Barracuda
Your journey, secured.

CHECKLIST

Email Incident Remediation

When it comes to email incident response, time is money. Not only can inefficient incident response monopolize precious IT resources but can result in stolen data, financial loss, and brand damage. Having a remediation strategy can minimize the effects of a potentially devastating email attack. Use this remediation checklist to help prepare your organization for effective incident response.

Prepare

Plan ahead by aligning technology, people, and processes.

Technology

- □ Deploy API-based inbox defense technology to detect sophisticated email fraud.
- □ Securely back-up sensitive data.
- □ Leverage an automated incident response platform.

People

- □ Create a security culture.
- □ Use continuous simulation and training.
- □ Teach users to identify the 13 Email Threat Types

Processes

- □ Document an actionable process for incident response. Use the proceeding checklist items as a template for this process.
- □ Communicate the process to key players.
- □ Make it readily available for quick reference.

Escalate

Reduce monitoring time and quickly escalate to an incident response platform that provides you with the following capabilities:

- □ A central location to monitor and prioritize threats that have been reported or discovered post-delivery.
- □ Proactive threat hunting using a wide variety of classifiers such as unusual locations, suspicious logins, and inbox rules.
- □ Automatic remediation of malicious content.
- □ Mailbox integration for single-click user reporting.

Identify

Identify the nature of the attack, its scope, and the impact on users and infrastructure.

- □ Automate incident creation based on reported emails, post-delivery detection of malicious content, and potential incidents based on past threats.
- □ Gather threat details from the malicious email and identify all affected users and their actions (click, forward, reply, etc.).
- □ Coordinate with your team to understand the status of the incident at all times to maximize efficiency.

Contain

Respond fast and swiftly to minimize the spread of the attacks.

- □ Remove the suspicious email from all affected user inboxes.
- □ Block access to malicious websites.
- □ Alert all affected users, both internal and external.
- □ Enable continuous remediation to stop any future instances of the same attack.

Recover

Recover any lost data and improve your security posture.

- □ Restore data from cloud backup.
- □ Monitor endpoint health.
- □ Reset user passwords.
- □ Update email security policies to blocklist malicious senders, geos, etc.
- □ Utilize community-sourced threat intelligence to bolster your security.

Barracuda®
Your journey, secured.