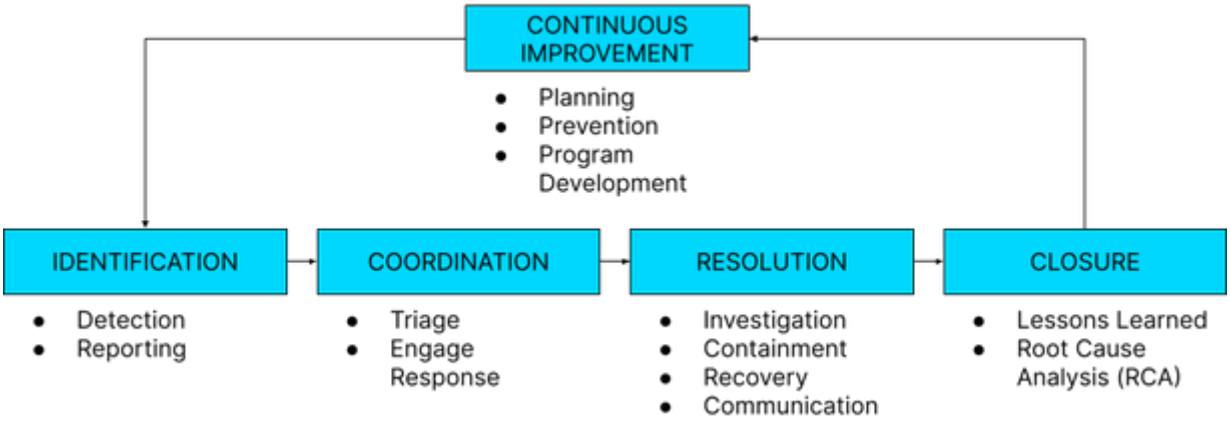
Dremio Security Incident Response Policy

Dremio Security Incident Response Policy

Date of Change	Responsible	Summary Of Change
October 2021	@ Emre Saglam	Added Incident Naming Step
July 2021	@ Emre Saglam	Initial Draft



Purpose

The purpose of this document is to describe the plan for responding to information security incidents at Dremio. This document will explain how to detect, identify and react to cybersecurity incidents and data breaches, determine their scope and risk, respond appropriately and quickly, and communicate the results and risks to all stakeholders.

Scope

This incident response plan applies to the information systems and networks of Dremio as well as any person or device that gains access to these systems or their data. This scope includes Dremio on prem and DCS/DaaS.

Definitions

An incident is an event that violates Dremio's security policies or that threatens the confidentiality, integrity or security of Dremio's information systems or their data.

Examples of incidents include:

- Data breaches
- Unauthorized use of a system
- Unauthorized use of the system as a gateway to other systems
- Unauthorized use of another user's account
- Execution of malicious code that destroys data

Roles and Responsibilities

Below are details about the roles and responsibilities of each member of Dremio to prevent and respond to a cybersecurity incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

Employees are responsible for:

- Abiding by Dremio's policies and procedures surrounding use of Dremio's information systems and their data
- Reporting cybersecurity incidents to security@dremio.com in accordance with the guidelines in Dremio's policies and procedures surrounding use of Dremio's information systems and their data
- Attending training on Dremio's incident response plan, as well as on cybersecurity in the workplace

Managers are responsible for:

- Promoting safe and secure use of Dremio's information systems and their data
- Taking every reasonable measure to protect data handled and stored by Dremio
- Providing Dremio's policies and procedures to their employees
- Assisting with investigations if required
- Reporting cybersecurity incidents to security@dremio.com in accordance with the guidelines in Dremio's policies and procedures

The Incident Response Team is responsible for:

- Assigning an incident commander for incident response plan execution
- Monitoring the implementation of this incident response plan
- Leading risk assessments and root cause analyses
- Leading employee training on this incident response plan as well as on cybersecurity in the workplace
- Reviewing this incident response plan on an annual basis
- Responding to all incidents where immediate assistance is required, taking steps to mitigate immediate risks
- Conducting an initial investigation of all incidents, taking steps to mitigate immediate risks
- Assisting with incident investigations conducted by other departments within Dremio
- Liaising with law enforcement agencies and participating in legal processes if required

SRE and IT team members are responsible for:

- Responding to all incidents where immediate assistance is required, taking steps to mitigate immediate risks
- Notifying all affected stakeholders about the cybersecurity incident or data breach

Incident Response Stages & Procedures

Continuous Improvement

Planning

- Dremio quarterly checks if the incident response plans are conforming to the policies and standards.
- Dremio reviews the plans and does a tabletop exercise yearly to confirm that the plans are effective.

Prevention

- For every P0 security incident, Dremio requires a Root Cause Analysis and Lessons Learned document to identify the improvements.
- Dremio applies these identified previous learnings or security best practices to the processes and technology stack for prevention purposes.

Program Development

- For incidents that require major uplift, Dremio assigns a program to address the findings and drives the program to the resolution.
- The program goals should address the gaps highlighted post-incident and must have deliverables associated with them with tight timelines.

Identification

Detection

- Dremio uses automated and manual processes to detect and identify incidents based on our system logs, application logs, physical access logs and other resources.
- A malicious activity can also be reported by an external party or an internal employee. Dremio reviews these reports and correlates these Indicators of Compromise (IoC) with our findings to enrich the detection process.

Reporting

- Dremio uses automated and manual processes to report the identified incident and issues to Dremio Security Team.

Coordination

Triage

- Incident responder reviews the facts about the incident and does the initial triage and declares an incident
- Incident responder creates a unique name for the incident. From this point the team communicates about the incident using this name only

- Incident response team assigns a severity on the incident (P0: Critical, P1: High, P2: Medium, P3:Low)
- Incident response team assigns a dedicated Incident Commander (IC) on all P0 incidents.

Response Formation

- Incident Commander designates leads from relevant teams and creates an incident response team.
- Incident response team is the evaluator and coordinator of the response effort.

Resolution

Investigation

- Incident response team collects the information and facts about the incident.
- Incident response team can pull in additional resources from the company to help with the investigation and future containment efforts.

Containment

- Incident Response team decides and operates with different resources in the company on steps to limit the damage to the company.
- Dremio immediately takes action on fixing the incident causing issues to stop the bleeding.
- Dremio can limit access to its resources if needed to contain and isolate the incident to a known set of resources and areas of the company.

Recovery

- Once the incident is contained, Dremio restores affected systems and services to their normal operational state.
- Dremio makes sure that the restored systems are benign.
- Dremio makes sure that the underlying issues do not regress to the restored systems. (See also Closure section in details)

Communication

- Incident facts are evaluated to decide whether Dremio should make a notification.
- Incident outcomes are communicated to the appropriate company leads by Incident Response team and/or Incident Response Commander.

Closure

Lessons Learned

- Incident Response team evaluates the response to the incident, if needed makes improvements to the response policies and procedures.
- Incident Response shares the analysis of the defects that caused the incident to the appropriate groups. Incident Commander can assign owners for security uplift detected by an incident.

Root Cause Analysis (RCAs)

- For P0 incidents a Root Cause Analysis document must be filed by the Incident Response Team.