eventus

eventussecurity.com

RED TEAM ASSESSMENT

Identify your cyber resiliency from real world threat agents & actors

SERVICE OVERVIEW

Red Team Assessment aims to simulate a potential adversary and use their expertise to challenge and test an organization's security measures.

The red team closely mimics a real attacker's active and stealthy attack methods by using TTPs seen on real, recent incident response engagements. This helps assess your security team's ability to detect and respond to an active attacker scenario.

Eventus Red Team Assessment combines both external attack surface and internal attack surface to correlate and showcase complete kill chain of an attack. We also perform Breach & Attack Simulation to perform targeted Advanced Persistent Attacks on the enterprise.

The whole engagement is mapped around the MITRE ATT&CK framework for providing detailed overview.

OUR METHODOLOGY

At Eventus, we combine best of the methodologies, into Hybrid Approach to showcase return on investment to the organization. We fuse the approaches of Black Box, Assumed Breach, and Goal Based into Time Boxed Hybrid Approach.

Below are some sample goals / missions that is taken into consideration during red team assessment.

SAMPLE GOALS/MISSION

- Compromise Critical Users
- Compromise Critical Assets
- Bypass EDR / EPP Solution
- Perform Data Exfiltration
- Compromise Domain Controller

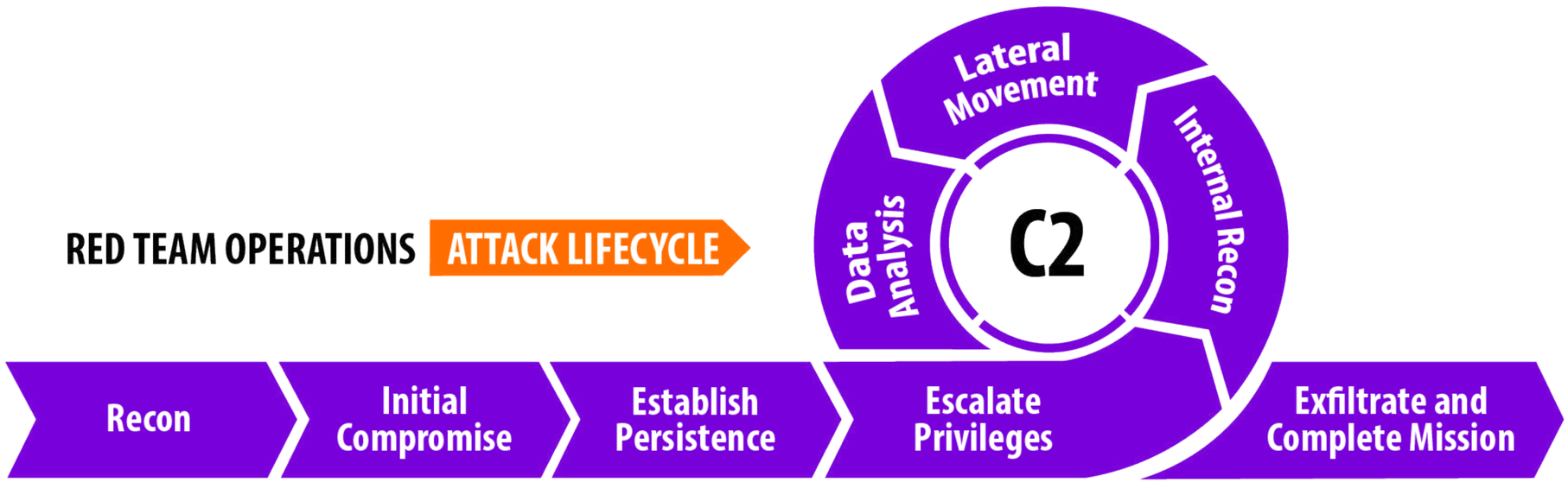
Quoted from Gartner Research:

Penetration testing helps to answer the question *'can they get in?'*

Red Teaming exercise answers the question *'does my security work?'*

WHO SHOULD CONSIDER RED TEAMING

- To know the cyber resiliency posture of the enterprise.
- Security Assessment using Real World Threat Actors.
- Specific Threat Profiles for your enterprise. which can be leveraged by Blue Team for Response Management.
- Identification of the gaps using controlled and simulated attacks.
- Identification of Threats & Vulnerabilities before it is exploited by an attacker.
- Have incident detection and response solution implemented and want to test them.
- Want to simulate multiple attack / incident / campaign scenarios based on latest knowledge of adversary tactics, techniques, and procedures (TTPs)



Red Team Assessment at Eventus utilizes the power of open-source intelligence as well as proprietary threat intelligence to correlate and produce set of result which serve as input to the next phase which is initial compromise.

To obtain initial compromise, social engineering techniques like phishing, vishing is used on the extracted information from surface web and dark web. Eventus also performs external attack surface analysis and exploitation of the public facing assets to get access to digital infrastructure.

Once access is gained, the red team attempts to escalate privileges to establish and maintain persistence within the environment by deploying a command and control infrastructure, just like an attacker would.

After persistence and command and control systems are established within the environment, the red team attempts to achieve the defined goals and mission.

WHAT TO EXPECT IN FINAL REPORT

- Executive Summary outlines the Engagement scope, project timelines, out-of-scope, quick view of overall findings mapped with business impact

- Technical Report - Technical Details on findings, step-by-step guide to simulate the exploitation, attack timeline, mitigation steps, MITRE framework mapping.

- Security Control Validation – Gaps identified in security controls, feeds to SOC / SIEM / MDR team to finetune the security monitoring solution.

RED TEAM ASSESSMENT ENGAGEMENT MODEL

Eventus offers different engagement models within Time-Based Hybrid Approach to let the client decide what floats their boat when they avail themselves of the red team assessment service. They can choose from

WEEKS	COVERAGE
4	External Attack Surface Analysis and Exploitation
5	External Attack Surface Analysis and Exploitation + Social Engineering
9	External Attack Surface Analysis and Exploitation + Social Engineering + Internal Attack Surface Analysis & Exploitation
10	External Attack Surface Analysis and Exploitation + Social Engineering + Internal Attack Surface Analysis & Exploitation + Ransomware Simulation

Contact us at

sales@eventussecurity.com

www.eventussecurity.com