Incident Response Plan

RampedUp's Incident Response Plan has seven stages. Proper execution of the response plan requires the efforts of various departments within an organization.

1. **Preparation**: The preparation step is critical. RampedUp Incident Response handlers can respond to cloud-specific events. Ensure logging is enabled using Amazon Elastic Compute Cloud (Amazon EC2), AWS CloudTrail, and VPC Flow Logs, collect and aggregate the logs centrally for correlation and analysis, and use AWS Key Management Service (KMS) to encrypt sensitive data at rest.
2. **Identification**: Also known as Detection, RampedUp uses behavioral-based rules for identifying and detecting breaches, and we are notified about which user accounts and systems need "cleaning up." We open a case number with AWS Support for cross-validation.
3. **Containment**: RampedUp uses AWS Command Line Interface (CLI) or software development kits for quick containment using pre-defined restrictive security groups. Save the current security group of the host or instance, then isolate the host using restrictive ingress and egress security group rules.
4. **Investigation**: Once isolated, determine and analyze the correlation, threat, and timeline.
5. **Eradication**: Secure wipe-files. Response times may be faster with automation. After secure wipe, delete any KMS data keys, if used.
6. **Recovery**: Restore network access to original state.
7. **Follow-up**: Verify deletion of data keys (if KMS was used), cross-validate with Amazon Support, and report findings and response actions.

This document offers guidance for employees or incident responders who believe they have discovered or are responding to a security incident.

Chief Technical Officer: Hunter Eskew

Development Manager: Ian Datang

Severity

Severity	Description	Response
High	A critical breach of RampedUp or customer data	**Identification**: RampedUp uses behavioral-based rules for identifying and detecting breaches and open a case number with AWS Support for cross-validation. **Containment**: RampedUp uses AWS Command Line Interface (CLI) or software development kits for quick containment using pre-defined restrictive security groups. **Investigation**: Once isolated, determine and analyze the correlation, threat, and timeline. **Notify:** Notify any impacted customers and remediation efforts.
Medium	An incident with significant impact to the platform	**Identification**: RampedUp is notified by users or AWS that platform isn't available. **Investigation**: Once isolated, determine and analyze the correlation, threat, and timeline. **Eradication**: Secure wipe-files. Response times may be faster with automation. After secure wipe, delete any KMS data keys, if used. **Recovery**: Restore network access to original state. **Notify:** Notify any impacted customers and remediation efforts.
Low	A minor incident with low impact	**Identification**: RampedUp is notified by user **Investigation**: Once isolated, determine and analyze the correlation, threat, and timeline. **Eradication**: Create a HOT-FIX for remediation **Notify:** Notify any impacted customers and remediation efforts.

Internal Issues

Issues where the malicious actor is an internal employee, contractor, vendor, or partner requires sensitive handling. Please contact the CTO directly and do not discuss with other employees. These are critical issues and must be pushed to follow up.

Response Steps

For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, remediate our vulnerability, and document a post-mortem with the lessons of an incident.

1. CTO will determine if a lawyer be included and attorney client privilege between responders will begin.
2. A central "War Room" will be designated.
3. The following meeting will occur at regular intervals until the incident is resolved:

Breach Response Meeting — Agenda

- Update Breach Timeline
- New Indicators of Compromise
- Investigative Q&A
- Emergency Mitigations
- Long Term Mitigations (including Root Cause Analysis)
- Everything Else

We will *Update a Breach Timeline* with all known temporal data related to the incident. All *Indicators of Compromise* will be updated and shared among breach responders. The group will add new knowns and unknowns to the *Investigative Q&A*. A list of tactical *Emergency Mitigations* will be updated. A list of long term, post breach *Long Term Mitigations* will be updated. Once items related to response are covered, technical responders may leave the meeting and meta-topics (*Everything Else*) related to the breach are discussed (communications, legal issues, blog posts, etc) with leadership.