Acalvio ShadowPlex for Red Team Exercises

How security teams can leverage cyber deception and Acalvio ShadowPlex to ensure successful red team exercises

Overview of Red Team Exercises

Red team exercises are an approach to simulate adversarial actions to enable organizations to assess their readiness in the event of a cyberattack. Organizations conduct periodic red team exercises to gain an understanding of the security posture and identify any areas of improvement in the posture.

Teams involved and types of red team exercises

The teams involved in a red team exercise are typically:

Red team: team that simulates adversarial actions is called the red team. The red team typically compromises of skilled researches with knowledge in offensive security and adversarial activity.

Blue team: the blue team represents the internal security team that is responsible for the defense, setting strategies, and selecting security controls.

The specifics of a red team exercise can vary based on the goals and objectives but the general aim is to measure the effectiveness of the security controls of an organization.

Mission or objectives of a red team exercise

The mission or objectives of a red team exercise are typically set to provide a goal for the red teamer to compromise a critical asset or to exfiltrate sensitive data. These are indicative of the goals that a real adversary would have in the environment.

Examples of the goals of a red team exercise would include:

- Gain access to the credentials of a domain administrator account in Active Directory
- Gain administrative control over an important application, such as an ERP/CRM system
- Exfiltrate data from an important data repository, such as a database server or an important network share

What is a failed red team assessment

In a red team exercise, the goal of the red team is to complete their mission without getting stopped by the blue team. The goal of the blue team is to monitor the alerts raised by the security controls and block/isolate the red team. This is mechanism of assessing the preparation of the organization to detect and respond to a cyberattack.

A failed red team assessment occurs when the red team completes the mission or objectives with the blue team unable to detect and respond in time. This can occur due to a combination of reasons: no alerts raised by the security controls, too many low fidelity alerts being raised, resulting in blue teams unable to process the alerts in time, or the alerts being raised with very high delays, resulting in the red team completing their mission prior to the alerts being processed by the blue team.

Why do organizations fail a red team assessment

Despite having multiple security controls, organizations routinely fail a red team assessment. Red teams exploit detection gaps in traditional security solutions by using stealthy offensive techniques such as living off the land (LotL) exploits, use of cached credentials for lateral movement, targeting unmanaged endpoints due to lack of EDR tooling, use custom and polymorphic malware variants that generate new disabling agent-based security solutions, clearing log evidence as measures to evade traditional security solutions.

Alerts, when raised, are often slow due to the challenges with identifying malicious activity through baselining and anomaly-based detection approaches. Red teams leverage the slow alert processing to rapidly move in the environment, completing their mission prior to the blue team getting visibility to alerts.

A failed red team assessment is indicative of lack of sufficient strength in the security tooling, with the gaps in the detection demonstrating an opportunity for a real adversary to exploit these gaps and result in a breach.

Actions after a failed red team assessment

Security teams are assigned the task of strengthening the security posture as a countermeasure for a failed red team assessment. These countermeasures include:

- Hardening the security configurations and settings of existing security controls, to reduce the attack surface
- Deploying deception technology as a defense layer to detect threats that bypass traditional security solutions

How cyber deception improves visibility

Cyber deception is based on predicting the goals of the adversary (red teamer), setting relevant traps for the adversary, and observing for interactions with the traps. Deceptions are not used in existing workflows, any interaction with the deceptions is an immediate indicator of malicious (red team) activity. Deceptions are agnostic to attacker TTPs, providing visibility to evolving threats that leverage novel attack TTPs that bypass traditional security solutions.

Acalvio ShadowPlex: Robust platform for Active Defense and cyber deception

Acalvio ShadowPlex is a robust and proven Active Defense platform that combines cyber deception and AI to provide proactive defense for organizations. ShadowPlex provides purpose-built deceptions for deployment during blue team actions. ShadowPlex deceptions include

- A comprehensive and extensible deception palette of 350+ prebuilt deceptions includes highly realistic decoys, breadcrumbs, baits, honey accounts, and honeytokens tailored for different computing environments and attack types
- Deceptions provide coverage across a large set of enterprise assets, including identities, endpoints, applications, data, and network
- Deceptions to detect multiple attacker tactics: ShadowPlex deceptions can detect most of the tactics in the MITRE ATT&CK framework, providing comprehensive detection coverage which is of essence for blue teams
- AI for autonomous deception recommendation, freeing up time from blue teams for deployment of deception
- Does not require endpoint agents or affect existing infrastructure or applications
- Auto triaged alerts that provide actionable intelligence for SOC teams and are mapped to the MITRE ATT&CK framework for standardized incident response
- Integrates with SOAR, SIEM, EDR, cloud security, network management, and other security and IT management tools to ensure interoperability with the enterprise security ecosystem

ShadowPlex deceptions have been deployed in numerous red team exercises, conducted by leading enterprises and federal agencies, **with the deceptions detecting the red team in every single occurrence**!

How ShadowPlex deceptions provide an effective countermeasure for a failed red team exercise

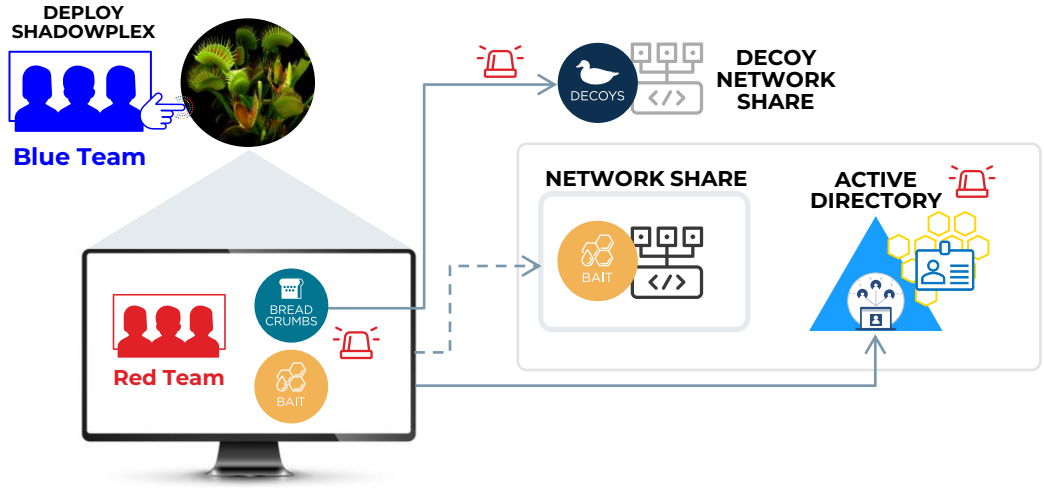
Security teams can leverage the prebuilt deceptions in ShadowPlex to gain visibility for threats that bypass the traditional security solutions. By eliminating the detection gaps, blue teams can gain visibility to stealthy red teaming actions and ensure that subsequent red teaming actions are detected through the enhanced security controls.

Early detection of red teaming actions through the proactive deployment of deceptions: ShadowPlex deception playbooks

Security teams can deploy ShadowPlex deceptions at strategic locations through the pre-packaged deception playbooks in ShadowPlex. This sets the initial defensive landscape, deploying decoys adjacent to the real assets, deploying honey accounts in identity stores, deploying endpoint deceptions (breadcrumbs, baits, honeytokens) on endpoints. Security teams can directly leverage the pre-packaged playbooks available in ShadowPlex to gain the benefit of the deception deployment with minimal administrative effort.

ShadowPlex playbooks leverage AI algorithms to deploy realistic and enticing deceptions that both blend into the environment and serve as lures to attract the threat actor/red teams. The deceptions are placed at strategic locations, on all the attack paths leading to the mission or objective of the red team, to provide visibility for red teaming actions. The deceptions provide early and precise detection of red teaming actions and divert the red team toward the deceptions and away from the real assets, protecting the real assets. ShadowPlex deceptions detect multiple attacker tactics, including discovery/reconnaissance, credential access, privilege escalation, defense evasion, lateral movement, persistence. This provides comprehensive and early visibility to the red team actions. The ShadowPlex alerts are auto triaged, high fidelity, and are mapped to the MITRE ATT&CK framework, providing a standardized taxonomy for incident response. Blue teams can investigate the alerts or configure automated response policies in ShadowPlex to isolate the threat (red team) and prevent the red team action from completing their objective or mission.

Blue Team deploys deceptions for early detection of Red Teaming actions

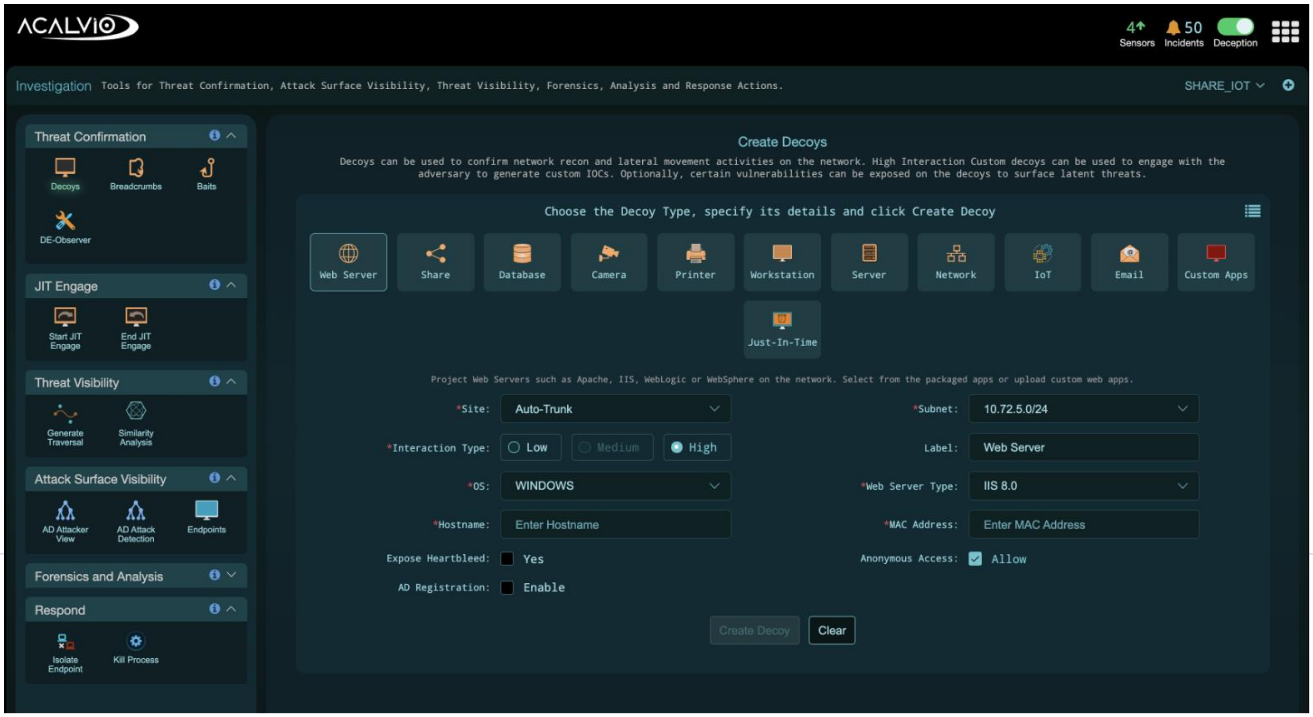


Gather threat intelligence by engaging with the adversary (red team): ShadowPlex high interaction decoys

Security teams that are looking to gain additional visibility into attacker TTPs and generate threat intelligence can deploy ShadowPlex high interaction decoys as part of the initial deception deployment. ShadowPlex high interaction decoys enable defense teams to engage with the adversary (red team) in a safe and secure, instrumented decoy environment. The generated threat intelligence provides insights to blue teams on the novel attacker TTPs employed by the red team, this insight can be used to strengthen the security configurations of existing security controls to reduce the attack surface.

Divert/slow down/gather threat intelligence through the deployment of additional deceptions during an ongoing red/purple team exercise: ShadowPlex threat investigation workbench

Red teaming exercises can be iterative, often known as a purple teaming exercise, where there is collaboration between the blue team and the red team and an iterative and phased approach to the overall red teaming exercise, with a goal of continuous improvement to the security posture. In addition to the initial set of deceptions deployed at the start of the red teaming exercise, blue teams can leverage the ShadowPlex threat investigation workbench to deploy additional, purpose-built deceptions as part of an ongoing red teaming exercise. These deceptions can be used to divert or slow down the red team and/or gather additional threat intelligence by engaging with the red team through the deployment of high interaction decoys.



Summary: gain an effective and proven security solution to ensure successful red teaming exercises

In summary, ShadowPlex deceptions eliminate the detection gaps associated with traditional security solutions. This provides assurance to defense teams that they are well protected for real adversaries and have sufficient coverage for threat detection and response to isolate threats and prevent breaches. ShadowPlex deceptions enable blue teams to gain threat intelligence for attacker TTPs, to strengthen existing security controls. ShadowPlex deceptions represent a powerful approach that provides an effective countermeasure for a failed red team exercise and also serves as a key element of a purple team exercise.

ACALVIO

Acalvio, the leader in cyber deception technology, helps enterprises actively defend against advanced security threats. Acalvio Active Defense Platform, built on 25 issued patents in autonomous deception and advanced AI, provides robust solutions for Identity Threat Detection and Response (ITDR), Advanced Threat Detection, OT Security, Zero Trust, Active Directory Protection and Ransomware Protection. The Silicon Valley-based company's solutions serve Fortune 500 enterprises, government agencies and are available to deploy
on-premises, in the cloud or via marquee managed service providers. For more information, please visit **www.acalvio.com**

© 2024 Acalvio Technologies, Inc. All rights reserved.