WHITE PAPER

Adobe® Incident Response Overview

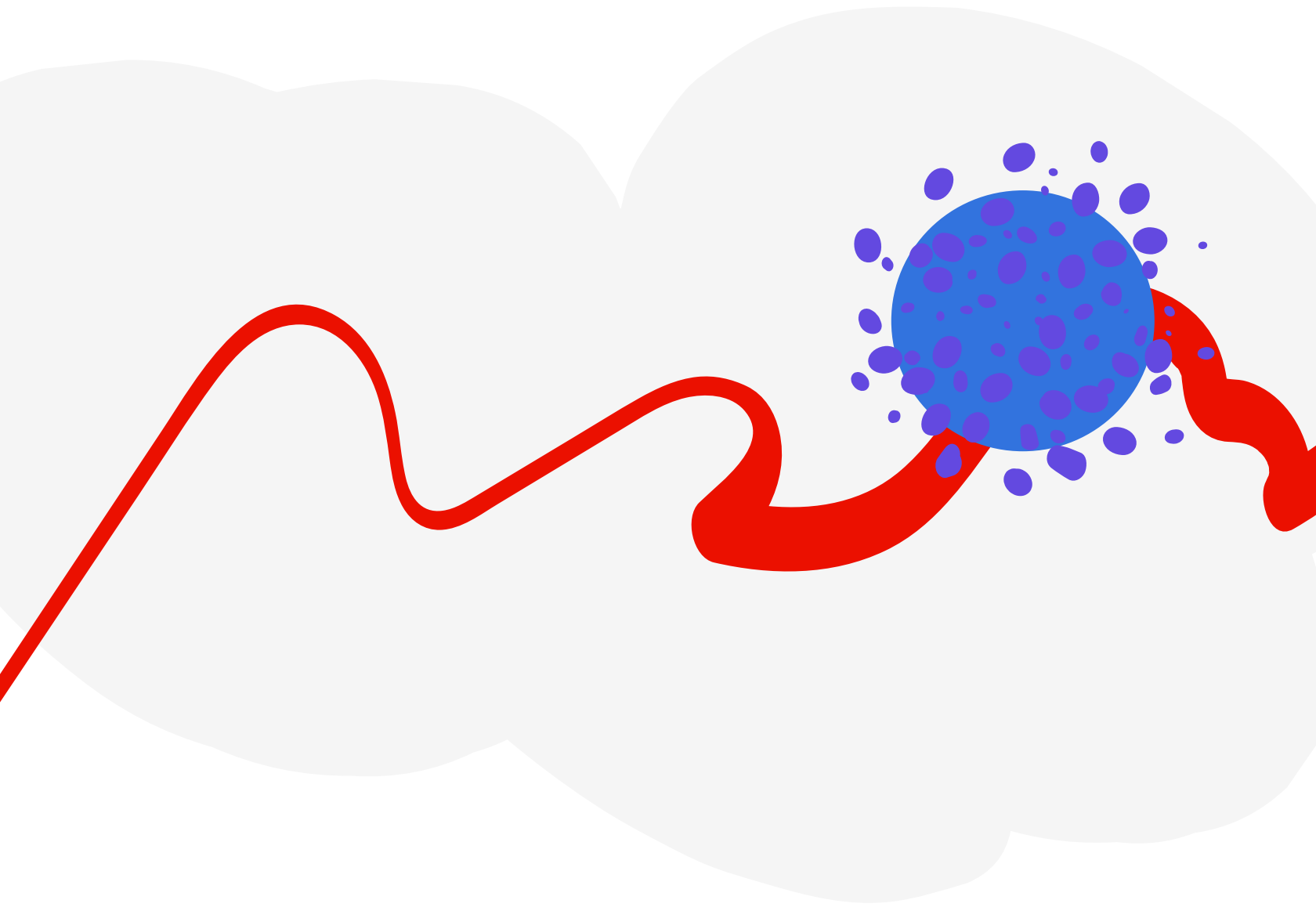


Table of Contents

Introduction 3

The Adobe Incident Response Program 3

Security Monitoring and Threat Intelligence 4

- Monitoring and Detection 4
- Threat Intelligence 4
- Forensics 4
- Automation 5

Vulnerability Handling and Incident Response 5

- The Adobe Incident Response Lifecycle 5

The Adobe Incident Response Organization 9

Conclusion 10

Introduction

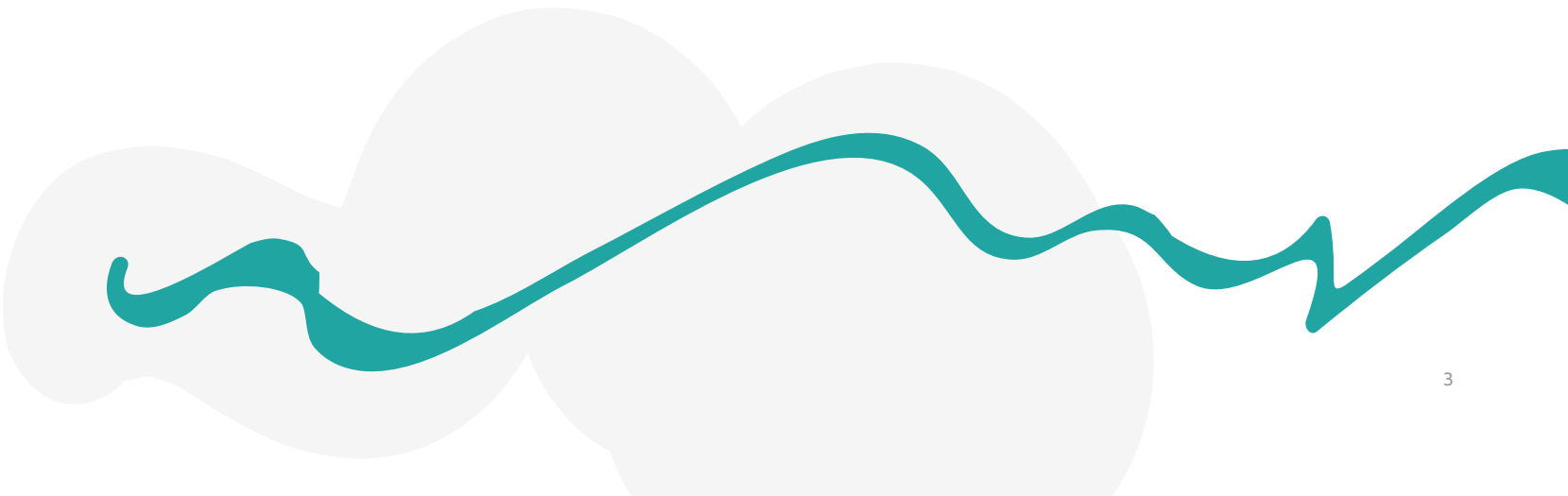
Trust. It's what Adobe works every day to gain from our customers. The security, privacy, and availability of our customers' data is important to us, which is why the Adobe Incident Response (IR) program includes both proactive security monitoring and threat intelligence as well as vulnerability handling 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 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 swift 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 and bad actors, nation-states and otherwise, 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 number of attack vectors. A solid, well-thought-out 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 strategy, outlined in this paper, plays an important role in maintaining compliance. Our program includes proactive security monitoring and threat intelligence, as well as vulnerability monitoring and handling and reactive incident response to 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 can 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 to detect potential issues as well as industry threat intelligence information. We leverage automation and 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 SIEM tools helps Adobe 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. Adobe employees continually tune the SIEM tools to filter out noise, eliminate false positives, and help ensure the proper prioritization of the most critical threats.

Threat Intelligence

New vulnerabilities and threats evolve each day and Adobe strives to quickly respond to mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT and SANS, Adobe also subscribes to multiple industry threat feeds and security alert lists issued by major security vendors, which provide threat intelligence information from industry peers as well as adjacent industries. We use industry standard tools and employee reviewers to filter through the intelligence we receive and to appropriately rank intelligence based upon 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 are designed with a goal of decreasing the time from detection to 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 to ensure deadlines are met, and generate dashboards with daily, weekly, and yearly trend analysis for all vulnerabilities to help ensure we are meeting 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 robust and proven incident response process.

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.

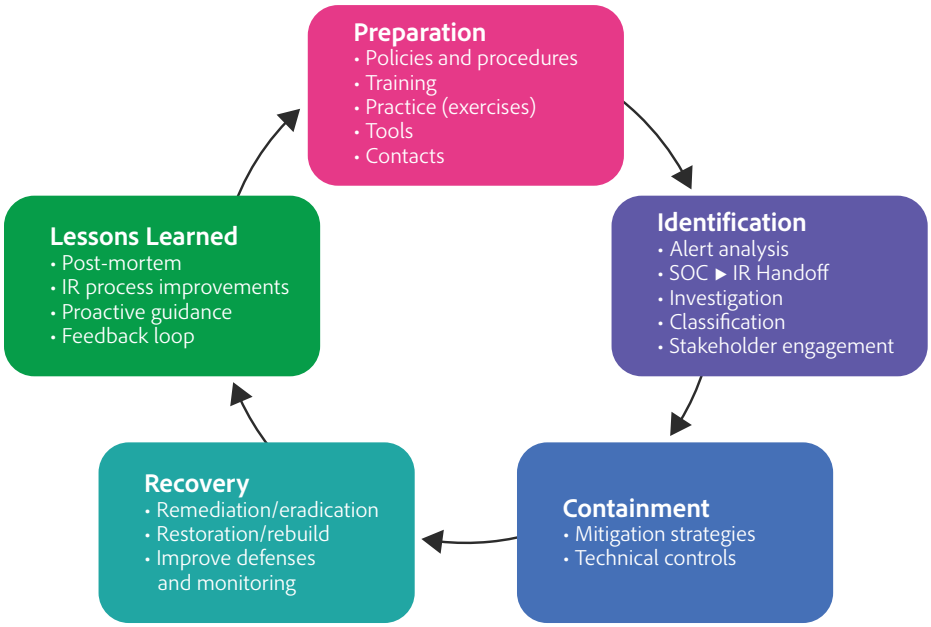


Figure 1: The Adobe Incident Response Lifecycle

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 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
- Alert and 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
- Tool kit inventory, improvements, and regular updates

Phase II: Identification

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 crowdsourced 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. Adobe has several defined triggers, including:

- 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, which 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 triggers, the incident response team takes over investigation and mitigation of the incident. Vetted security intelligence is shared with appropriate groups across Adobe to ensure that all employees benefit from the knowledge learned from incidents.

Phase III: Containment

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 Adobe 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, Adobe considers the following:

- How and from where was the threat launched?
- What assets or products 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 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 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 handler 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, the following areas and actions are considered:

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

Customer notification is also covered in this phase of the incident response lifecycle. For product-related vulnerabilities, Adobe follows the 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 in order to remediate the vulnerability. All other customer notifications are made by Adobe as necessary and appropriate pursuant to contractual, regulatory, and statutory requirements that are relevant and applicable in the context of the vulnerability or incident.

Phase V: Lessons Learned

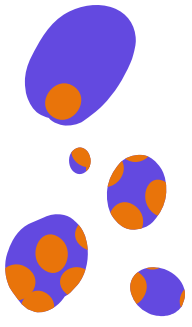
After an incident has been resolved, Adobe enters the final phase of the incident response lifecycle, which includes processes and feedback loops, including a retrospective. This analysis highlights what went right and what went wrong in the incident, how to better defend the organization, and where the organization should focus resources. We feed 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 our Security Coordination Center (SCC). Operating 24/7, the SCC 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 SCC, the Adobe Security Operations Center (SOC) handles general threats to Adobe cloud services, infrastructure, and proprietary corporate information monitoring and alerting, and includes the security monitoring, threat intelligence, and 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.

In addition, the Adobe Privacy Incident Response Team (PIRT) promptly engages in the process to drive the investigation and legal analysis of any privacy or other legal

considerations that may be relevant in the context of a vulnerability or incident. As part of this investigation and analysis, PIRT evaluates and determines whether notifications to customers, individuals, regulators, or any other third parties are legally necessary or appropriate.

All Adobe incident response teams work together and with other stakeholders within and outside the company to 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 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 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.