Recorded Future®

DATA SHEET

Recorded Future Identity Intelligence for Cortex XSOAR

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 Palo Alto Networks Cortex XSOAR'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.

XSOAR and Recorded Future Identity Intelligence

Recorded Future's integration for XSOAR 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 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 Recorded Future Identity Intelligence, teams are able to quickly prioritize identity threats and initiate downstream response workflows, integrated directly into their existing security and identity tools.

Recorded Future Identity Intelligence 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.

Features

- **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 or recycled passwords and hashes 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

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

As identity compromises are detected and pulled into Palo Alto Networks Cortex XSOAR, automation makes it possible to enrich the exposed accounts, verify if the user is still an employee, check to see whether the current password or hash matches the exposed password, and then to check if this was a recycled password. Recorded Future Identity Intelligence also provides deep context on the compromised identity, including related IP addresses and operating systems, to give organizations the context needed to accurately and confidently remediate the threat. XSOAR will launch actions to begin to resolve the identified issue, such as opening a support ticket, forcing a password reset, or notifying 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 no longer has to be a complex and time-consuming manual process.

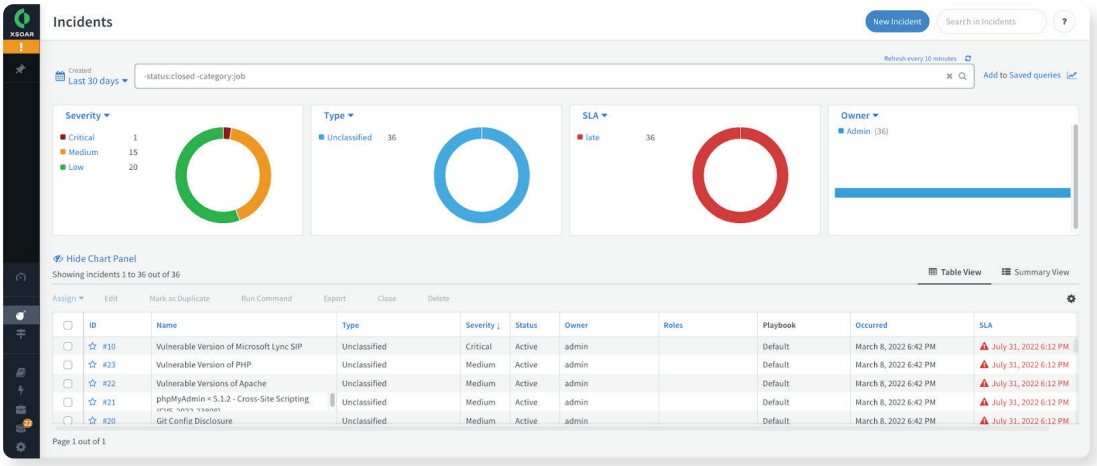
By eliminating the need to manually aggregate, correlate, and triage information, Recorded Future Identity Intelligence integrated into XSOAR empowers analysts to dramatically reduce the amount of time it takes to detect, investigate, and respond to identity fraud and real risks to their business.

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 XSOAR audits active corporate credentials and enables teams to 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 XSOAR, security teams are notified when Recorded Future detects use of recycled or commonly used passwords and password hashes. Security teams are then empowered to educate the specific employees identified about password security best practices and prevent brute force attacks.



Recorded Future Identity Intelligence integrated into XSOAR 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.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com @RecordedFuture