DATA
SHEET

Identity Intelligence for Microsoft

Prevent Corporate Risk Resulting from Identity Compromises

Millions of phishing emails are sent every day, targeting the weakest link in any organization's security posture - employees. This frequent human error opens the door for attackers to gain network access through credential dumping. Meanwhile, overburdened and understaffed security teams have a duty to mitigate threats resulting from leaked passwords, recycled or reused credentials, and identity exposures.

What security teams need now more than ever is a force multiplier. The combination of Microsoft Sentinel's powerful automation and orchestration platform integrated with the Recorded Future Identity Intelligence module is exactly that. Together, they provide the technical force needed to identify and remediate credential leaks in a matter of minutes.

Microsoft and Recorded Future Identity Intelligence

Recorded Future's integration for Microsoft supercharges Active Directory capabilities for identity risk monitoring, providing real-time evidence on exposed credentials and enabling teams to quickly prioritize identity threats and initiate downstream response workflows in Microsoft Sentinel.

The Recorded Future Identity Intelligence module enables security and IT teams to detect identity compromises, for both employees and customers, and respond confidently — without any manual research. Recorded Future automates the collection, analysis, and production of intelligence from a vast range of open source, dark web, and technical sources, and then combines it with world-class research to help drive an accelerated response by security teams. This approach produces real-time intelligence at massive scale, offering an unmatched source of truth for identity authenticity.

BENEFITS

- **Accelerate incident response** from hours to minutes when passwords are exposed
- **Save time and scale resources** by reallocating analysts time previously spent on manual tasks
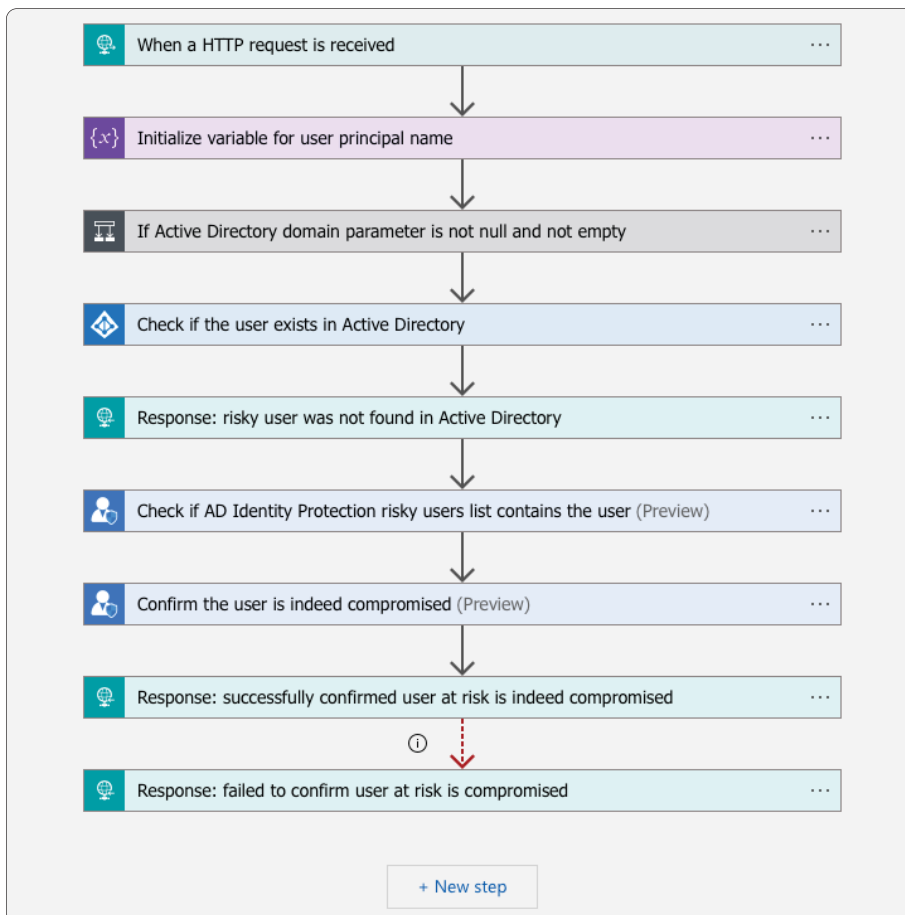- **Comply with NIST password best practices** by leveraging automated password audits

FEATURES

- **Identity Compromise Monitoring:** continuous monitoring for leaked passwords, recycled or reused credentials
- **Automated Password Audits:** compare current passwords against lists of exposed and recycled passwords
- **Integrated Response Controls:** trigger actions like opening a support ticket, force a password reset, or notify the user of finding

By integrating with Microsoft Active Directory, Recorded Future Identity Intelligence complements Microsoft's risk scoring of users as low, medium, or high risk by providing additional insights and transparent context into identity compromises. This additional validation of potential threats gives teams the confidence to conduct deeper analysis and incident response in Microsoft Sentinel.

As identity compromises are detected and pulled into Microsoft Sentinel, automation makes it possible to enrich the exposed accounts, verify if the user is still an employee, check to see whether the current password matches the exposed password, and confirm if it was a recycled password. Depending on the results of this process, Microsoft can then launch actions to begin to resolve the identified issue. Assuming the credentials are valid and current, Sentinel may kick off actions to open a support ticket, force a password reset, and/or to notify the user of the findings.

Since all of this can be done with full automation on a recurring scheduled query, monitoring and responding to identity exposure credential dumps is no longer a complex and time-consuming manual process for analysts.By eliminating the need to manually aggregate, correlate, and triage information, the Recorded Future Identity Intelligence integrated into Microsoft empowers analysts to dramatically reduce the amount of time it takes to detect, investigate, and respond to identity fraud and real risks to their business.

⊕	When a HTTP request is received ⋯
{x}	Initialize variable for user principal name ⋯
⊞	If Active Directory domain parameter is not null and not empty ⋯
◈	Check if the user exists in Active Directory ⋯
⊕	Response: risky user was not found in Active Directory ⋯
👤	Check if AD Identity Protection risky users list contains the user (Preview) ⋯
👤	Confirm the user is indeed compromised (Preview) ⋯
⊕	Response: successfully confirmed user at risk is indeed compromised ⋯
⊕	Response: failed to confirm user at risk is compromised ⋯

+ New step

Recorded Future Identity Intelligence integrated into Microsoft empowers analysts to dramatically reduce the amount of time it takes to detect, investigate, and respond to identity fraud and real risks to their business.