SLATE Incident Response Policy

Version	Comment	Effective date
1.0	Initial version	September 25, 2020

Introduction

This document defines the roles and responsibilities for parties involved in addressing Security Incidents which involve the SLATE Platform.

For the purposes of this document, a Security Incident (incident) is any known or suspected event that compromises or has the potential to compromise any SLATE information asset, including computing infrastructure, confidential data, or computing service.

For information regarding violations and enforcement, please refer to the SLATE Master Information Security Policies & Procedures located at [https://slateci.io/docs/security-and-policies/index.html].

Roles and Responsibilities

SLATE Platform Administrators

The Security Operations Staff (SOS) will be directly responsible for carrying out incident response procedures.

When the SOS become aware of an incident, they will confer to select a Coordinator for the response to it. The Coordinator will generally be the member of the SOS who is best positioned to lead the response, for example due to being located at the affected site, having close contact with stakeholders who are affected, or having detailed knowledge of a SLATE system which is affected.

They will inform and confer with the SLATE Information Security Officer (ISO) as appropriate, and work with the Coordinator to organize necessary communication with Edge Administrators (and security personnel at Edge Clusters' host institution) and Application Administrators.

Other SLATE Roles

Edge Administrators and Application Administrators will report incidents, and coordinate with the SOS to investigate and resolve incidents. Incident reports should provide essential information

This document is a policy of the SLATE (Services Layer at the Edge) project, supported by the National Science Foundation Office of Advanced Cyberinfrastructure: "CIF21 DIBBs: EI: SLATE and the Mobility of Capability", award number OAC-1724821.

about Who, What, When, and Where, as may be known to the reporter.

It is expected that Edge and Application Administrators will have their own response procedures which they will continue to follow in an incident. This includes communication with security teams of affected virtual organizations as appropriate. SLATE seeks to cooperate with these, and this policy does not supersede them.

Communication

During handling of an incident the Security Operations Staff should communicate privately with each other and other involved parties. Communication among the SOS may be via closed Slack channel, and incident notes may be stored in Google Drive, with permissions limited to individuals involved in the investigation. Communications may be sent by email as long as there is no reason to suspect that email accounts or infrastructure are compromised.

All communication regarding security incidents should be marked in accordance with the Traffic Light Protocol (TLP, https://www.first.org/tlp/) for classifying information. By default, communication within the SOS and between the SOS and security personnel at Edge sites should be classified as TLP Red. When handling of an incident is concluded, final conclusions should be shared with all affected organizations using the TLP Amber level, and any public report, such as to be shown on the SLATE website, should be written appropriately to be classified as TLP White.

Escalation Paths

The primary contact address for security issues is security@slateci.io.

Members of the SLATE team who observe a problem which they believe indicates a possible security incident should also promptly contact the Security Operations Staff. This may be done either via the above email address, or through other project-internal communications channels, such as Slack.

The SOS is responsible for beginning and carrying out the incident response procedures. They should also inform the ISO in the event of an incident which appears to be genuine. When the SOS team observes a problem, they should contact the local security personnel at the affected site to coordinate a response.

External Documentation

SLATE will maintain the following on an ongoing basis in order to facilitate response to an incident:

- Relevant contact information for secure communication to and between incident response team members during an incident, e.g., phone numbers and email addresses not hosted on SLATE infrastructure: https://docs.google.com/document/d/1go0DItrKXRbHNK4oBzO6IxrE2vhcMZsE_fBM-iRthLI

- SLATE Platform staff should cooperate with host institutions to monitor SLATE infrastructure, such as by using host institution vulnerability scanning and intrusion detection systems. Mechanisms for accessing data produced by these systems and shared with SLATE should be documented.
- An asset inventory detailing all SLATE Platform IT assets.
    - Overview of SLATE Platform Internals and Security
    - SLATE Information Assets
- One or more documents describing recommended procedures for addressing specific types of security incidents. These procedures should be updated as needed, whenever improved methods are invented.

General Response Procedures

Security Operations Staff

1. Accept and acknowledge reports of security incidents from Edge Administrators, Application Administrators, and host institution security personnel, in addition to proactively monitoring for indicators of compromise.
2. Take action to contain the incident and prevent it from spreading to other systems or organizations as much as possible.
    a. Gather and preserve as much information as possible about what has happened and how.
    b. Record the actions taken, with particular attention to noting times.
3. Assist Edge and Application Administrators to identify the causes and extents of security incidents.
4. Ensure that all affected parties within the Federation are notified within one working day of an incident becoming known. Besides contacting SLATE Edge and Application Administrators, also contact local organization security personnel at affected sites.
5. Coordinate investigation and resolution of security incidents with all affected parties.
6. Facilitate sharing of necessary information among affected parties working to investigate and resolve incidents.
7. Assist in taking necessary actions to correct vulnerabilities and restore proper operation of systems and services and access thereto.
8. If vulnerabilities in one or more applications from the SLATE Application Catalog are found to have contributed to a security incident, coordinate with the relevant Application Developers to ensure that the vulnerabilities are corrected.

9. After each incident is resolved, prepare a report on what took place and how it was dealt with. Reports should be written to be distributed to all affected organizations with a TLP Amber classification, and simplified versions should also be prepared which can be released to the public as TLP White. Such reports should be completed within one month of resolving an incident. The ISO should be consulted to review the drafting of these reports as well as whether its release can be approved by SLATE's management or is escalated to institutional leadership.

In addition to this general procedure, the SOS should maintain documentation on specific procedures for dealing with security incidents affecting particular information systems or classes of systems within the SLATE Platform.

Edge Administrators

1. Follow any security procedures in place with your own organization or site.
2. Take action to contain the incident and prevent it from spreading to other systems or organizations as much as possible.
    a. Gather and preserve as much information as possible about what has happened and how.
    b. Record the actions taken, with particular attention to noting times.
3. Report security incidents affecting the SLATE Federation to the SLATE Platform Team and other participants in the SLATE platform who are suspected to be affected (particularly Application Administrators of applications on affected Edge Clusters) as soon as possible, within at most one working day of an incident becoming known. Share relevant information to allow other parties to determine the impact of an incident. Information sharing should be conducted using the Traffic Light Protocol.
    a. Contact information for other participants in the SLATE federation can be found through the SLATE Portal.
4. Investigate and resolve security incidents within your Edge Cluster(s) and any other affected information systems administered by your organization, in coordination with your local security experts.
5. Share updated information with other affected parties as appropriate.
6. Seek to understand the underlying causes of security incidents to prevent reoccurence.
7. Respond to requests from the SLATE Security Operations Staff and other affected parties in the SLATE Federation working to address security incidents within at most one working day.
8. Take necessary actions to correct vulnerabilities and restore proper operation of systems and services and access thereto.
9. Collaborate with the SLATE Security Operations Staff to compose a report on each incident which can be shared with all affected organizations. Reports should be written to suit a TLP Amber classification, and simplified versions should also be prepared which can be released to the public as TLP White. Such reports should be completed within one month of resolving an incident.

Application Administrators

1. Follow any security procedures in place with your own organization.
2. Take action to contain the incident, preventing it spreading to other systems or organizations as much as possible.
    a. Gather and preserve as much information as possible about what has happened and how.
    b. Record the actions taken, with particular attention to noting times.
3. Report security incidents affecting the SLATE Federation to the SLATE Platform Team and other participants in the SLATE platform who are suspected to be affected (particularly Edge Administrators of any Edge Clusters on which affected applications were installed) as soon as possible, within at most one working day of an incident becoming known. Relevant information to allow other parties to determine the impacts of incidents should be shared.
4. Investigate and resolve security incidents within your Applications(s) and any other affected information systems administered by your organization, in coordination with your own organization's security experts.
5. Share updated information with other affected parties as appropriate.
6. Seek to understand the underlying causes of security incidents to prevent reoccurence.
7. Respond to requests from the SLATE Security Operations Staff and other affected parties in the SLATE Federation working to address security incidents within at most one working day.
8. Take necessary actions to correct vulnerabilities and restore proper operation of systems and services and access thereto.
9. Collaborate with the SLATE Security Operations Staff to compose a report on each incident which can be shared with all affected organizations. Reports should be written to suit a TLP Amber classification, and simplified versions should also be prepared which can be released to the public as TLP White. Such reports should be completed within one month of resolving an incident.

This document is a policy of the SLATE (Services Layer at the Edge) project, supported by the National Science Foundation Office of Advanced Cyberinfrastructure: "CIF21 DIBBs: EI: SLATE and the Mobility of Capability", award number OAC-1724821.