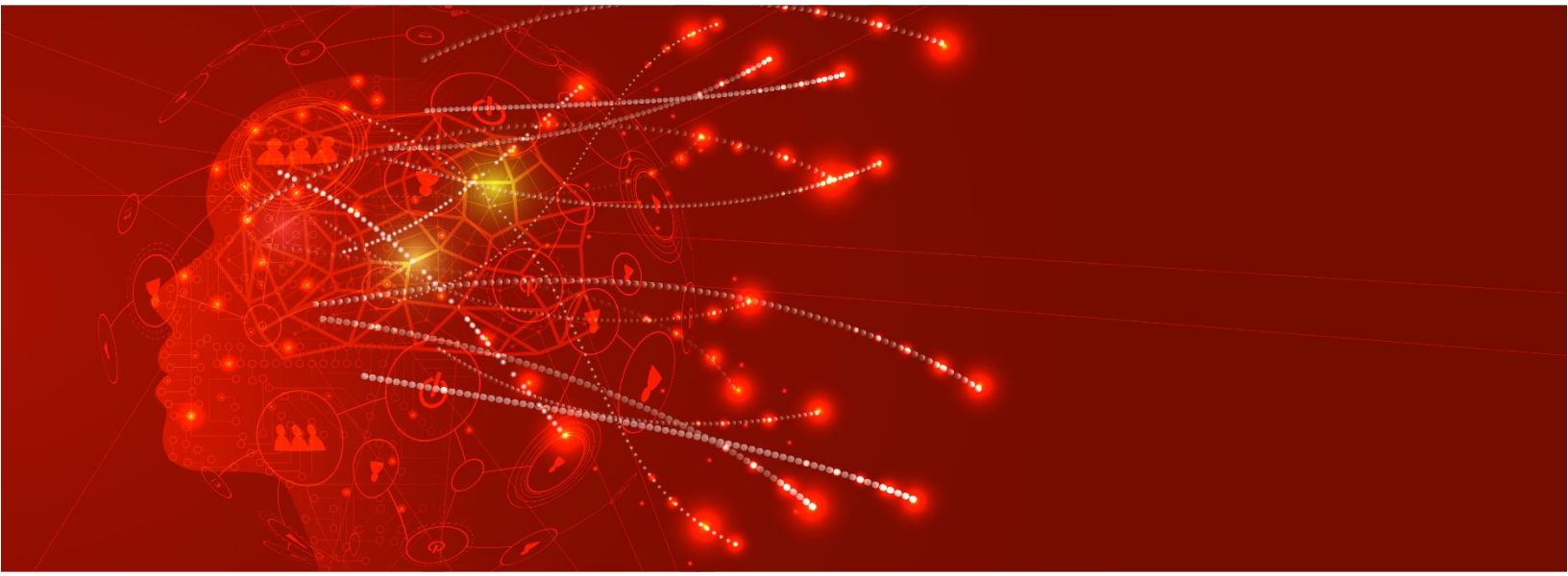
Whitepaper

CyberStack Continuous Automatic Red Teaming



Red Team Security Validation Challenges

Traditional penetration testing and red team exercises are limited engagements that may take place just once a quarter or even just once a year. While this may meet organizations' compliance requirements it does not effectively validate security due to the rapid development and proliferation of threats. The time between engagements is a gap in an organization's security validation and these quarterly or yearly exercises can permit a significant number of risks to your environment.

IT environments have become incredibly complex, with IoT devices, cloud environments and remote work infrastructure all leading to an increase in the number of alerts generated. The sheer number of alerts can fatigue and slow down security teams responding to security validation exercises. This requires teams to effectively prioritize alerts based on their risk.

Yet another challenge of traditional security validation is the impact on production systems. Thorough security validation might strain an organization's infrastructure such that it interferes with business operations. It is imperative to reduce the risk to business operations when choosing tools and methods to validate your security.

Finally, pentesting and red teaming require expertise that many teams may lack. This may require organizations to work with consultants and external organizations with the required knowledge and experience to step in. Organizations may not have the time, resources or personnel to dedicate to training their staff to be effective in these roles.

Continuous Automated Red Teaming

Continuous Automatic Red Teaming (CART) addresses several limitations and challenges of traditional red teaming and pentesting exercises. It automates key red teaming functions and greatly reduces the time between engagements to give your organization up to date security validation.

Automation: Previously manual tasks are automated so that teams can focus on more complicated red teaming tasks. Automation also ensures that the tasks can be carried out consistently.

Attack Surface Visibility: Attack surface management helps you gain visibility over known and unknown vulnerabilities. Your organization receives a full view over its assets including shadow IT. External attack surface management ensures that potential attack vectors accessible via the internet are identified and remediated or flagged for your team to take action.

Iterative Improvement: The continuous approach ensures that your team will be able to remediate vulnerabilities and then test the measures put in place.

Simulated Attacks: Test your security posture against actual tactics, techniques and procedures (TTPs) that are used by threat actors. Understand the strengths and weaknesses in your organization's ability to prevent, detect, respond to and recover from attacks.

CyberStack CART

Effectively validate your security posture with the latest in red teaming with CyberStack Continuous Automatic Red Teaming (CART). CyberStack CART combines red team tools and methods such as external attack surface management, penetration testing and attack simulation to provide you with all the benefits of red team exercises in an automated platform. Our CART platform agentlessly discovers assets like IP addresses, domains and databases. It continuously monitors your environment and executes automated simulated attacks to test your security controls and overall incident response capabilities.

Where traditional pen testing engagements are point in time engagements that only capture a small portion of your overall exposed assets, CyberStack CART runs continuously and identifies non-critical assets that could allow attackers to breach your defenses. These non-critical assets are often not secured as well as mission critical assets but historically have been involved in major breaches. Moreover, the dynamic nature of modern IT environments means that point in time pen tests or red team exercises can miss important changes to your environment as well as new threats.

Featured Highlights

- **External Attack Surface Management:** CyberStack CART identifies assets that are missed by traditional attack surface management by targeting non-critical assets as well. The EASM function reduces the number of false positives and captures the changes occurring to your environment as well as the evolving threat landscape.
- **Attack Simulation:** Evaluate your security posture by executing realistic attacks against your organization. These attacks will allow you to understand the strengths and weaknesses of your defenses and implement improvements to your controls and processes accordingly.
- **Vulnerability Assessment:** Proactively identifies vulnerabilities in your environment and provides risk-based prioritization to ensure your team remediates the most critical gaps first.
- **Remediation Actions:** CyberStack CART will improve your mean time to respond by automatically blocking malicious activities, reconfiguring security settings and patching detected vulnerabilities.
- **Automated Playbooks:** Playbooks provide consistent workflows that automate red team functions such as identifying assets, executing simulated attacks and remediating gaps in your security.

Why CyberStack CART?

Traditional penetration testing and red teaming are on demand exercises that can leave your organization vulnerable to attack in the months or years between engagements. CyberStack CART ensures that your organization is constantly aware of both known and unknown vulnerabilities, TTPs in addition to providing prioritized risk assessments so your team can focus on remediating critical gaps in your security posture on a continuous basis.

Attack Surface Visibility

Gain continuous visibility on your external attack surface through continuous external attack surface management (EASM) to discover unmanaged applications, unused databases, open ports and more.

Increase Efficiency

Reduce the number of false positives with attack surface validation and leverage automated red teaming to point your team towards critical security concerns.

Targeted Threat Hunting

Execute regularly updated playbooks to target specific TTPs such as ransomware and 24-hour CVEs.

SOC Integration

iG2 CART can ingest data from your SIEM to provide more context and improve the quality of your alerts.

Experts on Demand

If your team is stuck on how to move forward, consult with our experts to provide guidance on external attack surface management, executing attacks, responding to alerts or more.

CyberStack CART Process

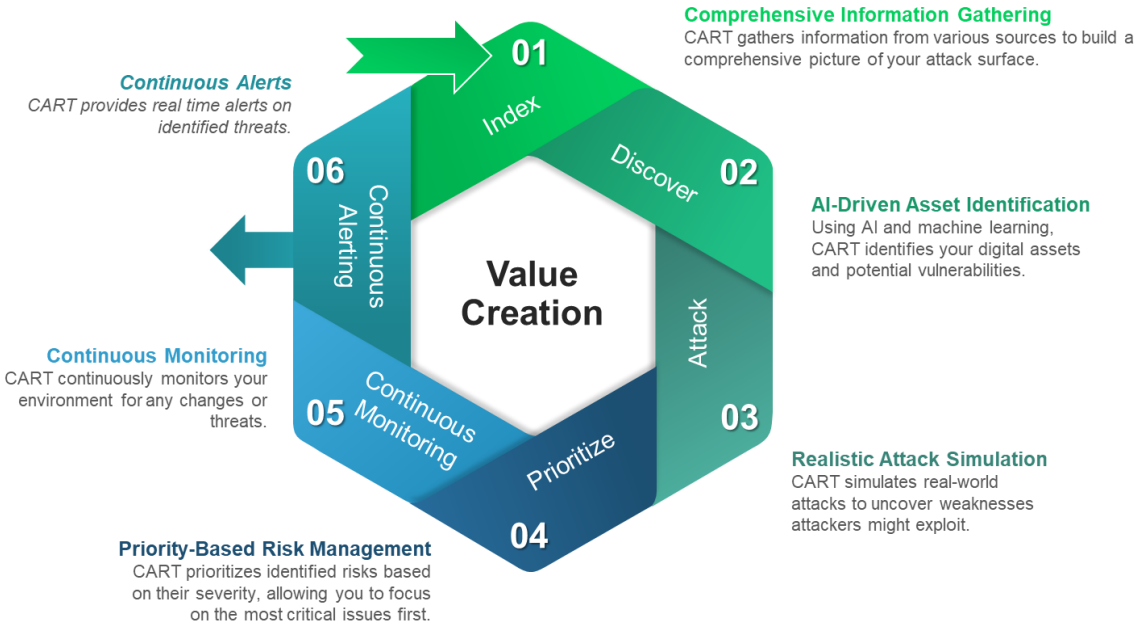


Figure 1: CART Process

Comprehensive Information Gathering: CyberStack CART starts by gathering data from billions of IP addresses worldwide in combination with intel from Threat intel, Honeypot and others to ensure it can capture all elements of your attack surface.

AI-Driven Asset Identification: The solution identifies your assets using AI and machine learning. This helps to identify attack vectors such as unmanaged applications, open ports, sub-domains and more.

Realistic Attack Simulation: After viable attack vectors are identified, CyberStack CART launches simulated attacks on your environment based on actual TTPs used by malicious actors.

Priority-Based Risk Management: Alerts are prioritized based on the risks to your environment so your team can focus their efforts on delivering the most impact.

Continuous Monitoring: Our solution tracks changes to your environment to help identify potential threats.

Continuous Alerts: CyberStack alerts based on identified threats and vulnerabilities so your team can remain up to date.