



WHITE PAPER

THE LARES INSIDER THREAT METHODOLOGY

INSIDER THREAT

Insider threats occur when individuals within your organization – employees, contractors, or others – misuse their authorized access to compromise your business's critical assets.

ABOUT LARES

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching since 2008.

For more information, visit lares.com, contact us at (720) 600-0329, or follow Lares on Twitter @Lares_.



CONTACT INFORMATION

1580 N. Logan St. Ste 660, PMB 79199, Denver, CO 80203, USA

+1 (720) 600-0329
sales@lares.com

www.lares.com

Executive Summary

Insider Threat assessments evaluate an organization's ability to identify and respond to malicious activity from a trusted user's context or connectivity into the environment. Insider Threats are like Red Team engagements in that they are objectives-based; However, the assessment is carried out from an asset the organization provides. These engagements differ from traditional network penetration testing because, unlike network penetration testing, the consultant does not cast a wide net looking to identify as many vulnerabilities as possible. The consultant assesses the environment and a path that would lead them to the objectives specified by the client.

Insider Threat Assessments are an excellent option for organizations looking to evaluate their ability to detect and respond to a threat actor within their environment without purchasing a full-scale Red Team. Consultants performing these engagements are generally trying to evade detection by the Security Operations Center (SOC), so there is a heavy focus on stealth. Testers often "live off the land" and leverage utilities and software already within the environment to aid in remaining undetected.

Insider Threats operate under an "Assumed Breach" methodology whereby the testing organization simulates that Threat Actors have bypassed perimeter defenses. The engagement is designed to give companies insight into the mind of a skilled adversary by utilizing carefully chosen Tactics, Techniques and Procedures. Consultants often avoid exploiting technical vulnerabilities of systems to maximize the chance of remaining undetected during the engagement.

Methodology Overview

Planning and Preparation

Technical Execution

Documentation and Reporting

Assessment Process

The following phases are conducted during a typical Insider Threat assessment.

Phase I: Planning and Preparation

1.1 Defining Objectives

Lares works with the client to devise an objective, or objectives, that the customer would like the consultant to try to achieve. Some sample objectives might be:

- Access to Personally Identifiable Information (PII).
- Gaining access to Intellectual Property (IP).
- Compromising Source Code repositories or Continuous Integration / Continuous Deployment (CI / CD) pipelines.
- Escalating privileges to Domain Admin within an Active Directory domain.

1.2 Establishing a Trusted Network and Communication Cadence

This step involves identifying parties on the client side that are aware of the testing and will be communicating with the consultant. The group of individuals that are “read in” to the engagement may be referred to as a “Trusted Agent Network,” “White Cell,” or “White Team.” This group knows what is happening on the testers’ side and the defensive side.

During this process, the following will be established:

- How should communications occur? Many clients prefer communication channels that are “out of band” and not visible within the organization.
- The cadence of updates provided by the consultant to the client.
- Members of the client’s team that the consultant can engage with.

Insider Threat Assessments will help organizations answer:

Can a specified objective be accessed starting from an account with “regular” user privileges?

Can abnormal behavior within the network be detected, given an organization’s current telemetry and alerting capabilities?

Are the procedures of the SOC sufficient to quarantine a threat in the event malicious activity is detected?

Phase I: Planning and Preparation (cont.)

1.3 Establishing a Deconfliction Plan

This step involves establishing a plan to confirm whether malicious activity observed by the Security Operations Center during the engagement belongs to the tester. The deconfliction plan ensures that an organization does not need to invest significant resources into Incident Response if the consultant's actions trigger alerts.

The information established at this phase includes:

- Lares will establish the information they require with the client to appropriately confirm if the activity is theirs (timestamps, source IP addresses, affected users, etc).
- How can the consultant regain access if the SOC successfully isolates them?

1.4 Provisioning Access

The last element of preparation for an Insider Threat assessment is discussing how access will be provided to the client environment.

To maximize the chances of a successful engagement, Lares recommends:

- Creating a “standard user” account mimicking the permissions of a typical employee in a business unit outside of IT.
- Provisioning the account as far in advance of the engagement as possible.
- Providing the same type of access that a remote employee would have. (Laptop + VPN, / Virtual Desktop Infrastructure, etc)
- Ensuring the account does not reference security testing:
 - Do not name the account after the name of the tester or use names that might indicate the purpose of the account (for example, Johnny Pentest).
 - No references to security testing in account details.

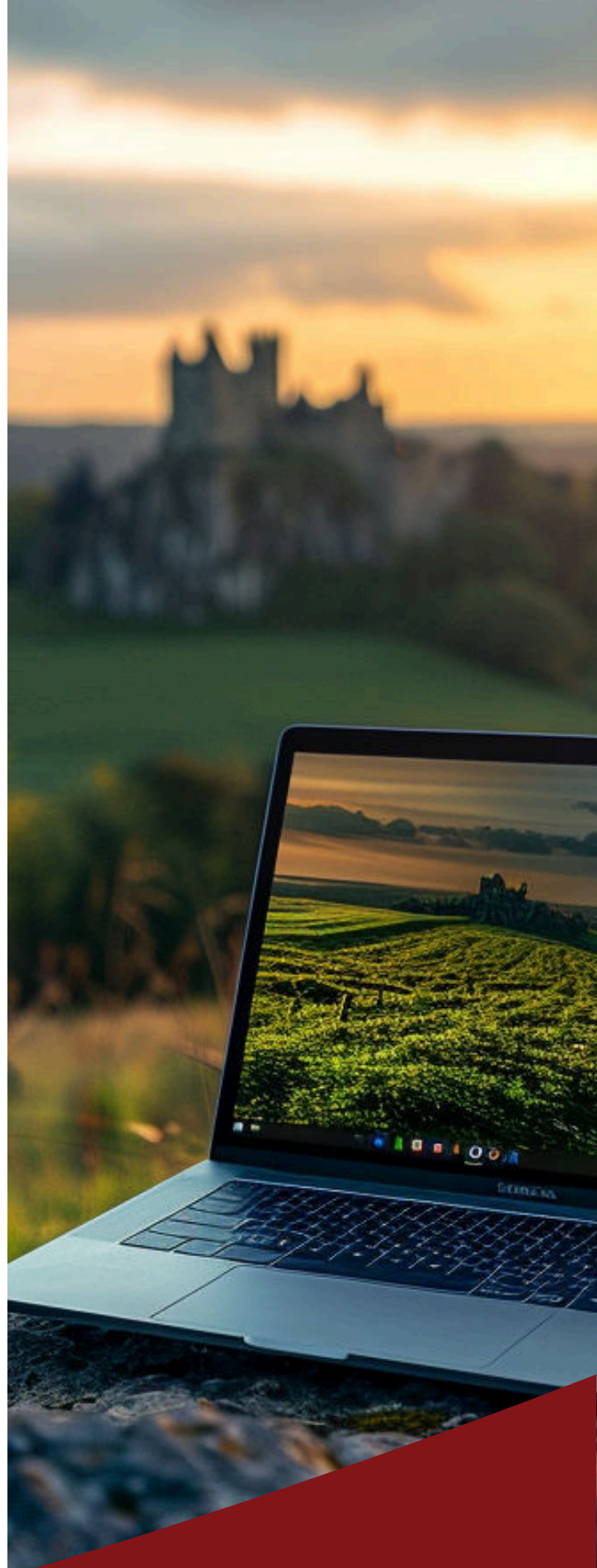
Phase II: Technical Execution

The Technical Execution phase represents the testing phase of the assessment. The consultant has access to the environment, is aware of their objective, and is working towards achieving the objective(s).

Every assessment will follow a different path. However, many Insider Threat Assessments will include the following:

- Navigating to accessible data stores and repositories to identify as much information as possible about the objective(s).
- Active Directory / Identity Provider enumeration to identify groups or accounts that might be useful to achieve the objective(s).
- Using “Living off the Land” techniques and leveraging software and utilities already within the testing environment.
- Lateral movement.
- Utilization of software identified as malicious by Anti-Virus and Endpoint Detection and Response (EDR) products.

During the engagement, the consultant may generate alerts or arouse suspicion from the Security Operations Center. The SOC is encouraged to execute its playbooks if malicious activity is discovered and eradicate the threat as if the attack were real.





Phase III: Documentation and Reporting

This phase involves documenting the results of the previous phases and making recommendations to resolve any issues discovered. The consultant documents efforts during the engagement and that documentation is assembled into a report broken into multiple sections:

- **High-Level Engagement Overview** – This section includes the Executive Summary, positive security practices observed, overall risk assessment, and conclusion.
- **Attack Narrative** - An in-depth overview of the engagement, including the consultant's actions during the assessment.
- **Technical Findings** - A list of findings and associated risk severity ratings identified during the engagement. Remediating identified deficiencies will help bolster the organization's ability to detect and defend against malicious insiders.

Conclusion

Insider Threat assessments are a great option for organizations wanting to test the efficacy of their detection and response capabilities against adversarial tradecraft. Lares is a pioneer and industry leader in the development and utilization of techniques designed to test and organizations ability to respond to threats originating from the context of a trusted user.

If you want to learn more about Insider Threat assessments or how our experts can help scope and execute an effective test for your business, please contact us. We would be happy to discuss the many ways in which we can help keep your organization safe. Thank you for reading!





LARES

A DAMOVO COMPANY

ABOUT LARES

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching since 2008.

For more information, visit lares.com, contact us at (720) 600-0329, or follow Lares on Twitter @Lares_.



CONTACT INFORMATION

1580 N. Logan St. Ste 660, PMB 79199, Denver, CO 80203, USA

+1 (720) 600-0329
sales@lares.com

www.lares.com