
Security for
Everyone
TOP 10 IMPORTANT
THINGS ABOUT
CONTINUOUS
AUTOMATED RED
TEAMING

Security for Everyone

CONTENTS

3	What is Continuous Automated Red Teaming?
4	How Continuous Red Teaming Works
5	Top 10 Important Things About Continuous Automated Red Teaming
8	Sources

WHAT IS CONTINUOUS AUTOMATED RED TEAMING?

Continuous Automated Red Teaming (CART) is a proactive security testing approach that continuously simulates real-world attacks against an organization's systems and networks. It aims to identify and remediate vulnerabilities before malicious actors can exploit them. CART differs from traditional red teaming in several significant ways.

Firstly, CART is ongoing and runs continuously, as opposed to traditional red teaming, which is typically conducted periodically or as a one-time engagement.

Secondly, CART is automated, relying on software to simulate attacks and analyze the outcomes. This automation adds scalability and cost-effectiveness to CART, setting it apart from traditional red teaming.

Moreover, CART relies on the latest threat intelligence to ensure it is testing against the most up-to-date attack vectors, helping organizations stay ahead of emerging threats.

HOW CONTINUOUS RED TEAMING WORKS?

CART typically follows a four-step process:

Discovery:

The CART team employs various tools and techniques to identify all of the organization's assets, including networks, systems, applications, and data.

Assessment:

The CART team assesses the security of the organization's assets by emulating attacks and analyzing the results.

Prioritization:

Vulnerabilities are prioritized based on severity and the likelihood of exploitation.

Remediation:

The CART team collaborates with the organization to address the identified vulnerabilities.

CART can be implemented using various approaches, with a common method involving the use of a cloud-based platform. This allows organizations to adapt their CART program as needed, accessing the most current threat intelligence.

TOP 10 IMPORTANT THINGS ABOUT CONTINUOUS AUTOMATED RED TEAMING

1 PROACTIVE VULNERABILITY IDENTIFICATION

Continuous Automated Red Teaming (CART) takes a proactive approach to security, with a primary focus on **identifying and rectifying vulnerabilities before they become the target of malicious actors.** By perpetually evaluating an organization's security infrastructure, it maintains a state of preparedness that significantly reduces the likelihood of data breaches, financial losses, and reputational damage.

2 CONTINUOUS MONITORING

In stark contrast to periodic security assessments, CART operates **tirelessly, 24/7, throughout the year.** This perpetual vigilance ensures organizations remain shielded against the most contemporary threats. It affords the capability for immediate responses to emerging risks, thus diminishing the window of opportunity for cybercriminals to capitalize on vulnerabilities.

3 AUTOMATION FOR SCALABILITY

Automation is a cornerstone of CART's functionality, offering the **ability to simulate a diverse range of attacks and vulnerabilities.** This automation enhances scalability and cost-effectiveness when compared to traditional manual red teaming. CART adeptly manages substantial workloads without necessitating an extensive human resource allocation.

4 INTEGRATION OF THREAT INTELLIGENCE

CART is deeply rooted in the utilization of the latest threat intelligence. This practice ensures that organizations **test their defenses against the most current attack vectors, accurately reflecting the ever-evolving threat landscape.** CART remains in sync with the dynamic tactics, techniques, and procedures employed by cybercriminals.

5

TAILORED TO ORGANIZATION'S NEEDS

CART can be **customized to harmonize with the distinctive needs and objectives of each organization.** This flexibility encompasses the specification of attack types to simulate, testing frequency, and the format of reporting. Customization ensures that security assessments seamlessly align with an organization's specific security strategies.

6

INTEGRATION WITH SECURITY ECOSYSTEM

CART seamlessly integrates with an organization's existing security tools and processes. This integration elevates the **overall effectiveness of security operations by streamlining the detection, response, and remediation of security incidents.** The outcome is a cohesive and well-coordinated security ecosystem.

7

IMPROVED INCIDENT RESPONSE

Regular CART testing greatly contributes to enhancing an organization's incident response capabilities. Through continuous practice of response plans and procedures, organizations are better equipped to effectively manage real-world security incidents. This state of preparedness effectively **minimizes response times and mitigates the impact of security breaches.**

8

ENHANCED COMPLIANCE

Many industry regulations and standards mandate that organizations demonstrate ongoing security testing efforts. CART serves as the means to satisfy these compliance requirements by providing a continuous stream of evidence from security assessments. This level of compliance **ensures a seamless adherence to regulatory obligations.**

9

REDUCED INSURANCE PREMIUMS

Implementation of CART programs can result in reduced insurance premiums for organizations. Insurance providers frequently offer discounts to organizations that exemplify a proactive stance toward security. By substantially reducing the likelihood of costly data breaches and related financial losses, CART **yields significant savings in insurance costs.**

10

COMPETITIVE ADVANTAGE

CART equips organizations with a potent competitive advantage. By demonstrating a steadfast commitment to security, organizations establish trust with customers and partners who prioritize secure business relationships. This trust translates into a competitive edge within the market, **attracting and retaining key stakeholders while fostering enduring business success.** Furthermore, a robust security posture differentiates an organization from its competitors, enhancing its overall reputation and appeal.

SOURCES

- FireCompass. (2021). " Continuous Automated Red Teaming" Retrieved form https://www.firecompass.com/continuous-automated-red-teaming/

- IBM. (2023). "How continuous automated red teaming (CART) can help improve yourcybersecurityposture" Retrieved from
- https://www.ibm.com/blog/how-continuous-automated-red-teaming-cart-can-help-improve-your-cybersecurity-posture/

- LinkedIn (2023). "The Importance of Continuous Red Teaming in Cybersecurity" Retrieved from https://www.linkedin.com/pulse/importance-continuous-red-teaming-cybersecurity/

- Invgate (2022). "Continuous Automated Red Teaming: Security Testing for Threat Landscape" Retrieved from
- https://blog.invgate.com/continuous-automated-red-teaming

- Synopsys (2023). "Red Teaming" Retrieved from https://www.synopsys.com/glossary/what-is-red-teaming.html