Version 2.0

IBM Cloud Pak for Security
Resilient

Reduce time to respond to and remediate complex cyber threats with orchestration and automation

Organizations face growing security operations challenges - the volume and severity of cyber attacks is increasing, and at the same time hiring and retaining IT security professionals remains difficult. These factors, and others, are contributing to the need for the adoption of security orchestration automation and response (SOAR) tools that can help security teams respond to and remediate complex cyber threats.

IBM Security Resilient empowers security analysts by automating common security operations and incident response (IR) processes, guiding them through the necessary steps to resolve complex cases. They can access important security information quickly with the relevant incident context, enabling accurate decision making and decisive action. It leverages automation to increase the productivity of security analysts and improve the effectiveness of deployed technologies—alleviating the skills gap and alert fatigue.

Solution highlights

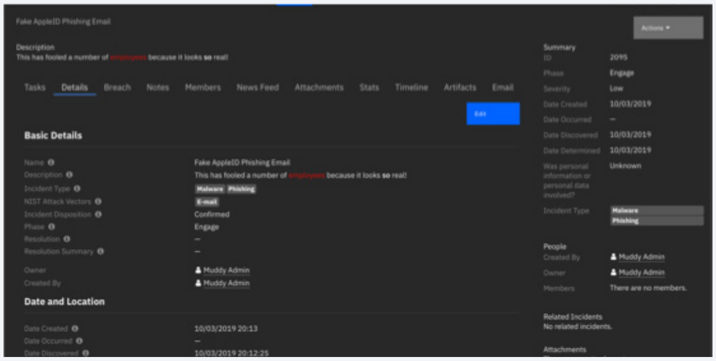
Reduce remediation time by automating manual and repetitive tasks

Improve security effectiveness with orchestration and automation across the incident response process

Prioritize analyst workload by guiding actions with customized playbooks

Improve team collaboration with consistent processes and workflows

Embed best practices through incident response playbooks for common threats



Fake AppleID Phishing Email

Description
This has fooled a number of employees because it looks **so** real!

Basic Details

Name	Fake AppleID Phishing Email
Description	This has fooled a number of employees because it looks **so** real!
Incident Type	Malware Phishing
NIST Attack Vectors	E-mail
Incident Disposition	Confirmed
Phase	Engage
Resolution	–
Resolution Summary	–
Owner	Muddy Admin
Created By	Muddy Admin

Date and Location

Date Created	10/03/2019 20:13
Date Occurred	–
Date Discovered	10/03/2019 20:12:25

Summary

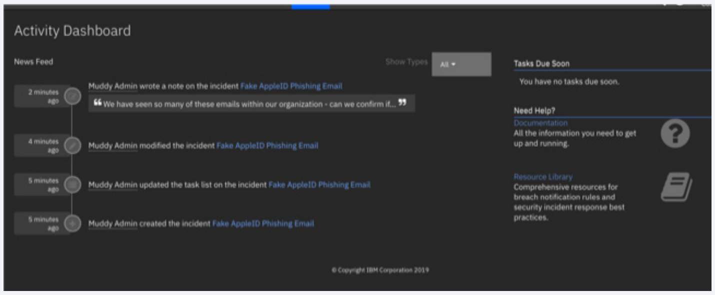
ID	2095
Phase	Engage
Severity	Low
Date Created	10/03/2019
Date Occurred	–
Date Discovered	10/03/2019
Date Determined	10/03/2019
Was personal information or personal data involved?	Unknown
Incident Type	Malware Phishing

People

Created By	Muddy Admin
Owner	Muddy Admin
Members	There are no members.

Related Incidents
No related incidents.

Attachments



Activity Dashboard

News Feed

2 minutes ago — Muddy Admin wrote a note on the incident Fake AppleID Phishing Email
“We have seen so many of these emails within our organization - can we confirm if... ”

4 minutes ago — Muddy Admin modified the incident Fake AppleID Phishing Email

5 minutes ago — Muddy Admin updated the task list on the incident Fake AppleID Phishing Email

5 minutes ago — Muddy Admin created the incident Fake AppleID Phishing Email

Tasks Due Soon
You have no tasks due soon.

Need Help?
Documentation
All the information you need to get up and running.

Resource Library
Comprehensive resources for breach notification rules and security incident response best practices.

© Copyright IBM Corporation 2019

IBM **Security** Learn more at **ibm.com/products/cloud-pak-for-security/resilient**

Measure and improve security operations center (SOC) effectiveness: Reduce the manual steps in incident response through security orchestration and automation, which can be invoked at any step in the incident response process, to improve SOC productivity, processes, and time to resolve.

Streamline security operations management: A common security operations challenge is managing IT complexity. IBM Security Resilient helps security analysts to manage disparate security products across the organization via extensive 3rd party apps and integrations for common security and IT ops tools.

Establish standard IR processes: Security orchestration and automation is a process, not a product. It requires strong foundational blocks—trained people, proven processes, and integrated technologies. With IBM Security Resilient, develop and maintain incident response playbooks for common threats that codify industry best practices and internal procedures.

Proactively manage incident response: Allow security teams to automatically adapt their IR processes to real-time incident conditions, enabling a fast and complete response, with dynamic playbooks. With agile and adaptive workflows built on a sophisticated logic engine, dynamic playbooks update IR plans automatically as new information about an incident is uncovered, using organizations' security tools to ingest data about an incident.

Empower your security team: Enable security teams to orchestrate incident response with visually built, complex workflows based on tasks and technical integrations, and no special programming or coding skills.

Learn more at
ibm.com/products/cloud-pak-for-security/resilient