CYBERSECURITY SOLUTIONS:

Identity Posture Analysis

getstarted

The challenge

The identity threat landscape is increasingly severe, with even prominent trusted identity providers falling victim to attacks. This highlights the sophistication and persistence of attackers, who employ methods such as phishing, social engineering, and MFA push fatigue.

Strategizing your defense can be challenging. Your identity landscape encompasses all users and accounts across multiple identity providers and the systems that manage them. Identifying all these components is difficult enough, let alone robustly protecting them.

Our solution

The Identity Posture Analysis (IPA) workshop is a **vendor-neutral** review of your identity infrastructure (including any cloud-based identity provider). Its purpose is to help you find and secure the gaps in your identity infrastructure and identify insights for improving your identity posture.

Goals

Key outcomes of the IPA include:

- **Improvement of Identity and Access Management (IAM) Hygiene:** We identify absent/weak MFA, dormant accounts, over-privileged users, and more.
- **Insight into Identity Population:** Gain a unified view of all identities, including detailed activity and device mappings.
- **Increased Knowledge of Identity Threats**: Get insight into the identity-related attacks that are most relevant to your organization.
- **Compliance and Alignment with Relevant Standards:** Monitor for alignment and compliance with the following best practices and regulatory requirements:
  - Center for Internet Security (CIS) best practices
  - Cybersecurity Maturity Model Certification (CMMC)
  - MITRE ATT&CK framework
  - National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - Payment Card Industry Data Security Standard (PCI)
  - Sarbanes-Oxley Act (SOX)
- **Identification of License Savings Opportunities:** Take advantage of license insights to save on inactive accounts.

Workshop details

Our Identity Posture Analysis (IPA) engagement spans two weeks and requires API integrations with select components of your identity stack, such as your primary Cloud Identity Provider (Cloud IdP) used to manage digital entities in the cloud, such as Microsoft Entra ID (formerly Azure AD), Okta or Google Workspace. There is no impact on production and no agents to deploy.

Major milestones include:

Activity	Description
Day 1: Overview Call	30 to 45-minute call to review the Identity Posture Analysis process, technical requirements, and the report outcomes.
Day 2: Integration Workshop	30 to 45-minute workshop to configure API integration between the identity intelligence instance (the tools) with your primary Cloud IdPs.
Day 3-5: Check-up call	30 to 45-minute call to review the integration, answer questions, and highlight critical risks. Discuss and perform optional API integration with additional SaaS application for data enrichment (Salesforce, GitHub, Amazon Web Services), event notification (Microsoft Teams, Slack), ticketing creation (Jira or ServiceNow) and remediation (Microsoft Entra ID, Okta, or Cisco Duo).
Day 14: Presentation and discussion of findings and recommendations	Present the IPA report (1 hour): • Review summary of your current identity infrastructure • Discuss recommendations
Day 21: Data deletion	Upon completion of Identity Security Assessment, tenant and all data will be deleted.

Workshop deliverables

The IPS report will include:

- A summary of the current state of your identity infrastructure.
- Personalized recommendations, with options, for improvement of identity posture.

compucom®
Technology Driven.
People Powered.

Learn more about Compucom and how we source, integrate, and support your technology needs at compucom.com