Recorded Future

SWIMLANE

SOLUTION BRIEF

Swimlane and Recorded Future

Prevent Corporate Risk Resulting from Identity Compromises

CHALLENGE

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 Swimlane'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.

THE SOLUTION

Recorded Future's integration for Swimlane continuously monitors for identity compromises, pulling in only those that align with the organization's domain. From here it is able to decipher the threat each set of credentials pose, filtering to the ones that meet the organization's password strength requirements, and then automates response actions necessary for the severity of risk. Armed with real-time evidence on exposed credentials, provided by the Recorded Future Identity Intelligence module, teams are able to quickly prioritize identity threats and initiate downstream response workflows, integrated directly into their existing security and identity tools.

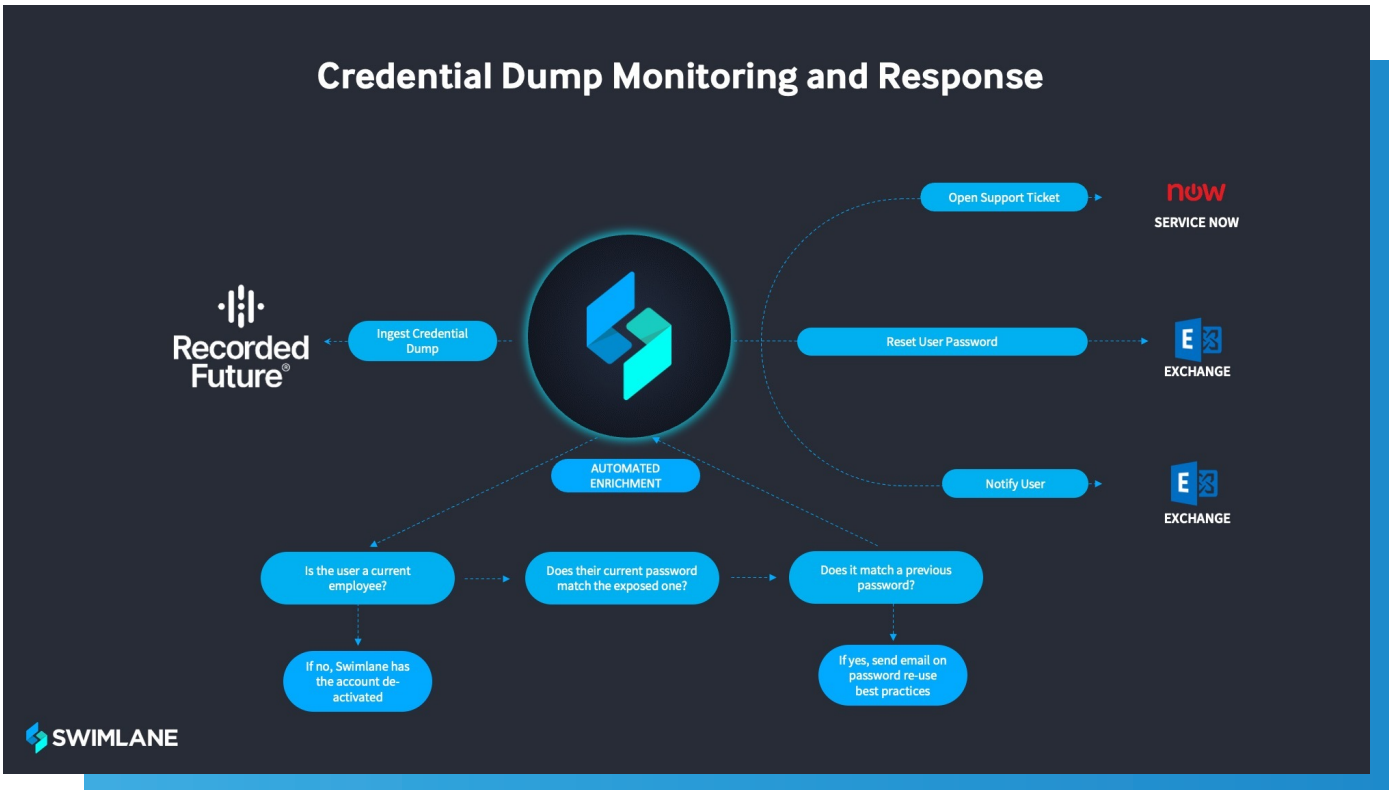
SOLUTION BENEFITS

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 in favor of more strategic work

Comply with NIST password best practices by leveraging automated password audits

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.



BUSINESS VALUE

As identity compromises are detected and pulled into Swimlane, 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 then to check if this was a recycled password. Depending on the results of this process, Swimlane can then launch actions to begin to resolve the identified issue. Assuming the credentials are valid and current, Swimlane may kick off actions to open a support ticket, force a password reset, and/or to notify the user of the findings. In the case of a false positive based on recycled credentials, Swimlane would close the alert and move on to the next alert or exposure. Since all of this can be done with full automation on a recurring scheduled query, monitoring and responding to identity exposure credential dumps no longer has to be a complex and time-consuming manual process.

SOLUTION SUMMARY

- Identity Compromise Monitoring: Continuous monitoring for leaked passwords, recycled or reused credentials, identity and credential exposure
- Automated Password Audits: Compare current passwords against lists of exposed passwords, and recycled passwords to ensure active passwords are not compromised
- Integrated Response Controls: Trigger actions like opening a support ticket, force a password reset, or notify the user of findings in order to remediate detected vulnerabilities

USE CASE SPOTLIGHT:

Revoke Application Access from Former Employees

Employees are leaving the workforce or changing jobs at a record pace. Securely offboarding employees requires IT and security teams to follow procedures to ensure that the departing employees access to corporate systems is revoked. This process is often manual, and therefore error prone. The Recorded Future integration for Swimlane audits active corporate credentials and automatically revokes access in the event that a former employee still has active logins. This results in the remediation of vulnerabilities and time saved for analysts.

Mitigate Ransomware With Company-Wide Secure Passwords

Recycling and reusing passwords is security taboo, but employees inevitably do it anyway. This leaves corporate systems more vulnerable to external threats, and security teams are left to react when a password has been compromised. With the Recorded Future integration for Swimlane, Swimlane notifies security teams when Recorded Future detects use of recycled or commonly used passwords. Security teams are then empowered to educate the specific employees identified about password security best practices.

BETTER TOGETHER

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable.

About Swimlane

Swimlane is at the forefront of the security orchestration, automation and response (SOAR) solution market and was founded to deliver scalable security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages.