SOAR
SOLUTION
OVERVIEW

Splunk SOAR: Recorded Future Leaked Credential Handling Playbook

Use Case

Leaked credentials can provide a company insight into the future where the next business compromise impact may arise from. Oftentimes, these credentials are sold and purchased on dark web marketplace forums, harvested via malware, or simply dumped into a cloud storage for public access.

Recorded Future’s leaked credential alerts provide companies with actionable intelligence for the compromised accounts that can be used to reset employee or customer passwords, stopping a breach before it can happen.

Issue

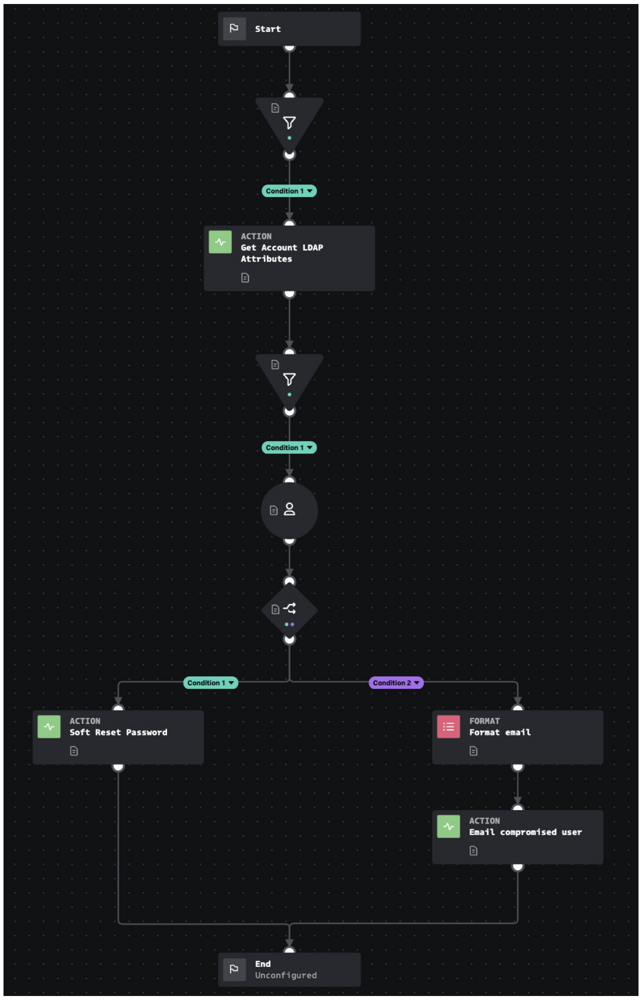
Credential leaks can be tedious to manually address and respond to. Oftentimes, security teams are broken up into separate groups with individual responsibilities. An identity management team might be separate from the threat intelligence team which might be separate from the incident response team.

Sending a request from one team to another will consume minutes if not hours. By automatically resetting an employee credential with a SOAR tool, a security team can respond and contain risk as soon as an alert is received.

Solution

This playbook responds to the Recorded Future monitoring of leaked credentials exposed on the internet alerts. The accounts are first verified if they exist within Active Directory and if they are currently active (enabled/disabled).

If an account exists and is active, a manual prompt to 'soft reset' the account at the next login is issued. A ‘soft reset’ will inform the employee to reset their password next time they log on. This manual prompt can be removed and replaced with an automated reset depending on one's comfort level.



Technical

From a technical perspective this playbook will need the following configured:

- The LDAP app installed with read/write permissions (delegated permissions for password resets are recommended) from Splunk SOAR **https://splunkbase.splunk.com/app/5908**
- The Recorded Future app for Splunk SOAR installed and configured **https://splunkbase.splunk.com/app/6050**

This service will require the Brand Intelligence Module and the Splunk SOAR Integration. The playbook will be included with the Recorded Future App on the Splunk SOAR marketplace.

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