform, but your solution of choice depends on a variety of factors, including your current environment. Keep in mind these important properties:

- **Your ecosystem—**Know the elements of your ecosystem. What endpoints are in place and which operating systems are installed? Should all endpoints be included in the BAS platform? Ensure all operating systems are supported by the platform you want to implement.
- **Deployment—**When it comes to deployment options, certain BAS platforms are mostly cloud based, whereas others are fully hosted on-premises. Some solutions make use of agents that you must install on endpoints that you want to include in your simulations, whereas others use packages that you can execute without agents.
- **Your defensive technologies—**Can the BAS platform integrate into your defensive solutions, such as endpoint detection and response (EDR), security information and event management (SIEM), and security organization, automation, and response (SOAR)? If not, you essentially have two standalone solutions with a wall between the offensive and defensive aspects, at odds with the basic BAS properties. You don't want to be manually mapping test cases against security controls and the resulting prevention/detection.
- **Configuration—**Validate your BAS deployment and the results of your attack simulation and security control validation. You want to ensure that a specific test case was detected due to the employed technique and not because of other detections. Suppose, for instance, that you have a loose executable that would run five test cases, but based on static signatures, the EDR has flagged the executable as malicious. In such a case, you do not want the five test cases to be marked as successfully defended against because detection happened on the executable itself. In contrast, suppose that you have whitelisted your BAS agent in the EDR and want to test a process injection technique. Because of whitelisting, the EDR ignores further actions performed by the agent and your process injection technique is not alerted on, whereas it would have been otherwise. Ensure the proper configuration of your deployment before trusting the results.

- **Company size—**Although there is no hard requirement on the company size, neither in terms of minimum nor maximum, attackers usually consider the mid and small markets to be the “easiest” targets. These companies often do not have a large security budget, and in such cases, a BAS solution can provide the best bang for the buck. However, bigger companies with a large number and/or multiple layers of security controls can also greatly benefit from BAS solutions. Manual testing of all possible attack paths covering all security controls will be tedious and not cost-effective.

Despite its usefulness, organizations need to consider several caveats before deploying a BAS platform.

Security Control Validation

One of the more prominent use cases of BAS solutions is the validation of security controls. This validation includes making sure that every control in place is working as intended as well as testing and measuring their performance, both atomically and collectively, across prevention and detection layers. A good BAS solution provides the best return on investment by:

- Validating preparedness to prevent and detect the most relevant and latest threats
- Measuring and benchmarking the performance of security controls
- Supplying real-time data (either via continuous validation or on demand) to help prioritize defensive actions
- Obtaining actionable insights and recommendations to maximize utilization of tools

What security controls can BAS platforms validate? Every countermeasure aimed at minimizing security risks to physical or cyber assets is a security control, whether it is aimed at avoiding, minimizing, detecting, or responding to risks. However, for this use case, we focus on technical security controls aimed at protecting cyber assets. A simple example is ensuring the proper configuration of firewall rules to filter out undesired or malicious traffic, but a good BAS solution validates all technical controls, such as web/mail gateways, endpoint protection, data loss prevention (DLP), cloud defenses, IDS/IPS, IAM/PAM (identity and access management / privileged access management) solutions, and SIEM.

We cannot validate all of these controls in the same fashion. Some require validation in terms of prevention, whereas others are better suited for detection validation. See Table 1 on the next page for an overview of common controls and desired insights corresponding to prevention and detection.

As a result, security control validation identifies missing or misconfigured security controls and determines their efficiency against potential attacks. Security control validation, however, is just the first step in advancing to a higher security posture.

Table 1. Common Controls and Insights for Prevention and Detection

	Prevention	Detection
Common Controls	• Firewalls • Next-gen firewalls (NGFWs) • Web application firewalls (WAFs) • Intrusion prevention systems (IPSs) • Endpoint protection platforms • Application control • Identity and access management	• Intrusion detection systems (IDSs) • Endpoint detection and response (EDR) • Security incident and event management (SIEM) • Security orchestration, automation, and response (SOAR)
Insights	• Exploit prevention • Web application attack prevention (injections, for example) • Malicious traffic filtering • Data exfiltration prevention • Malicious code execution prevention • Known attack prevention	• Events are correctly and consistently timestamped. • Logs and telemetry are captured and parsed. • Correlation rules are in place and result in alerts. • Proper response is initiated following alerts (in the case of SOAR).

The Future of BAS: Threat-Centric Defense and Security Control Mitigation

To truly improve an enterprise's security posture and resilience against actual attacks, reputable BAS platforms have already moved to threat-centric models. They also provide mitigation advice. These features will become increasingly more important, and BAS solutions will need to continuously improve to deliver such value for their customers. What follows is what the more advanced BAS providers offer.

Threat-Centric Defense

Having your security controls validated is one thing, but knowing which chain of failing controls could lead to a successful attack is another. With threat-centric defense, BAS platforms aim to provide:

- **End-to-end testing of attacks, with TTPs simulated across the Kill Chain—**Many BAS solutions start from an assumed breached model, but advanced solutions can also perform test cases aimed at gaining a foothold in the target organization (for example, by validating email gateway security controls, web application firewall defenses, and web proxy security). In addition, validation of an attack path toward your crown jewels helps to protect what is most important: the systems underpinning your business, which are also the objectives an adversary would be going after.
- **Validation of readiness against specific threats—**By emulating the TTPs used by relevant threat groups (think advanced persistent threats [APTs] or ransomware gangs), we can validate whether security controls are effective along an attack path that such a specific threat would take. To support this, the BAS platform should also be able to incorporate threat intelligence related to adversary behavior.

- **The capability to simulate the latest threats and attacks—**You want a BAS solution that not only knows the absolute number of real-world threats but also quickly incorporates emerging threats into its simulations. Implementing attack campaigns incorporating the latest identified vulnerabilities or TTPs by a relevant threat actor could allow an organization to tweak its security controls and thus defend against a future attack.
- **Custom adversarial content based on attack techniques and research by the platform provider's red team (assuming they have one)—**Many red teams perform their own research to come up with new ways of executing code, circumventing defenses such as EDR. A BAS platform backed by a skilled red team can provide interesting insights as opposed to more generic tests.

A threat-centric approach for security control validation clearly provides more useful insights than those provided by atomic testing of security controls.

Security Control Mitigation

Even with security control validation using a threat-centric approach, you're still not improving your security posture and defenses significantly. Once you know where the gaps are, the next step is to mitigate any lacking security controls. Someday a BAS platform will perform automatic mitigation, but in the meantime, the following are ways in which your BAS solution can help mitigate security control gaps:

- Providing **mitigation advice** based on executed test cases and lacking controls is a minimum requirement. Advanced BAS platforms take mitigations even further by providing vendor-specific insights, both in terms of prevention and detection. Armed with **vendor-agnostic and vendor-specific mitigation insights**, the blue team and organization administrators can start upping their game.
- To improve security controls used for detection, such as EDR and SIEM, detailed **detection analytics** provided by the BAS platform are essential. A basic use case is to identify whether the specific technique was detected. However, just knowing which technique was detected does not suffice to support improving detection capabilities. The blue team needs to develop detection rules for the missing alerts, which is impossible without ingestion of the required logs. A complete BAS platform should therefore also determine whether the necessary logs are collected. In case these logs are not already being ingested, guidance on which log source to use and which particular logs to collect will enable proper alert creation.
- Similar to the red team providing custom adversarial content, having the BAS platform's **blue team** examining the existing solution's inventory and technology integrations can help with **custom mitigation advice**. Each threat's TTPs can be validated for fine-tuning mitigations, identifying mitigation alternatives, and providing prevention signatures or detection rules.

- Finally, to avoid an overload of follow-up actions, **mitigations should be prioritized**. Even with a BAS solution in place, the SOC and operational teams still have their main job to do: Keep attackers out. With prioritized mitigations, security teams know where to begin and what to implement first to mitigate the riskiest gaps in their security controls.

With prioritized mitigations, security teams know where to begin and what to implement first to mitigate the riskiest gaps in their security controls.

When performing security control validation and mitigation using a threat-centric approach, you get a winning combination to increase your security posture. A streamlined architecture combining these elements looks like that presented in Figure 2.

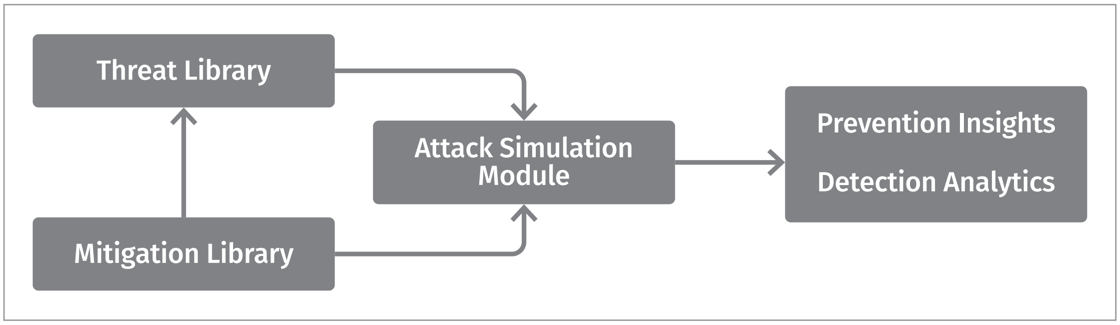

Figure 2. Streamlined Architecture of Threat-Centric Defense with Security Control Validation and Mitigation

Obviously, a strong interconnection exists between the threat library and mitigation library; for every threat and tested controls, relevant mitigations are needed. The threat emulation module executes selected campaigns and retrieves corresponding mitigations for lacking controls. This information is reported to return a prioritized overview of prevention insights and detection analytics aimed at improving both detection and response.

Conclusion

Even with millions invested in cybersecurity, companies still fall victim to malicious attackers due to failed security controls. Although manual validation using vulnerability assessments, penetration testing, and even red teaming can provide insight into weaknesses, it does not provide a complete picture of the full set of security controls that make up a company's defenses, nor is it the most cost-effective way to perform security control validation.

BAS platforms aim to provide a solution to this matter by providing automated, continuous, and repeatable validation of security controls for an increased return on investment and optimized security spending. They are not a deploy-and-forget solution, however. Before choosing a BAS solution, know your ecosystem and technologies to ensure that it integrates with your existing setup. Determine whether an on-premises or cloud deployment is most appropriate and test your configuration before starting security control validation, which is one of the more prominent use cases for BAS platforms.

Security control validation consists of making sure that every control in place is working as intended as well as testing and measuring their performance, both atomically and collectively, across prevention and detection layers. Advanced BAS platforms can perform threat-centric validation to determine readiness against realistic attacks and threats. In addition, they can provide in-depth mitigation advice, both vendor agnostic and vendor specific, to assist in prevention and detection improvement.

Sponsor

SANS would like to thank this paper's sponsor:

PICUS