Incident Response Overview

Overview

At Adobe, the security, privacy and availability of our customers' data is a priority. We believe that a company-wide, cohesive incident response program is as critical to the success of an organization as the company's product strategy. To that end, Adobe implements a comprehensive incident response program that includes proactive security monitoring, reactive incident response to software, service, and industry security incidents, and proactive guidance to ensure that employees across the company benefit from the knowledge learned from incidents. Focused on the greatest areas of risk, our corporate incident response program is designed to help enable our customers' trust in security with Adobe.

Table of Contents

The Adobe Incident Response Organization

The Adobe Incident Response Organization consists of two (2) main groups:

- The **Adobe Security Coordination Center (SCC)**, which is responsible for all proactive security monitoring and reactive incident response for all Adobe assets across the entire corporation; and
- The **Adobe Product Security Incident Response Team (PSIRT)** drives Adobe's vulnerability disclosure program. By providing customers, partners, pen-testers and security researchers with a single point of contact and a consistent process to report security vulnerabilities identified in Adobe products and services, PSIRT encourages the external security community to disclose security issues privately and in a manner that minimizes risk to customers, Adobe infrastructure and the brand.

The SCC is a centralized group within Adobe that consists of the Adobe Security Operations Center (SOC), which handles monitoring and alerting, a threat intelligence team, and an incident response (IR) team. These teams work together and with other stakeholders within and outside of Adobe to drive the prevention and early detection of security incidents as well as to continuously improve the company's security posture and maturity. The threat intelligence team focuses on threat actors and methodologies, while the SOC team handles alerts and the triage thereof. Once an alert hits specific incident triggers, the incident response team takes over investigation and mitigation of the incident. The SCC also curates and shares vetted security intelligence to appropriate groups across the organization, to ensure that employees within Adobe benefit from the knowledge learned from incidents.

Figure 1: The Adobe Security Coordination Center (SCC) works with internal and external stakeholders to continuously improve the company's security posture and maturity.

The Adobe Product Incident Response Team (PSIRT)

While the SCC handles general threats to Adobe cloud services, infrastructure, and proprietary corporate information, Adobe PSIRT manages the response to Adobe product vulnerabilities disclosed or discovered by third parties, specifically those that come from independent security researchers. PSIRT encourages private disclosure in a manner that minimizes risk to customers, Adobe infrastructure and the Adobe brand. Adobe PSIRT provides a communication channel for industry partners, independent researchers, CERTs and other stakeholders to privately disclose security vulnerabilities impacting Adobe software, services and infrastructure. PSIRT validates these submissions, and then works with the impacted technology owner to remediate or mitigate the vulnerability.

Proactive Security Efforts

Adobe's proactive security issue identification efforts include continuous monitoring of Adobe services and infrastructure as well as industry threat intelligence information.

Monitoring and Forensics

The security operations center in the SCC uses commercially available security information and event management (SIEM) solutions to consume and analyze various data sources. Local and remote analysis is conducted in a state-of-the-art forensics lab. The SCC uses the information gathered through SIEM 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. Employees continually tune the SIEM tool to filter out noise, eliminate false positives, and help ensure the most critical threats are properly prioritized.

Threat Intelligence

Adobe subscribes to industry threat feeds and email lists, which provide threat intelligence information from industry peers as well as adjacent industries. Information is received in a structured format that enables easy distribution into our SIEM systems. Adobe has a multi-faceted threat intelligence program using a combination of automation using industry standard tools and employee reviewers to filter through the intelligence we receive. The combination of external and internal sources is used to appropriately rank intelligence based upon necessary course of action.

Industry Collaboration and Knowledge Sharing

Adobe collaborates with other software vendors and technology companies to share knowledge and security threat information. In addition, Adobe participates in industry organizations, such as FIRST.ORG, MAPP (Microsoft Active Protections Program) CISO Coalition, SAFECode (the Software Assurance Forum for Excellence in Code), and MAAWG (Messaging, Malware and Mobile Anti-Abuse Working Group), as well as other private, inter-company incident response working groups.

Penetration Testing

Adobe approves and engages with leading third-party security firms to perform penetration testing that can uncover potential security vulnerabilities and help improve the overall security of Adobe products and services. Upon receipt of the report provided by the third party, Adobe documents these vulnerabilities, evaluates severity and priority, and then creates a mitigation strategy or remediation plan.

Reactive Security Efforts

The primary objective of Adobe's incident response efforts is to return systems to a known good state that is free of compromise. Because each security incident is unique, defining rigid, step-by-step instructions for handling each incident is impractical. Instead, Adobe has created a well-defined, methodical flow for each defined security incident.

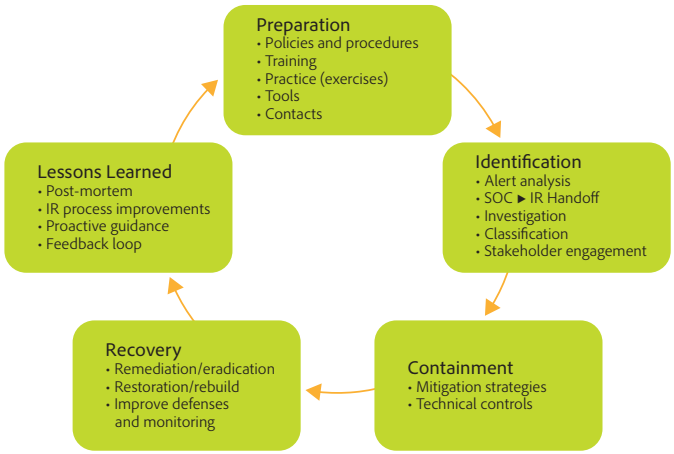

Figure 2: Adobe Incident Response Lifecycle

Phase I: Planning and Preparation

While it is always easier to plan and prepare for security incidents than to repair and recover from them, incidents do occur, despite best efforts and intentions of company employees. In order to help mitigate any potential issues that inhibit the incident response process, Adobe has implemented the following key elements across the company:

- Security policies and procedures
- Alert and Incident response handling methodologies
- Call tree and notification processes for solutions, products and support teams
- Regular skill development, improvement and training for information security staff
- Incident response plan testing, team drills and tabletops
- Collection of threat and vulnerability intelligence
- Tool kit inventory, improvements and regular updates

Phase II: Identification Feedback Loop

Adobe defines a security alert as "a notification or event, that, when taken in conjunction with additional information beyond the event itself suggests a potential threat to a system, environment, process or workflow that may result in disruption of service, liability, brand impact or possible compromise to the confidentiality, integrity or availability of Adobe infrastructure." Security alerts may be system-generated or initiated by an individual, and can take the form of user/customer notification, an anomaly detected by internal Adobe personnel, an alert from a software tool monitoring the network or its endpoints or a communication from threat intelligence channels and security researchers, including crowd-sourced penetration testing organizations.

To be classified as a security *incident*, an alert must be accompanied by confirmation, validation or a reasonable suspicion that an Adobe-defined incident trigger has also been met. The SCC has several defined triggers, including:

- Involvement or compromise of Personal Information (PI)
- Notification about a suspected security incident from an external (non-Adobe) party
- Any security event that impacts the broader technology industry (i.e., issue with commonly used open source code)
- Impact to confidential and/or restricted data
- Suspected malicious access to non-public data
- In-progress active exploitation
- Active or required involvement from law enforcement, legal, customer communications, PR or other third party
- Requested classification of an alert as an incident by any member of the SCC

Any security alert can be escalated to incident status for further investigation when the results of a preliminary investigation are inconclusive.

Incident Severity Levels

Adobe defines incident severity as follows:

Severity	Description	Definition
0	Crisis/Critical	Incident of such severity as to require all available resources and the participation of C-level executives.
1	High	Causing severe impact/damage/disruption to customers, employees, infrastructure. Probable or known impact of restricted data (as defined in the Adobe Data Handling and Classification Standard). Probable or known impact of confidential data (as defined in the Adobe Data Handling and Classification Standard) that is a customer asset or employee, customer, or vendor personal data.
2	Medium	Causing moderate impact/damage/disruption to customers, employees, infrastructure. Probable or known impact of confidential data (as defined in the Adobe Data Handling and Classification Standard) that is not a customer asset or personal data. Known by a third party.
3	Low	Causing minor/negligible impact/damage/disruption to customers, employees, infrastructure. Probable or known impact to internal data (as defined in the Adobe Data Handling and Classification Standard).
4	Informational	Causing no impact/damage/disruption to customers, employees, infrastructure. No action required, but should be tracked.

Figure 5: Adobe incident severity classifications

After a severity level has been set, the SCC begins incident handling and response, which includes gathering data (e.g., logs and forensic images) to help determine the root cause of the incident as well as the best course of action for mitigation.

Phase III: Containment Feedback Loop

The purpose of the containment phase is to limit any damage and prevent any further damage from occurring. Incident handlers work with incident responders within the SCC to understand and document the necessary steps to minimize the effects of the Incident. Based on recommendations from the incident handler, incident responder(s), and other stakeholders, a containment strategy is implemented by the appropriate parties. In the incident containment phase, the SCC considers the following:

- How was the threat launched and from where?
- What assets have been impacted and what damage has been done?
- Is the incident limited to a single machine or has there been lateral movement in the network?
- Do we need to review logs or conduct memory forensics to better understand the threat?
- What is the motive and methodology behind the malicious activity?
- Do we need to gather additional intelligence in order to monitor the threat in other areas of the business?
- What is the service impact upon containment?
- How can we measure and track the success of containment?

Phase IV: Remediation and Recovery

Once the SCC contains a security incident, it moves on to the remediation and recovery phase of the incident lifecycle, which works towards ensuring that systems are cleansed of any malicious or other illicit content and ready to be used again within the organization. The incident handler works closely with stakeholders to determine the timing of incident remediation, eradication and recovery and the assignment of testing and validation. This process may not be swift, as it takes time, careful planning and adequate resources to be successful. While the exact steps involved in remediation and recovery are dependent on the organization and the incident type, the following areas and actions are considered:

- Patching and hardening system images
- Reimaging systems
- Implementing password changes
- Improving monitoring and defenses

Where necessary, customer notification is also covered in this phase of Adobe's incident response lifecycle. If the incident is determined to manifest itself as a product vulnerability, Adobe follows the PSIRT notification process, which includes issuing a customer bulletin about the incident and an estimated timeframe for resolution. Adobe issues another PSIRT bulletin upon implementation of the product fix.

For all other incidents (i.e., non-product vulnerabilities), Adobe immediately issues a customer notification if we are legally or contractually required to do so. Customer notification requirements are governed by the laws and regulations of the countries in which the incident occurred.

Phase V: Lessons Learned

After an incident has been resolved, the SCC enters the final phase of the incident response lifecycle, which includes processes and feedback loops, such as a port-mortem analysis. By conducting a post-mortem analysis for incidents, which highlights what went right and what went wrong, how to better defend the organization, and where the organization should focus resources, the SCC can provide proactive guidance to and drive improvements across the entire Adobe organization and, when required, to supporting processes.

How Incident Response Impacts Regulatory Compliance

A solid, well-thought-out incident response plan is a critical component of regulatory compliance, as most regulations include a formal, documented IR plan as a requirement for compliance. Adobe's robust strategy, outlined in this paper, for both proactive and reactive security measures plays an important role in maintaining compliance. It includes multiple layers of controls to help ensure the security and privacy of customer information as well as Adobe products, creating a fall-back plan if any single control happens to fail. Constant updates to the IR plan help Adobe make sure we stay up to date on the latest incidents and can remain compliant now and in the future.

For information about the various compliance standards and regulations supported by Adobe offerings, please see the Adobe Cloud Services Compliance Overview.

Conclusion

Adobe strives to ensure that our incident response, mitigation, and resolution process is nimble 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 highest levels of security for all Adobe products and services.

Please visit the Adobe security information site at http://www.adobe.com/security for more information about security efforts across our products and services.

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com