INTSIGHTS
Defend Forward™

Microsoft

Solution Brief

IntSights for Microsoft

Mitigate Credential Leakage with Active Directory Integrations

Most enterprise security breaches originate with an account compromised by password spray, breach replay, or phishing. Organizations are constantly looking for ways to eliminate credential compromise and shrink their attack surface. In addition to retiring older, less secure protocols, actively limiting access entry points, and exercising more rigorous control over administrative access to new and existing resources, organizations can take a more proactive approach that focuses on end-to-end detection, alerting, and remediation.

IntSights helps customers protect their operations, employees, executives, and, most importantly, their end customers (and their data). Leveraging unique integrations with Active Directory (Azure/cloud and Windows Server/ on-prem), IntSights is turning the tables on proactive defense by transforming aggregated and analyzed threat intelligence into automated security-driven actions. By continuously monitoring your external risk profile, aggregating and analyzing millions of threat feeds, and automating the risk mitigation lifecycle, IntSights delivers a comprehensive, fully automated alerting to remediation methodology.

Integration Overview: How It Works

Active Directory Credential Leakage Mitigation Process

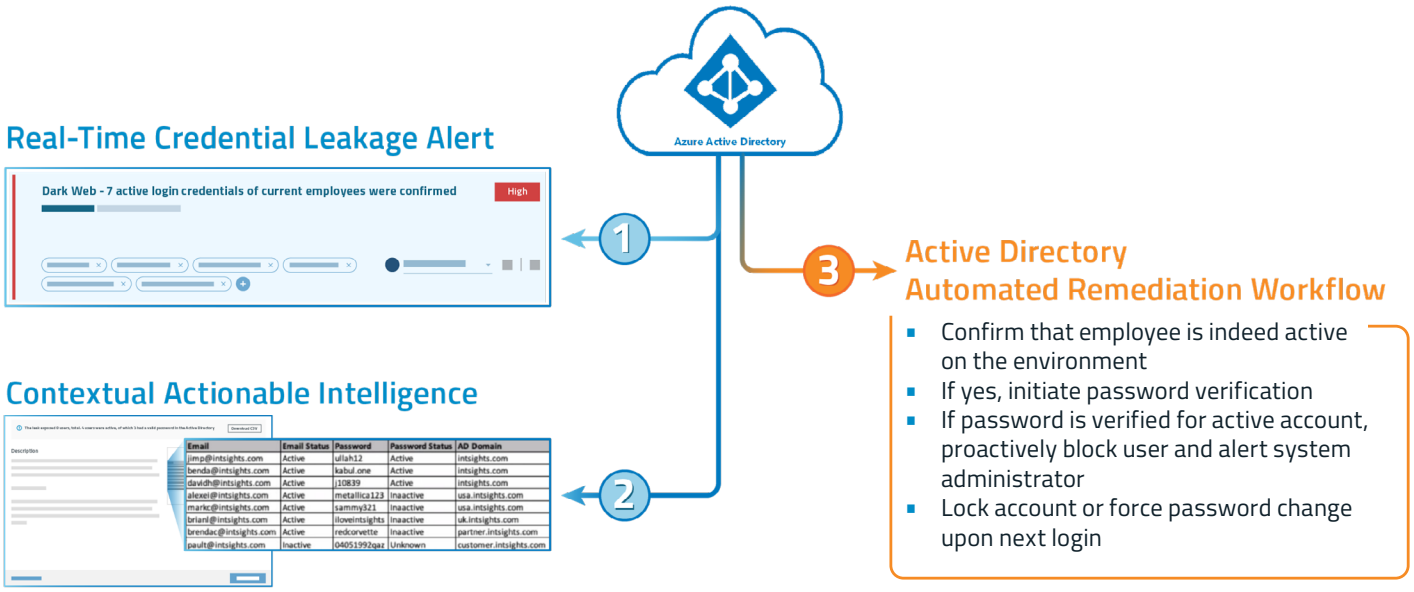
By continuously monitoring the clear, deep and dark web for compromised credentials, IntSights allows organizations to protect themselves from the outside in. This integration is designed to help security practitioners leverage automation to regain control, fully understand the lifecycle of a compromised credential, and keep enterprise data safe.

IntSights automatically delivers an alert whenever it detects leakage of organization-specified credentials. The tight integration with Azure Active Directory, Microsoft's cloud-based identity and access management service, allows immediate validation of usernames and passwords in the Azure AD environment. Consequently, security practitioners can automatically remediate affected users by actively enforcing a password change upon next login or completely blocking access to the compromised accounts.

Integration Benefits

- **Tailored Intelligence:** Continuous scanning of clear, deep, and dark web forums, chat rooms, and social media platforms to identify potential credential leaks
- **Real-time Alerting:** Automated notifications to employees and security teams about potential credential leakage with instructions for immediate remediation actions
- **Out-of-the-box Integration:** Direct integration with Active Directory configurable to force credential updates upon next login to ensure immediate threat remediation and employee protection

Visit: Intsights.com Call: +1 (800) 532-4671 Email: info@intsights.com



- IntSights continuously monitors forums, chat rooms, and social media platforms to identify credential leaks associated with an organization's domains in real time.
- If usernames and passwords are found, IntSights delivers real-time contextual alerts with actionable notifications on the incident and begins an automated process validating the corresponding employee in the Azure Active Directory.
- IntSights' unique visibility and granular alerting allow differentiating between active/inactive users and valid/invalid credentials. If the employee is validated, IntSights confirms the detected password by matching it against the employee's existing password in the Azure Active Directory.
  - If username or passwords do not match the existing entry, IntSights will alert system administrators on its online availability.
  - If username and passwords match the existing entry, IntSights notifies relevant personnel on the leaked credential availability and, based on predefined policies, either locks down the account or requires a password change upon next login.

For additional information on this unique integration, please watch the Azure Active Directory Explainer Video.

Safeguard Your Organization with Office 365 Exchange Online Integration

The IntSights platform also shares threat indicators with Microsoft Exchange Online, a cloud-based hosted messaging solution that gives users access to email, calendar, contacts, and tasks from PCs, the web, and mobile devices. IntSights uses the Exchange "protection" module to block attacks. Domains and IPs are shared with the Exchange server to block malicious IOCs.

IntSights External Threat Protection

The IntSights External Threat Protection (ETP) Suite is the only all-in-one solution purpose-built to detect and neutralize threats outside the wire. Enterprise security teams gain unparalleled visibility into threats targeting their organizations across the clear, deep, and dark web. Integrated one-click remediation ensures prompt enforcement capable of executing simultaneous workflows to initiate external takedowns and push IOCs to internal security devices or applications for immediate threat validation and blacklisting. IntSights ETP delivers the critical data and comprehensive protection security teams need to effectively safeguard their organizations from today's proliferating external threats.

The IntSights Advantage

Proprietary Collection

Gather intelligence from the deepest and hardest-to-reach places on the web.

Tailored Intelligence

Instantly discover threats that matter most to your business by mapping intelligence to your digital assets.

Orchestrated Mitigation

Coordinate proactive response to dismantle and block threats before they cause damage.

Visit: Intsights.com Call: +1 (800) 532-4671 Email: info@intsights.com

About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on LinkedIn, Twitter, and Facebook.

About Microsoft

Microsoft (Nasdaq "MSFT" @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

Learn more about how IntSights and Microsoft can help you build better cyber defenses by actively mitigating credential leakage. Request a demo.