

THE RED REPORT 2023

Key Recommendations

to improve your defense against the Top 10
ATT&CK techniques used by adversaries



Leverage Behavioral Detection

To identify attacks that may have been missed by traditional security measures, security teams should prioritize behavioral detection of abnormal activity rather than solely relying on the blocking of known IOCs.



Regularly Test and Optimize Security Controls

As attackers constantly develop new attacks and evasion techniques, regular testing and tuning security controls are crucial for detecting and preventing the latest attack techniques.



Uncover Attack Paths

Security teams should reveal the attack paths to identify vulnerable assets and data at risk that might lead to a breach of systems and prioritize the most critical security gaps for mitigation.



Operationalize MITRE ATT&CK

Adversaries use diverse tactics, techniques, and procedures (TTPs) to carry out cyberattacks. Operationalizing MITRE ATT&CK can help organizations identify, detect, and prevent cyberattacks.

Want to learn more about the ATT&CK techniques and emerging threats
that dominate the cybersecurity landscape?

[READ FULL REPORT](#)