

Best Practices for Email Incident Response Processes



Understand the Threat

- **Identification:** Detect suspicious emails and phishing attempts.
- **Reporting:** Encourage employees to report any suspicious activity.



Evaluate the Risk

- **Analysis:** Utilize automated tools to analyze potential threats.
- **Categorize:** Classify the threats based on their severity and potential damage.



Act Swiftly

- **Response:** Quickly take actions against identified threats.
- **Mitigation:** Isolate and eliminate the threats to minimize damage.



Learn and Improve

- **Review:** Analyze the incident and response to identify any areas for improvement.
- **Train:** Regularly update and train employees to better identify and respond to threats.



Automate and Secure

- **Automation:** Implement automated solutions like Keepnet's Incident Responder for efficient and effective response.
- **Integration:** Ensure seamless integration with email servers for proactive threat management.



Start your **free trial** and see how Keepnet Labs maximize your incident response capability.



 info@keepnetlabs.com