DocuSign®

Incident Response and Security Operations Programs

Protecting our company helps us protect our customers. By keeping threats out of the environments we use to run our business and deliver our solutions, we ensure that we can continue to provide secure services without being disrupted by security incidents.

DocuSign understands that the rapid evolution and proliferation of cyberthreats and bad actors calls for relentless focus and continuing innovation, using the latest tools and best practices to stop threats and respond to incidents. Proactive security monitoring and threat intelligence help us understand the external security landscape and detect threats within our own environment. Our comprehensive and holistic approach to incident response encompasses preparation, identification, containment, remediation, recovery and lessons learned.

In the following pages, we provide an overview of DocuSign incident response and security operations programs, from security monitoring and incident response to threat intelligence.

DocuSign security analysts complement real-time data from our own systems with threat intelligence from across the industry to detect, identify and analyze potential threats against our data and our ability to provide secure services to our customers.

Security monitoring center

The DocuSign security monitoring center works around the clock to detect threats and incidents in our environments.

- Industry-standard security information and event management (SIEM) solutions are deployed to consume and analyze data from sources across our network
- SIEM tools are continually tuned to filter out noise, eliminate false positives and ensure proper prioritization of the most critical threats
- All security events are automatically fed into a queue monitored by security analysts to make informed decisions about the appropriate response for each threat, from a low-risk commodity threat to an advanced, high-risk security threat
- Incidents can be quickly and seamlessly escalated to advanced members of the security operations center (SOC), and escalated in turn as needed to the incident response team
- Risk assessments are performed for all DocuSign sites on a regular risk-based schedule
- Physical security plans are updated following each risk assessment
- News events in proximity to DocuSign offices, data centers and employees around the world are monitored for potential impact

Threat intelligence

With new threats and tactics emerging daily, DocuSign prioritizes threat intelligence to act quickly on the latest cybersecurity findings.

- Subscriptions to industry-wide vulnerability announcement lists including US-CERT and SANS, as well as threat feeds and security alert lists from major security vendors, keep us informed of the latest threats, bad actors and tactics
- DocuSign security analysts use their own expertise to scour the internet, including open source intelligence (OSINT), for any current developments that might affect our company
- Dark web research includes monitoring the same underground forums used by attackers, using automated alerts of keyword searches for DocuSign, DocuSign employees, personally identifiable information (PII) sharing, and other indications of a potential breach
- All threat intelligence is fed continuously into the SOC to ensure broad awareness and vigilance

Security monitoring and threat intelligence

Advanced analysis

The DocuSign advanced analysis team uses deep expertise into the characteristics and behavior of malicious software to quickly diagnose and take action on detected threats.

– Any malware detected on our network is reverse engineered to discover its purpose and function

– Breadcrumbs are gathered to understand how and by whom the code was created, even to the level of identifying a specific threat actor

– Code analysis helps advanced analysts detect whether the malware exists anywhere else on the DocuSign network

Threat hunting

Our threat hunting team uses information from our threat intelligence, advanced analysis, incident response and security monitoring teams to go on the offensive against threats.

– The team proactively and continually inspects our network for any sign of a potential threat

– Breadcrumbs uncovered by our advanced threat analysis team are used to detect previously unknown threats

Threat detection

Threat detection at DocuSign combines automated capabilities with expert analysis to identify existing threats and refine our ability to detect future threats.

– Automated detection capabilities are tuned to deliver information and cases to our security monitoring center based on high-value, immediately actionable threats

– False positives are filtered so that security personnel can focus on real threats

– New threats are built based on breadcrumbs and indicators of compromise (IOC) detected by teams throughout the SOC

– Direction from the advanced analysis team and other SOC groups are used to create new detections based on known or found threats, helping us continually refine our threat detection capabilities

Forensics

If infected systems or suspected compromised systems are found, a full bit-by-bit analysis is conducted.

– The forensics team determines how the attacker got into our systems, what they attempted to do, and where they went next

– Forensic analysis can also include a complete image capture or memory dump of impacted machines while following standards for evidence safe-holding and chain of custody

Incident response

At the core of the security operations center for DocuSign is the incident response team. Logging and alerts help us detect potential threats and respond quickly. Our response follows a five-phase approach from preparation through identification, containment, remediation and recovery, and lessons learned.

Logging and alerts

Logs from every DocuSign system are used to detect and alert the security monitoring center in the SOC on anomalous or otherwise predefined behavior.

- When analysts confirm a legitimate threat, we take immediate action to remediate and mitigate it
- Automation tools and processes decrease the time from detection to remediation
- Industry-standard SOAR (security orchestration, automation and response) platforms optimize the handling of vulnerabilities, alerts and events at scale

Response phase 1: Preparation

DocuSign's response to security incidents begins with advanced planning and preparation to avoid potential issues and accelerate repair and recovery.

- Detailed security policies and procedures include methodologies for alert and incident response handling
- Call trees and notification processes for solution, product and support teams help us mobilize a company-wide response
- Regular skill development, improvement and training keep our security staff at peak expertise
- Incident response plan testing, team drills and tabletop exercises assure our preparedness
- Security tools are regularly inventoried, assessed and updated to meet current standards and best practices

Response phase 2: Identification

Security alerts on potential threats to DocuSign systems, data or processes can be triggered based on indicators such as suspected unauthorized access to PII or other confidential data, in-progress exploitation, security events affecting the broader technology industry, or findings by a DocuSign security team or external security vendor.

- Security events are assigned a severity level based on internal operational policies
- Data such as logs and forensic images is used to determine the root cause of the incident and the best course of action for mitigation
- If specific incident triggers are met, the incident response team initiates investigation and mitigation of the incident
- Relevant security intelligence is shared across DocuSign security teams and other groups

Response phase 3: Containment

DocuSign incident handlers and responders work quickly to limit any existing damage and prevent further damage. The strategy for containment is based on considerations including the following:

- How was the threat launched, and from where?
- What assets or products have been impacted? Has damage occurred?
- Is the scope of the incident limited to a single machine, or has there been lateral movement across the network?
- Can log data or memory forensics help us understand the nature of the threat?
- Do we know the attacker's motive and methodology?
- Can we use threat intelligence to monitor the threat in other areas of our network?
- How will our services be impacted once the incident has been contained?
- How can we measure and track our success in containing the threat?

Response phase 4: Remediation and recovery

Once a security incident has been contained, remediation and recovery efforts ensure that systems are free of malicious or illicit content and fully operational.

- Incident handlers work closely with stakeholders to set a timeline for remediation, eradication and recovery, including testing and validation
- Based on the nature of the incident, incident handlers determine appropriate actions for remediation and recovery such as patching and hardening system images, reimaging systems, implementing password changes, and improving monitoring and defenses
- Customer notification processes include issuing a detailed security bulletin as well as other measures dictated by relevant contractual, regulatory and statutory requirements

Response phase 5: Lessons Learned

The final phase of the incident response lifecycle analyzes all of the phases that have come before to understand what happened, what went right and what could be done differently in the future. This information helps security teams across DocuSign better protect our organization and our customers.

Cybersecurity good citizenship

Even in highly competitive industries, cybersecurity is a responsibility shared by all. The more organizations collaborate effectively to prevent attacks from succeeding, the better we can deny bad actors the rewards they seek. In this spirit, DocuSign belongs to numerous industry groups specifically designed for cybersecurity knowledge sharing. Our analysts and leadership alike utilize their own networks of industry colleagues to learn from others while sharing our own perspectives on what works and what doesn't. By hearing about the experiences of other companies, we find ways to improve our own efforts. By showcasing our own findings and best practices, we help other companies become more secure and better prepared. Together, DocuSign and our peers across the digital economy are dedicated to staying one step ahead of cybercrime.

Additional resources

The security we offer our customers extends beyond what's outlined in this document. A number of additional resources are available that further demonstrate DocuSign's industry-leading security strategy.

Follow the links below for more details on how we approach and deliver security.
Trust Center

Policies: Terms of Use Privacy Policy

Use of Cookies

DocuSign®

About DocuSign
DocuSign helps organizations connect and automate how they prepare, sign, act on and manage agreements. As part of the DocuSign Agreement Cloud, DocuSign offers eSignature, the world's #1 way to sign electronically on practically any device, from almost anywhere, at any time. Today, over a million customers and more than a billion users in over 180 countries use the DocuSign Agreement Cloud to accelerate the process of doing business and simplify people's lives.

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
sales@docusign.com
+1-877-720-2040