DRUVSTAR®

Raising the Bar:

Cyber Attack Emulation: To Achieve Greater Resilience and Security

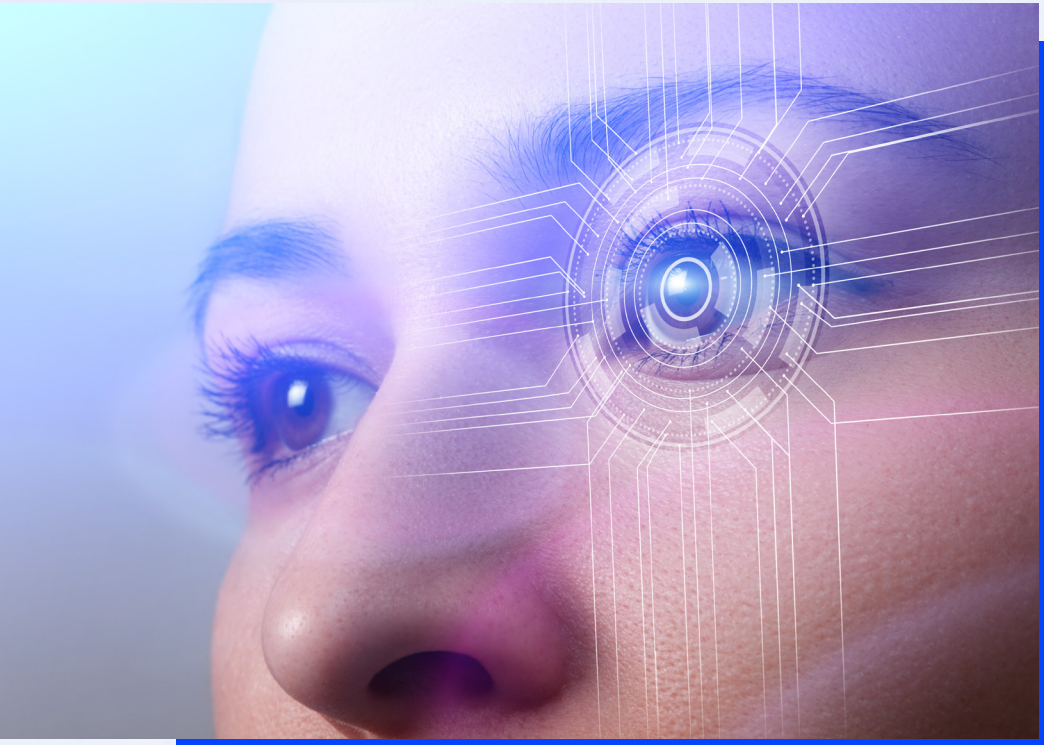


Table of contents

Introduction ---------- 1

Objective of Cyber Attack Emulation ---------- 2

It differs from traditional security testing methods ---------- 3

Implementing Cyber Attack Emulation ---------- 4

Emulation of Adversary Attack Pattern ---------- 5 - 6

Timelines ---------- 7

Outcome ---------- 8 - 9

Lessons Learned ---------- 9 - 10

DruvStar Solutions ---------- 11

Introduction

Cyber attacks are a major concern for organizations of all sizes due to the ever-growing dependence on technology and the internet. Average cost of data breach is $4.35 million globally and it takes on average 277 days to identify and contain a breach.

To be prepared for any potential cyber threats, businesses should use a human-implemented cyber attack emulation as a proactive measure. Taking an attacker's view of both known and unknown risks can help organizations adopt preventive measures before incidents happen.

The primary objective of such emulations are to assess the organization's ability to detect, respond to, and recover from a cyber attack. Through this, organizations can gain valuable insight into their security posture, allowing them to make the necessary improvements before an actual attack occurs.

Let's explore the benefits of cyber attack emulation and how it can help your organization achieve greater resilience and security

Being Proactive Pays Off

US$ 4.35 million
Average total cost of a data breach

277 days
To identify and contain a breach

Benefits over 3 years*

USD 2.6 million
Avoided compliance fines and penalties

USD 1.9 million
Avoided productivity losses

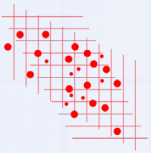
USD 1.4 million
Avoided reputational damages

*Forrester

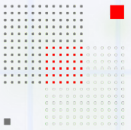
Objective of Cyber Attack Emulation

Testing the effectiveness of your security controls and incidence response

- Proactive and realistic way of testing security posture and effectiveness of incidence response
- Simulates real-life cyber attacks using the same tools and tactics as threat actors
- Identifies gaps and weaknesses in standard operating procedures, and security controls that were not found in security testing and audits
- Helps understand how attackers operate and exploit vulnerabilities
- Validates and optimizes security controls and policies
- Enhances understanding of attackers' tactics and vulnerabilities
- Prepares for real-life cyber attacks



Proactively simulates real-life cyber attacks



Learn weaknesses in security controls and incidence response

Improves preparedness for real-life cyber attacks

It differs from traditional security testing methods

Feature	Cyberattack Emulation	Security Testing
Scope	Entire network	Specific system or application
Frequency	Continuous and persistent	One-time or periodic
Feedback	Alerts in real-time, hopefully	Reports after the test
Methodology	Multiple attack vectors without scope restriction	Predefined scope and methodology
Framework	MITRE ATT&CK Framework	Varies depending on the Tester: OWASP, CIS, and other standards

Implementing Cyber Attack Emulation

How we at DruvStar Implemented a cyberattack emulation

Emulation of Adversary Attack Pattern

Delivery of Malware, Lateral Movement and Escalation of Privileges

Adversary attack patterns are the typical steps taken by malicious actors during a cyber attack. To emulate an adversary attack pattern, we used a threat-informed approach that selectively emulated behaviors with a higher likelihood of impact on the target. This approach ensured a more relevant assessment of the security defenses compared to random testing.

To emulate a realistic attack scenario, we conducted a security test that emulated typical attack patterns, such as delivering malware, gaining a foothold, and expanding access. We stopped before performing any impact techniques, such as data encryption or exfiltration, as the focus of this exercise was to assess defenses before the end is at hand.

1 Delivery of Malware

The delivery of malware refers to the process of getting a malicious software onto a target system. This is typically the first step in a cyber attack, as the attacker needs to get their malware onto the target system in order to start their attack. There are many ways that an attacker can deliver malware, including phishing, exploiting vulnerabilities, and using social engineering tactics.

For example, an attacker might send an email to an employee, disguised as an important message from a trusted source, with a malicious attachment or link. When the employee opens the attachment or clicks on the link, the malware is delivered to their system, allowing the attacker to start their attack.

2 Gain a Foothold

Once the attacker has gained access to a system, they may attempt to escalate their privileges, allowing them to perform actions on the system that they wouldn't normally be able to do. This can include installing additional software, modifying system settings, or even taking complete control of the system. They may also attempt to setup persistence, so that they can spread out their activity, or keep the access they already have if they lose access for whatever reason.

For example, an attacker might use a vulnerability in a web application to gain access to a system, then use that access to escalate their privileges and install a backdoor, giving them persistent access to the system.

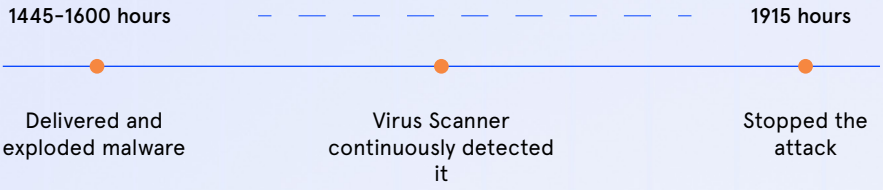
3 Expand Access

Once the attacker has delivered the malware and gained a foothold on the current system, they will typically attempt to move laterally across the target's systems, to gain access to sensitive information or systems. This is often done in preparation for a more serious attack, such as a data breach or ransomware attack. Expanding access can include several activities including discovery and credential access techniques, culminating with lateral movement. Lateral movement allows the attacker to gain access to more systems and to broaden their access to achieve greater impact against the target.

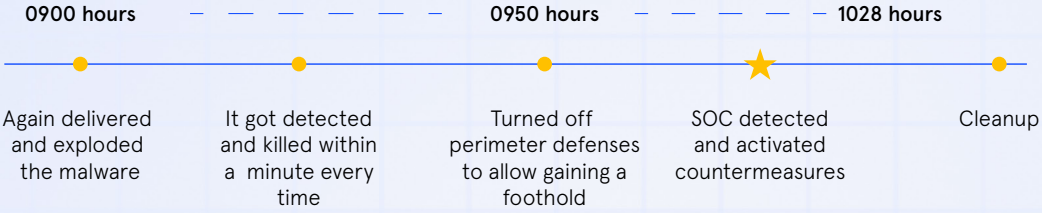
For example, a malicious actor may start by compromising a low-level employee's computer, then use the information they obtain from that system to move on to the company's servers. This can involve a range of tactics, including exploiting vulnerabilities, using stolen credentials, and leveraging social engineering techniques.

Timelines

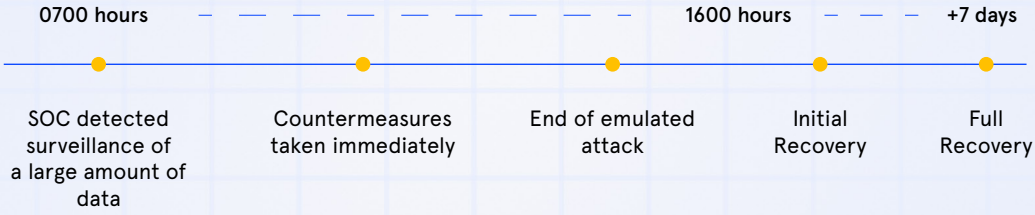
1 Day 1 - **First Attack**
Turned off the SIEM



2 Day 2 - **Second attack**
Turned on the SIEM



3 Day 3
Perceived attack



Outcome

The outcome of the cyber attack emulation performed by DruvStar was highly successful and provided valuable insights into the effectiveness of our cybersecurity solutions.

Throughout the 24-hour emulation, our detection technologies successfully identified and halted the attempts of the emulated adversary to deliver malware, establish a foothold, expand access, and achieve their desired outcomes. Our tools were able to detect the malicious activity in real-time, allowing our security operations center (SOC) analysts to swing into action and contain, escalate, contain, and block the ongoing activities. This highlights the importance of continuous monitoring and detection in responding to cyber threats and also the importance of having a well-trained and capable security team in place to respond to cyber threats.

One of the key highlights of the emulation was the involvement of an insider to deliver the payload. The activation of the payload required the cooperation of the insider, which showcased the importance of security awareness programs for all employees, including those with access to sensitive data. Our tooling caught the emulated bad actor activity in time, and our SOC analysts were able to contain the incident quickly, blocking the user account until a senior security engineer confirmed the cleanup.

The results of the emulation provided clear evidence of the efficacy of our security solutions and the robustness of our incident response process. The emulation helped validate our solutions and

showed that we have the right tools and processes in place to detect and respond to security incidents effectively. In conclusion, the cyber attack emulation was a valuable exercise that provided us with a wealth of information about our security posture. By emulating a real-life scenario, we were able to test the limits of our systems and validate our ability to respond to potential security threats.

24-hour emulation

DruvStar cybersecurity solutions detected malicious activity in real-time.

Enabled our SOC analysts to swing into action and contain, escalate, and block the ongoing activities.

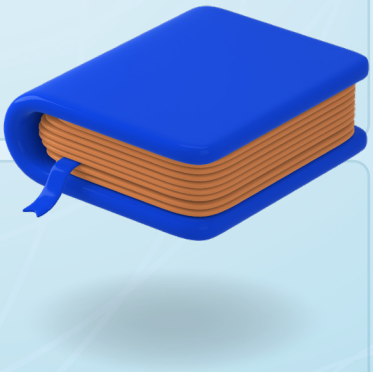
Lessons Learned

The Importance of Real-Time Detection and Response:

The emulation emphasized the need for real-time detection and response in the face of a cyber attack. Organizations need to have tools and technologies in place to be able to quickly detect and respond to a cyber attack. It further highlights the importance of having a dedicated and skilled SOC team in place.

Need for Continuous Threat Monitoring:

Continuous threat monitoring is essential to detecting and mitigating cyber attacks in real-time. The emulation showed that real-time monitoring is crucial in detecting, responding to, and blocking malicious activities before they can cause damage.



The Need for Regular Testing and Fine-Tuning:

The emulation highlighted the importance of regularly testing an organization's cybersecurity measures. By emulating real-world cyber threats, organizations can identify weaknesses and vulnerabilities in their systems that they may have otherwise missed. Regular testing helps to stay ahead of potential cyber threats and maintain a proactive approach to cybersecurity.

The Role of Insider Threats:

The emulation involved the use of an insider to deliver the payload, highlighting the importance of protecting against internal threats, whether witting or accidental, as well as external ones. This serves as a reminder for organizations to implement security measures that account for both internal and external threats.

The Value of Collaboration:

The emulation demonstrated the importance of collaboration between different departments within an organization, as well as between organizations. In the face of a real attack, quick and effective collaboration can be the key to successful containment and resolution.

Importance of Security Awareness Training:

The emulation highlighted the crucial role that security awareness training plays in detecting and preventing cyber attacks. Employees should be trained regularly to identify and report suspicious activity, including phishing emails and unauthorized access attempts.

The Importance of Continual Improvement:

Such emulations can help identify areas for improvement in your organization's security solutions and incident response protocols.They emphasize the importance of regularly assessing and refining your security posture to stay ahead of changing cyber threats.

DruvStar Solutions

We help **small to medium** size businesses in discovery of their vulnerabilities and help protect them with comprehensive SaaS based cyber-defense technologies

DRUVSTAR THREAT INSIGHTS™

- ✓ Managed Detection and Threat Hunting
- ✓ Security Incident & Event Management
- ✓ Incidence Response

DRUVSTAR DATAVISION™

- ✓ Comprehensive data visibility
- ✓ Automated policy implementation
- ✓ Access governance and compliance tools

DRUVSTAR® SECURITY ASSESSMENTS

- ✓ SecurityPenetration Testing
- ✓ DruvStar SWAT Analysis

AI Powered

Standards Based

CIS Center for Internet Security®

MITRE | ATT&CK®

NIST