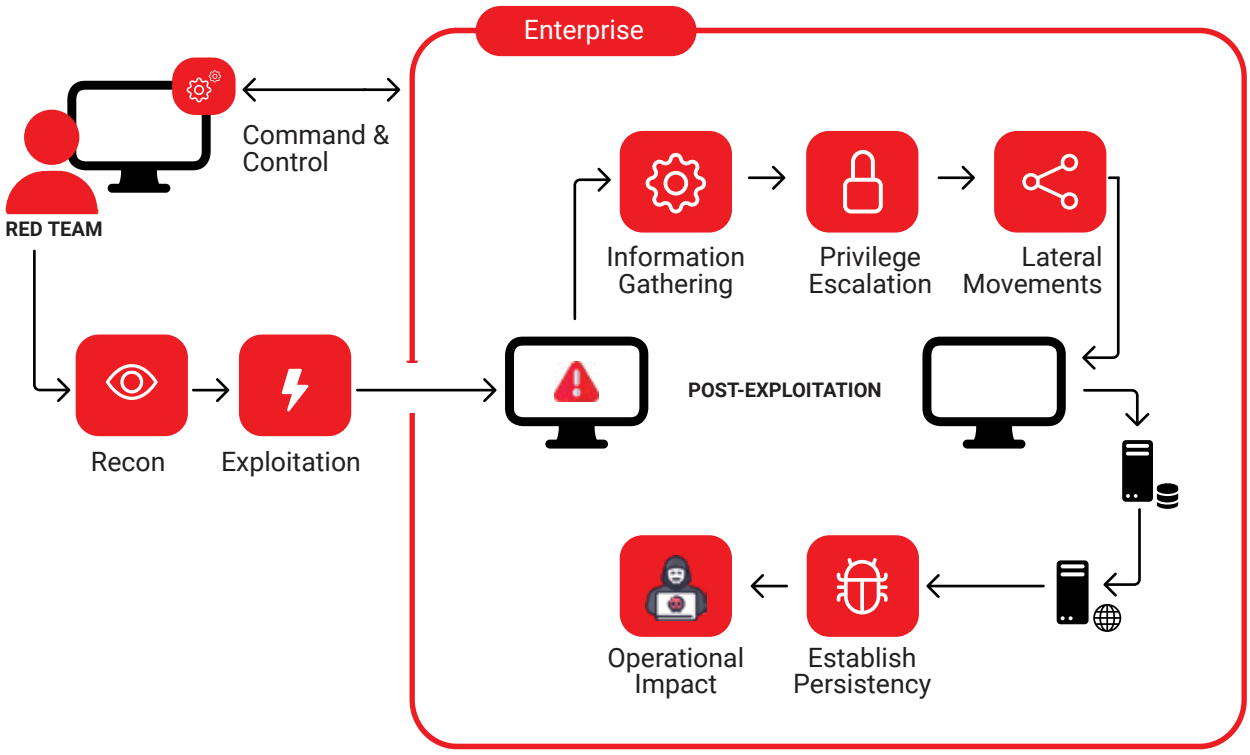
Datasheet

RED & PURPLE TEAM ACTIVITIES

ActiveBytes red team assessment is a goal-based adversarial activity that is based on a big-picture, holistic view of the organization from the perspective of an attacker. This assessment process is designed to meet the needs of complex organizations with critical assets through technical, physical, or process-based means.

Through expert red teaming assessment, you can understand how real-world attackers can combine seemingly unrelated exploits to cause damage to your assets or steal data. It is an effective way to show that even the most sophisticated firewall in the world means very little if an attacker can walk out of the data center with an unencrypted hard drive. Rather than choosing a single network appliance to secure enterprise sensitive data, it's better to take a defense in depth approach and continuously improve your people, process, and technology.

Red teaming uncovers risks in your organization that traditional penetration tests missed due to their narrow scope. Our red team assessors go beyond the test with many tactics



Our red teaming service phases

- Creating a threat profile for the target organization and passively and actively obtaining information about the organization

Passive reconnaissance (including OSINT and Dark Web Search) and Active reconnaissance

- Scheduling attacks to achieve set goals (such as accessing specific data, controlling infrastructure, compromising a specific user, running code on an organization's devices, and so on) and defined constraints. Initial attack vectors usually include:

Attacks on the user (social engineering)

Attacks on user devices

Perimeter attacks on the organization etc.

- Execution and documentation of attacks. This step usually includes

Escalation of privileges on the machines and information systems and other post-exploitation activities
Distribution of tools and modified malicious code within the scope of specified targets etc

- Creating a report from the red teaming engagement, which includes

List of successful attack vectors

Identified vulnerabilities in the target organization

Timeline of activities performed etc.

Key features of our Red & Purple team

- Offensive & defensive security experts
- Intelligence led testing
- Multi dimensioned attack tactics
- Detailed executive & technical reporting

Benefits of our red team service

- Simulation helps security teams learn real skills to handle threats or attacks
- Assessment of enterprise security posture
- Member of staff learns their role in incident response
- Improve security SOP in handling vulnerabilities & threats
- Measure & enhance people, process & technology
- Cost-efficient and address the critical needs first

Key features of our Red & Purple team

Here, our red and blue team work together to maximize cyber capabilities through continuous test feedback and knowledge transfer. Purple teaming can help security teams to improve the effectiveness of vulnerability detection, threat hunting and network monitoring by accurately simulating common threat scenarios and facilitating the creation of new techniques designed to prevent and detect new types of threats.

In purple team engagement, ActiveBytes focuses on people, processes and technology.

Based on this approach, we

- Establish the necessary processes, guidelines, and procedures for purple teaming
- Train the internal security team
- Design and implement the necessary technologies
- Identify relevant resources and implement analytics based on this methodology

Our purple team service helps to

- Identify gaps in cyber security defense mechanisms implemented
- Enhance security knowledge of the team
- Gain critical insight

RED TEAM

→ Vulnerability Assessments
→ Penetration Tests
→ Social Engineering

PURPLE TEAM

Improve organization security posture

Benefits of our purple team service

- Knowledge sharing to improve enterprise security posture
- Feedback mechanism to enhance detection & prevention controls
- Effective layered security approach

Contact us

contact@active-bytes.com +971 50 513 3973

www.active-bytes.com