

Understanding Automatic Remediation and Incident Response

<https://campus.barracuda.com/doc/79463560/>

Review the minimum requirements described in the [Overview](#).

Example Use Case

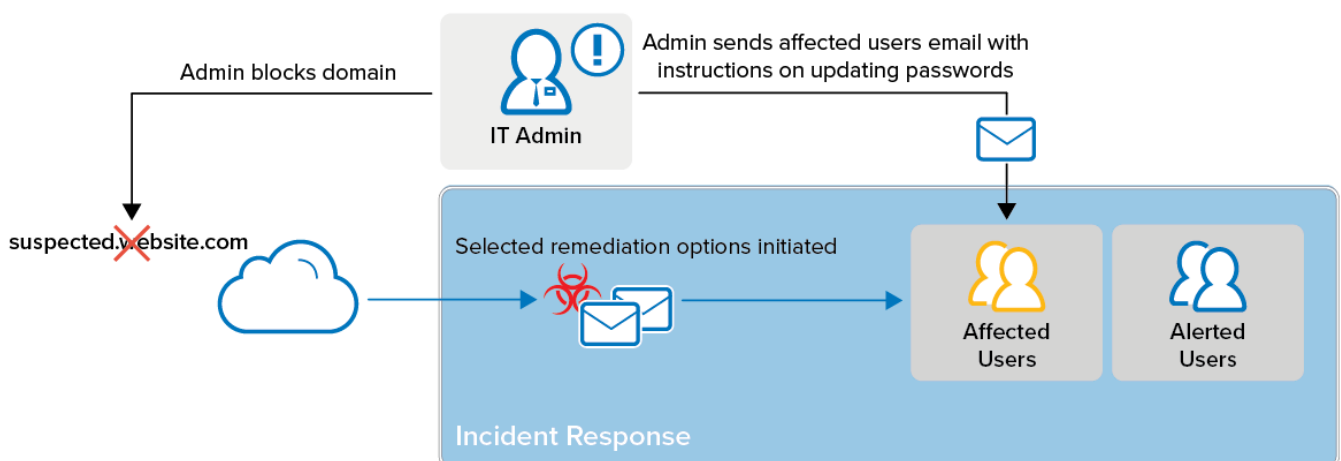
Organization A is hit with a phishing attack from outside the company. The IT team is alerted by an internal user who received the email containing the attack. The IT team must do the following:

- Determine all recipients that received the attack based on the email subject or sender email
- Alert the recipients that received the email in question that they need to change their password and delete the offending email
- Create rules to block future emails from this sender or this sender's domain.

The IT team performs Incident Response tasks including:

- Identifying affected users and providing instructions on updating passwords
- Creating rules in Barracuda Networks to block future emails from this sender or this sender's domain.
- Creating rules that block web access to domains found in the email body.*
- Determining if additional security training is necessary, using [Security Awareness Training](#).*

* This functionality requires Barracuda Email Protection [Premium](#) and [Premium Plus](#) plans.



Figures

1. IRunderstanding.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.