WHITE PAPER

The Adobe Incident Response Program

October 2024

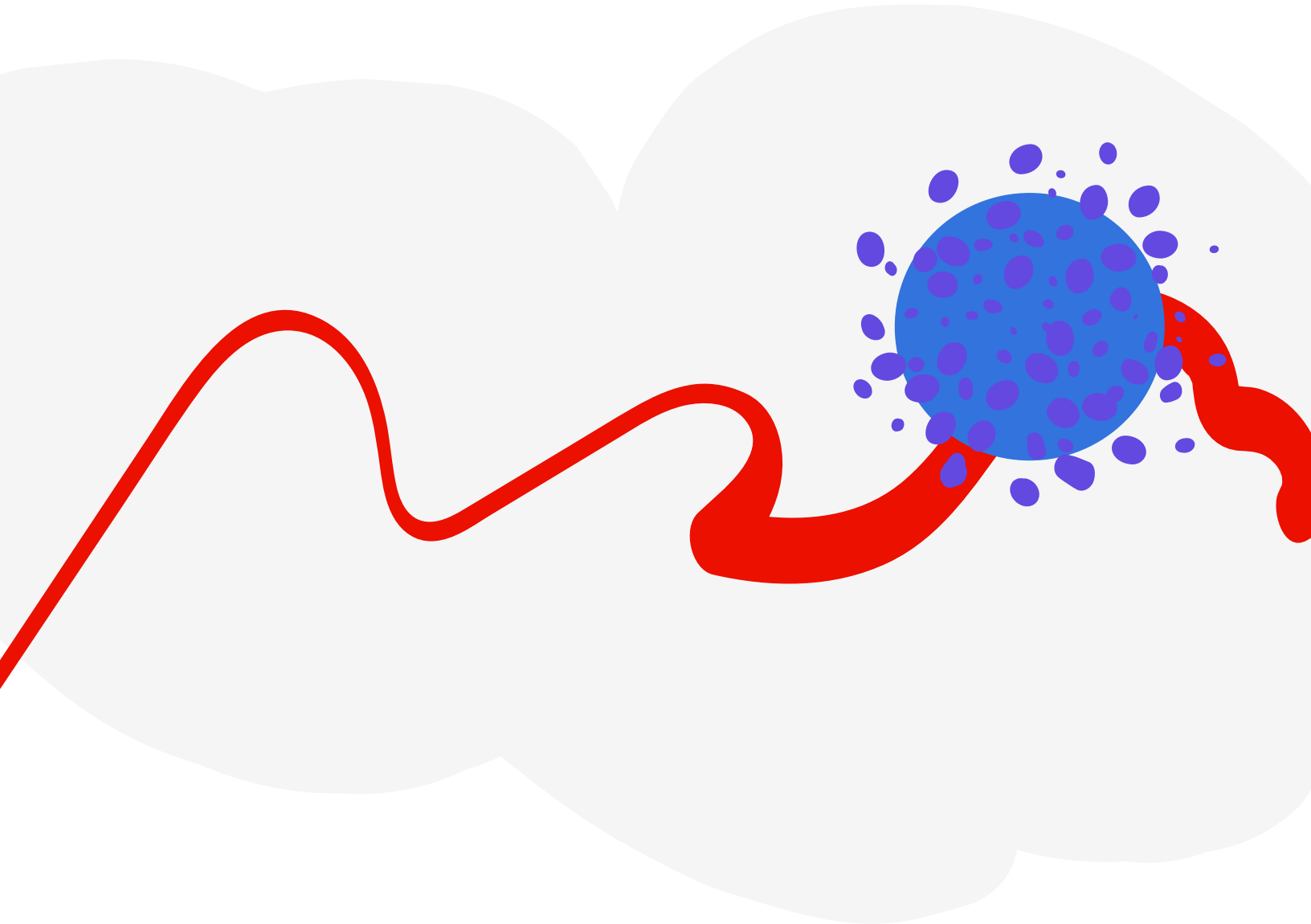

Table of Contents

Introduction

Trust. It's what Adobe works every day to gain from our customers. The security, privacy, and availability of our customers' data is important to us, which is why the Adobe Incident Response (IR) program includes both proactive security monitoring and threat intelligence as well as vulnerability handling and response to software, service, and industry security incidents. Designed, implemented, and managed by recognized experts in security, the Adobe Incident Response program is based on proven processes and leverages cutting-edge automation and machine learning to give a 360-degree view of the security posture of each of our products and services as well as our infrastructure – so customers and partners can deliver more trusted experiences to users every day.

This white paper describes the Adobe Incident Response program, including our comprehensive incident response process and the regulations and standards that govern it, as well as our vulnerability handling procedures, including detection, mitigation, and communication with customers for every potential event. The various security teams within Adobe work together and with industry peers to help ensure an effective incident response program.

The Adobe Incident Response Program

Due to the ever-increasing number of cyberthreats from a range of bad actors, including nation-states, incident response as a discipline has evolved significantly in the last few years. State-of-the-art incident response programs include both proactive monitoring and active mitigation to help protect customers from a wide range of attack vectors. A comprehensive incident response plan is also a critical component of regulatory compliance, as most regulations include a formal, documented IR plan as a compliance requirement.

Adobe's multi-layered strategy, outlined in this paper, plays an important role in maintaining compliance. Our program includes proactive security monitoring and threat intelligence, vulnerability monitoring and handling, and reactive incident response to help give customers peace of mind that their sensitive data remains safe and secure. Regular testing and updates to the IR plan help Adobe make sure we stay current on the latest incidents and remain compliant with our standards now and in the future.

Security Monitoring and Threat Intelligence

Our proactive security efforts include continuous monitoring of Adobe products, services, and infrastructure and analysis of industry threat intelligence to detect potential issues, and we leverage automation, AI (artificial intelligence), and ML (machine learning) to model potential threat vectors and train our systems to help detect emerging threats.

In addition, we collaborate with other software vendors and technology companies to share knowledge and security threat information. Adobe participates in industry organizations, including 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.

Monitoring and Detection

Adobe uses commercially available SIEM (security information and event management) solutions to consume and analyze various data sources. Information gathered through these tools helps Adobe to detect potential threats and make intelligent, informed decisions about the appropriate response for each threat, whether it is a low-risk commodity or an advanced, high-risk security threat. Adobe employees continually tune our SIEM tools to filter out noise, eliminate false positives, and help ensure the proper prioritization of the most critical threats.

Additionally, we deploy a suite of advanced security tools, including Cloud Security Posture Management (CSPM), Data Security Posture Management (DSPM), Data Loss Prevention (DLP), and Endpoint Detection and Response (EDR) systems. These technologies work in tandem to help enhance our security posture by continuously monitoring cloud environments, securing sensitive data, preventing data exfiltration, and detecting and responding to endpoint threats. Collectively, the tools act as our "early warning system" to help Adobe quickly identify vulnerabilities, determine potential impact to Adobe's infrastructure, systems, and data, mitigate risk, and respond swiftly to both emerging and persistent threats.

Threat Intelligence

New vulnerabilities are discovered every day, and Adobe strives to quickly respond to and mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT and SANS, Adobe also monitors multiple industry threat feeds and security alert lists issued by major security vendors. These sources provide threat intelligence information from industry peers as well as adjacent industries. We use industry-standard tools and employee reviewers to filter through and rank intelligence we receive based upon the necessary course of action.

Forensics

For incident investigations, Adobe follows an extensive forensic analysis process, which may include complete image capture or memory dump of the impacted machine(s), evidence safe-holding, and chain-of-custody record, as appropriate. Local and remote analysis is conducted in our state-of-the-art forensics lab. When needed and appropriate, we work with third-party forensics companies as well.

Automation

Adobe's automation tools and processes help decrease the time between detection and remediation. Adobe leverages industry-standard SOAR (Security Orchestration, Automation, and Response) platforms to optimize the handling of vulnerabilities, alerts, and events at scale. Among other areas, we implement automation to create and send new tickets to the correct engineering team for faster resolution, notify engineering owners of upcoming due dates throughout the entire lifecycle, and generate dashboards with daily, weekly, and yearly trend analysis for all vulnerabilities to help us meet our resolution-time objectives.

Vulnerability Handling and Incident Response

When a software, service, or industry-wide cybersecurity incident occurs that may impact or compromise the confidentiality, integrity, or availability of our infrastructure, or if a third party discovers or discloses a vulnerability in one of our products, Adobe follows our proven incident response process.

Customer notification of vulnerabilities not related to an Adobe product, such as industry-wide or third-party vulnerabilities, only occurs if internal investigations confirm an impact to our systems or customer data. Our customer notification process adheres to the relevant contractual, regulatory, and statutory requirements in the context of the specific vulnerability or incident.

If the vulnerability or incident involves privacy or legal issues, the Adobe Privacy Office and Cybersecurity Legal promptly engages in the process to drive the legal analysis of considerations that may be relevant in the context of a vulnerability or incident. As part of this investigation and analysis, the cybersecurity legal team evaluates and determines whether notifications to customers, individuals, regulators, or any other third parties are legally necessary or appropriate.

The Adobe Incident Response Lifecycle

The primary objective of our incident response efforts is to return systems to a known good state that is free of compromise. Because each 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.

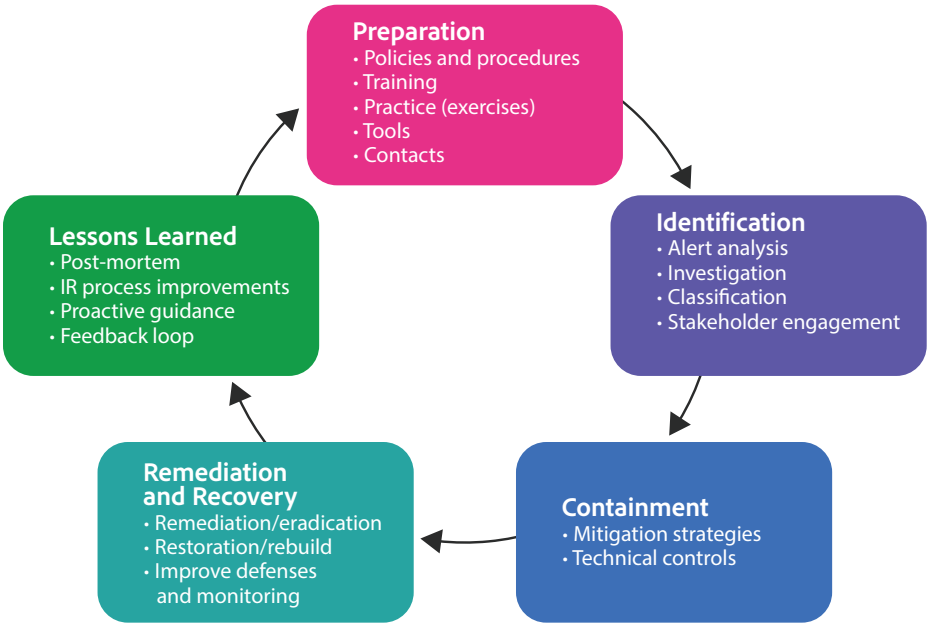

Figure 1: The Adobe Incident Response Lifecycle

Phase I: Preparation

While it is always easier to plan and prepare for security incidents than to repair and recover from them, incidents do occur, despite the best efforts and intentions of company employees. 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
- Incident response handling methodologies
- Call tree and notification processes for solution, product, and support teams
- Regular skill development, improvement, and training for information security staff
- Incident response plan testing, team drills, and tabletop exercises
- Collection of threat and vulnerability intelligence
- Toolkit inventory, improvements, and regular updates

Phase II: Identification

Security alerts are notifications of events 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 crowdsourced penetration testing organizations.

To be classified as a security incident, an alert must be accompanied by confirmation, validation, or a reasonable suspicion that the activity meets an Adobe-defined incident indicator. These indicators include:

- Involvement or compromise of Personally Identifiable Information (PII)
- Notification about a suspected security incident from an external (non-Adobe) party
- Any security event that impacts the broader technology industry (e.g., an 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 Adobe Incident Response organization (see next section)
- Inconclusive results from a preliminary investigation

Incident Severity Levels

After assigning a severity level for a particular incident according to our internal operational policies, Adobe begins incident handling and response. This process includes gathering data (e.g., logs and forensic images) to help determine the root cause of the incident and the best course of action for mitigation.

Once an alert hits specific incident indicators, the incident response team begins investigating and mitigating the incident. Vetted security intelligence is shared with relevant groups across Adobe to help ensure that the knowledge learned from incidents reaches appropriate teams.

Phase III: Containment

The containment phase focuses on limiting any damage or preventing further damage. Incident commanders work with incident responders to understand and document the necessary steps to minimize the effects of the incident. Based on recommendations from the incident commander, incident responder(s), and other stakeholders, a containment strategy is implemented by the appropriate parties.

Phase IV: Remediation and Recovery

Once Adobe has contained a security incident, we move to the remediation and recovery phase of the incident lifecycle, which works toward ensuring that systems are cleansed of any malicious or other illicit content and are ready to be used again within the organization.

The incident commander works closely with stakeholders to determine the timing of incident remediation, eradication, and recovery, as well as 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, Adobe considers the following areas and actions in the remediation and recovery phase:

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

The remediation and recovery phase of the incident response cycle may also include customer notification. For product-related vulnerabilities, Adobe follows our defined product vulnerability notification process, which includes issuing a security bulletin. These bulletins inform customers of the vulnerability category, vulnerability impact, severity, CVSS base score, CVSS vector, CVE number (as well as the affected versions), and the steps to take to remediate the vulnerability.

As noted previously, Adobe proactively notifies customers of vulnerabilities not related to an Adobe product, such as industry-wide or third-party vulnerabilities, if internal investigations confirm a notifiable impact to our systems or customer data. Adobe does not respond to inquiries concerning vulnerabilities if investigations determine that there is no impact to Adobe's systems or customer data.

Phase V: Lessons Learned

After an incident has been resolved, Adobe enters the final phase of the incident response lifecycle, which includes an incident retrospective. This analysis highlights how to better defend the organization, and where the organization should focus resources. The incident response team feeds this information back to appropriate teams to help drive improvements across the entire organization and supporting processes.

The Adobe Incident Response Organization

Adobe centralizes security monitoring, threat intelligence, and incident response for Adobe assets in the Adobe Cyber Defense Center. Operating 24/7, the organization is dedicated to information security and privacy with a mission to continuously monitor and improve Adobe's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Within the Adobe Cyber Defense Center, the Adobe Cyber Security Incident Response Team (CSIRT) handles general threats to Adobe cloud services, infrastructure, and proprietary corporate information monitoring and alerting and includes security monitoring, threat intelligence, vulnerability management, and incident response for external and industry-wide security threats.

The Adobe Product Security Incident Response Team (PSIRT) manages the response to vulnerabilities found within Adobe products, disclosed or discovered by third parties and independent security researchers. PSIRT provides 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 and encourages the external security community to disclose security issues privately and in a manner that minimizes risk to customers, Adobe infrastructure, and the brand.

When a vulnerability is discovered and submitted to Adobe, PSIRT validates the vulnerability and then works with the impacted product or service team to remediate or mitigate the vulnerability.

All Adobe incident response teams work together and with other stakeholders within and outside the company to help drive the prevention and early detection of and prompt response to security incidents as well as to continuously improve the company's security posture and maturity.

Conclusion

Adobe strives to ensure that our incident response, mitigation, and resolution process is nimble and efficient. We continuously monitor the threat landscape, share knowledge with security experts around the world, resolve incidents when they occur, and feed this information back to our development teams to help ensure the highest levels of security for Adobe products and services.

Please visit the Adobe Trust Center for more information about Adobe's security efforts and controls.