emSigner

eMudhra's Incident Reporting and Response Program

emudhra
Trust Delivered

Copyright

Disclaimer

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between eMudhra and the customer. However, eMudhra has made all reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions. eMudhra will, if necessary, explain issues, which may not be covered by the document.

Feedback

eMudhra welcomes customer comments as a part of the process of continuous development and improvement of the documentation.

Trademarks and Registered Trademarks

Products and product names mentioned in this document may be trademarks or registered trademarks of their individual proprietors.

Table of Contents

Safeguard Your Interests!

At eMudhra, we firmly believe that delivering Trust is a full-time job and not a part-time practice! emSigner's security policies have been designed to offer highest level of assurance to its users. Built in industry leading infrastructure and designed with best-in-class security features, emSigner's platforms are rigorously audited to protect customer data.

emSigner's security program is built on the following core principles-

Deliver Trust

We have over 10 years of experience in operating as a trust service provider in global markets. Leveraging this experience and expertise, we deliver trust across consumer and enterprise facing applications.

Cutting Edge Technology to Power Security

emSigner's technology stack uses industry leading techniques in cryptography, latest systems that guard end-points along with a host of security measures at application, network, and database levels to protect sensitive data. This is backed up by round-the-clock monitoring, logging, and continuous training & awareness programs.

eMudhra's Incident Reporting and Response Program

Security, privacy, and availability of customer's data is extremely important to us and hence eMudhra's Incident Reporting and Response program includes round the clock security monitoring and threat intelligence as well as handling of any vulnerabilities related to security incidents. In addition to all the controls that have been implemented in protection of the infrastructure and the information processed within, conventional wisdom recommends a high level of preparedness for a security incident. This document describes eMudhra Incident Reporting and Response program, including our comprehensive incident reporting process, the regulations that govern it, and measures taken to contain the incident while initiating communication channels for notification and take up corrective measures. Central to this process is the Incident Response Team (IRT), assembled with the purpose of addressing that particular circumstance where there is credible evidence of an incident.

Security Monitoring

We have deployed AWS GuardDuty which continuously monitors our networks to deliver intelligent security analytics and threat intelligence, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Continuous Monitoring and Accurate Threat Detection

Amazon GuardDuty enables us to continuously monitor and analyse all events related to emSigner. Information gathered through GuardDuty tools helps us to detect potential threats and make intelligent, informed decisions regarding an appropriate response for each threat, whether it is a low-risk commodity threat or an advanced, high-risk security threat.

Threat Intelligence

Threats evolve each day and so does eMudhra's security measures to mitigate and respond to newly discovered threats. We use industry standard tools that enable our Security team to filter through the intelligence that we receive and rank them appropriately based on necessary course of action.

Incident Response Team

eMudhra has constituted an Incident Response Team (IRT) that is responsible for coordinating and overseeing the response to incidents in accordance with policies defined. The responsibilities of the IRT team include-

1. Identify and confirm the incident

2. Supervise and direct a consistent, timely, and appropriate response to an incident

3.Provide appropriate communication to parties having a vested interest in the incident

4. Offer appropriate support to the Client or 3rd Party until the incident is resolved

5. Conduct a post-incident review

Incident Management Process

The first goal of the incident management process is to restore a normal service operation as quickly as possible and to minimize the impact on business operations, thus ensuring that the best possible level of service quality and availability is maintained.

The processes for incident handling and response are:

1. Discovery and reporting
2. Initial analysis and classification
3. Containment
4. Notification and communication
5. Corrective measures
6. Closure

Discovery and reporting

Incidents will be discovered through a variety of means including users, system administrators, engineers, and peers; monitoring of infrastructure, services, and resources by operations center; and through monitoring of intelligence channels. The main focus during this phase will be on monitoring security events in order to detect, alert, and report on potential security incidents.

Monitor: Monitor security events across various systems

Detect: Detect potential security incidents by correlating alerts

Alert: Create an incident ticket, document initial findings, and assign an initial incident classification

Report: Reporting process also include accommodation for regulatory reporting escalations

Incident Management Process

Initial Assessment and Classification

The IRT team classifies the incident into Severity 1, Severity 2, Severity 3, etc., classes based on impact and urgency. IRT provides initial acknowledgement and standard response (if any) related to incident.

Containment

The IRT team will determine appropriate activities and processes required to quickly contain and minimize the immediate impact to the Organization, Client, and 3rd Party.

Containment activities are designed with the primary objectives of:

- Counteract the immediate threat
- Prevent propagation or expansion of the incident
- Minimize actual and potential damage
- Restrict knowledge of the incident to authorized personnel
- Preserve information relevant to the incident

Notification/Communication

Designated persons will take action to notify appropriate internal and external parties, as necessary.

Corrective Measures

The IRT will determine the corrective measures to be executed to quickly restore circumstances to a normalized (secure) state.

Closure

The IRT will stay actively engaged throughout the life of the incident to assess the progress/status of all containment and corrective measures, and determine at what point the incident can be considered resolved. Recommendations for improvements to processes, policies, procedures, etc. will exist beyond the activities required for incident resolution and should not delay closing the Incident.

Post Incident Review

A review of incident-related activities is conducted to analyse the things that went right as well as the things that went wrong with regard to an incident, and come up with a better plan to defend the organization and focus resources. We feed this information back to appropriate teams to help drive improvements across the entire organization and supporting processes.

Monitor Post-Incident

Closely monitor for activities post-incident as the threat actors can re-appear again. Analyze system data for any signs of indicators tripping that may have been associated with the prior incident.

Update Threat Intelligence

Update the organization's threat intelligence feeds.

Identify Preventative Measures

The IRT lead will host a Post-incident Review after each incident resolution; this discussion should be scheduled within 2-3 weeks of the incident's remediation. The review is an examination of the incident and all related activities and events. All activities performed relevant to the incident should be reviewed with an eye towards improving the over-all incident response process.

Recommendations

The IRT's recommendations on changes to policy, process, safeguards, etc. are both an input to and by-product of this review. "Fix the problem, not the blame," is the focus of this activity. All discussion, recommendations and assignments are to be documented for distribution to the IRT and Administration, and follow-up by IRT Lead.

Conclusion

eMudhra strives to ensure that our incident response, mitigation, and resolution process is agile and accurate. We continuously monitor the threat landscape, share knowledge with security experts around the world, swiftly resolve incidents when they occur, and feed this information back to our development teams to help ensure the security of eMudhra's products and services.

eMail: support@emsigner.com

Web: www.emsigner.com

About eMudhra

As the world goes Digital, security is ever more crucial to protect identities, data, and enable trust in a digital society. eMudhra focuses on SECURE Digital Transformation to enable organizations to progress and evolve without sacrificing "Trust," which matters most in our society. With an end-to-end stack around trust services, PKI, Paperless transformation, and Digital Authentication, eMudhra is optimally placed to aid digital journeys where identity assertion is critical.

eMudhra chairs the Asia PKI Consortium, is a board member of the Cloud Signature Consortium and a member of the CA Browser Forum. Having been in business for over 12 years and built a reach that spans more than 50 countries, eMudhra is deeply committed to bringing change and helping societies across not just go digital but go digital in a secure way.