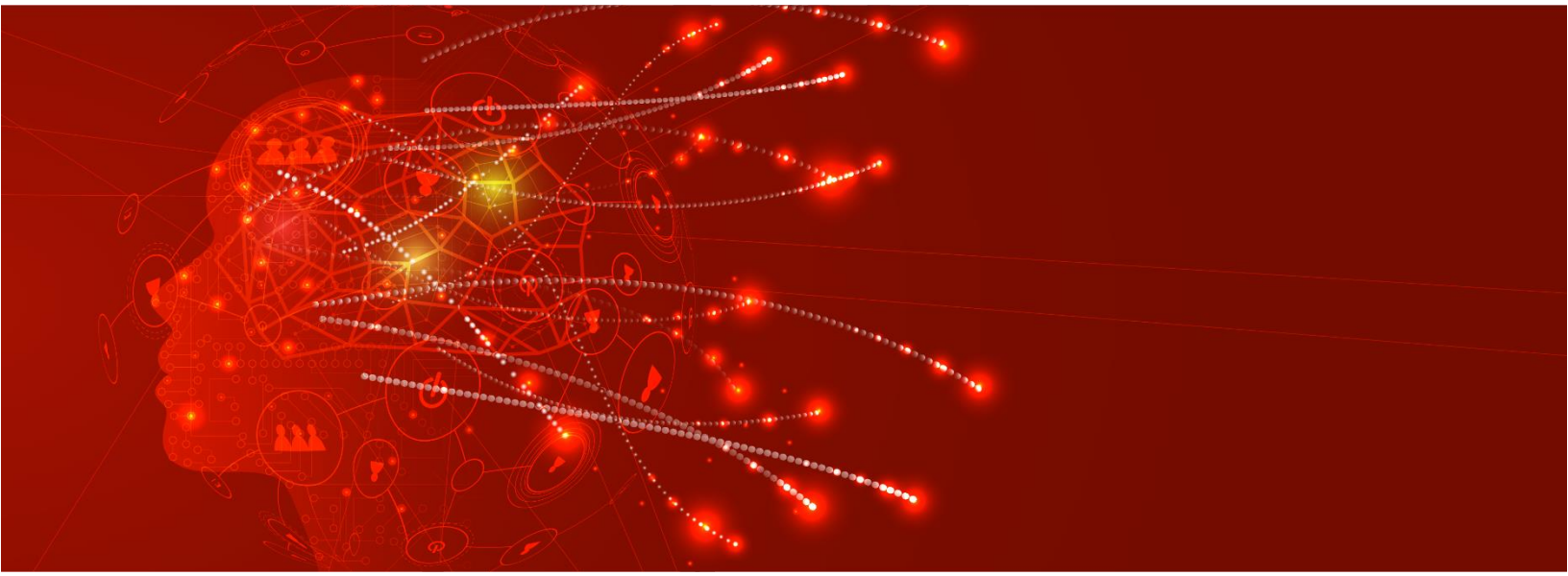
Datasheet

CyberStack Continuous Automatic Red Teaming



CyberStack Continuous Automatic Red Teaming

CyberStack Continuous Automatic Red Teaming (CyberStack CART) is the next evolution of traditional red teaming. CyberStack CART automates red team functions to provide continuous red teaming that provides visibility of your attack surface, emulates actual adversarial Tactics, Techniques and Procedures (TTPs) as well as offering risk assessments so your team can continuously improve your security posture. CyberStack's team of security experts manage the service so that your team can continuously focus on the most critical gaps in your security posture.

Why 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

CyberStack 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.

Continuous Automatic Red Teaming Features

External Attack Surface Management: CyberStack CART continuously monitors your environment for attack vectors and discovers assets such as domains, sub-domains, IP addresses, applications and more.

Automated Attack Simulation: CyberStack CART continuously simulates various attack scenarios including vulnerability scanning, penetration testing, and exploitation attempts all using automated tools and techniques.

Vulnerability Assessment: conducts regular vulnerability scans to identify weaknesses, misconfigurations, known and unknown vulnerabilities across the organization's infrastructure. These are prioritized based on severity.

Real-Time Alerts and Notifications: The solution generates automated alerts for detected security incidents, anomalies, or suspicious activities, providing timely visibility into potential threats.

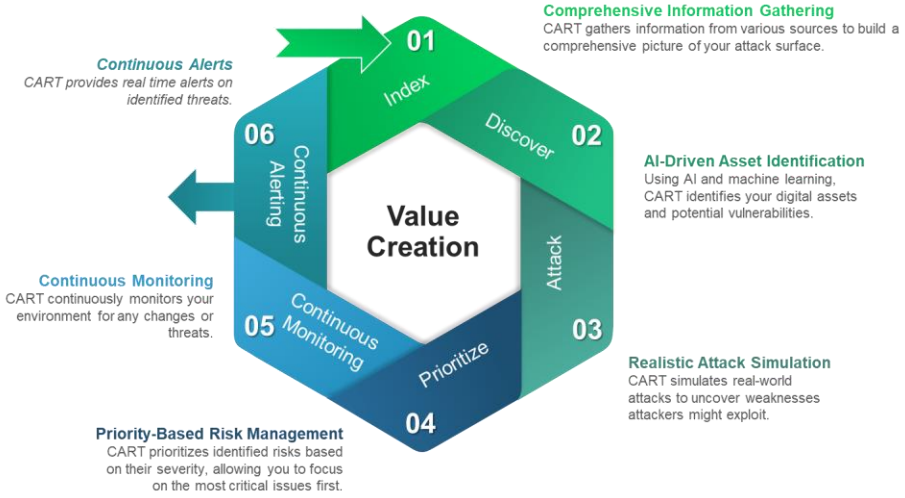
Automated Remediation: It can implement remediation actions such as applying patches, reconfiguring security controls or blocking malicious activities automatically.

Playbooks: CyberStack CART integrates with incident response tools to automatically trigger response actions based on regularly updated playbooks and workflows to reduce response time and minimize impact.

Reporting and Analytics: It provides detailed reports on findings, including identified vulnerabilities, successful attack paths, and recommended remediation actions, enabling informed decision-making and continuous improvement.

Integrations: CyberStack CART can integrate with Security Information and Event Management (SIEM) systems and other security tools to centralizes monitoring, correlation, and response across the organization's security operations.

CART Process



iG2 CART is designed to provide organizations with a continuous, comprehensive overview of their security posture.

Comprehensive Information Gathering: iG2 CART starts by gathering data about your environment to ensure it can capture all elements of your attack surface.

AI-Driven Asset Identification: Using the collected data, iG2 CART 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, iG2 CART launches simulated attacks on your environment based on actual TTPs used by malicious actors.

Priority-Based Risk Management: iG2 CART provides risk assessment and prioritization so your organization understands their security posture and how to improve it.

Continuous Monitoring: iG2 CART tracks changes to your environment. This helps to identify potential threats.

Continuous Alerts: iG2 alerts based on identified threats and vulnerabilities so your team can remain up to date.

Benefits of CART:

Cost-Effective Security Assessment: CART offers a cost-effective approach to continuously assess and improve cybersecurity posture by automating red teaming activities, reducing manual effort, and optimizing resource utilization.

Proactive Security Practices: It enables organizations to adopt proactive security practices by integrating automated red teaming into their security strategy, helping identify and address vulnerabilities before they are exploited by adversaries.

Accessibility of Red Teaming: It makes red teaming more accessible to organizations of varying sizes and industries, allowing them to conduct advanced security assessments and simulations without requiring extensive resources or specialized expertise.

Real-Time Visibility: By providing real-time insights into the organization's defense performance, CART enhances situational awareness and facilitates prompt response to emerging threats and security incidents.