Mandiant

Solution Brief

Accelerated Vulnerability Readiness Program

Benefits

- Accelerate secure code reviews using AI-powered tools to discover complex zero-day vulnerabilities before they impact business operations.
- Strengthen and scale vulnerability management capabilities through expert program design and optimization to handle machine-speed threats.
- Improve incident response preparedness and decision-making for executives and technical leaders during compressed attack timelines.
- Identify and prioritize strategic, design, and architectural risks across mission-critical applications to prevent scalable exploitation.
- Secure the software development lifecycle by resolving platform misconfigurations and securing CI/CD pipelines against emerging supply chain risks.

Overview

As adversaries leverage AI to accelerate vulnerability discovery and exploit development, legacy manual triage can no longer keep pace. Organizations relying on traditional assessment and patching approaches to absorb this surge of AI-enabled threats risk severe operational overload. To maintain resilience, organizations must strengthen and scale their vulnerability management capabilities through expert program design and optimization. The Mandiant Accelerated Vulnerability Readiness Program addresses this challenge by enhancing security across your software development lifecycle, deployment pipelines, hybrid IT infrastructure, third party platforms, and processes.

Our methodology evaluates cyber defense programs across foundational functions, aligning policies and assessing efficacy while integrating threat intelligence, business context, and AI-powered risk analysis for strategic prioritization. This comprehensive engagement delivers a customized remediation roadmap, expert program design, and a tailored Zero Day Response Playbook to ensure long-term security resilience to address AI-driven exploits and modern software supply-chain attack paths.

Program Areas

Mandiant organizes vulnerability readiness into six program areas

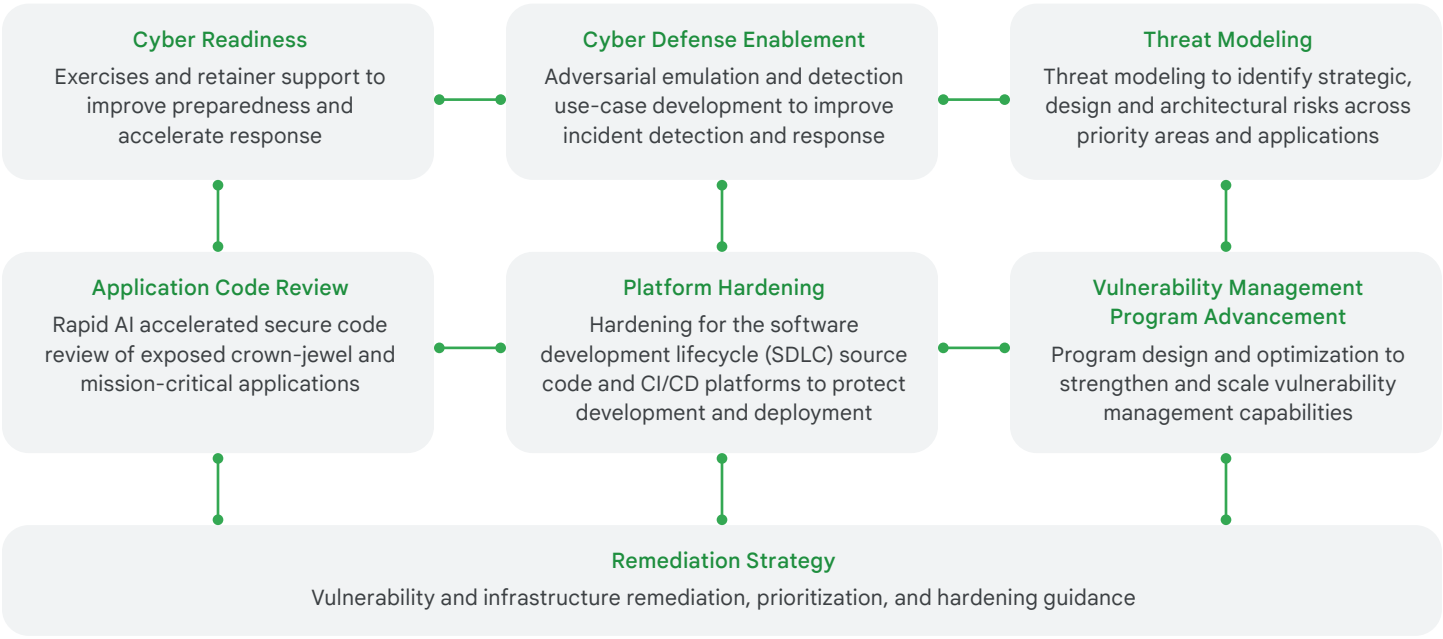

Figure 1. The Mandiant approach to vulnerability readiness.

Cyber Readiness

Improve preparedness and accelerate response with Cyber Readiness, validating your organization's ability to defend against highly compressed, machine-speed cyber incidents. By utilizing up to two tabletop exercises focused on strategic and technical readiness against accelerated attack timelines, the program prepares executives, boards, and C-suite leaders for effective decision-making and delivers a strategic recommendations report outlining program-level improvements to strengthen the people, processes, and governance required for effective cyber incident response and reduced SOC toil.

Remediation Strategy

Unify vulnerability and threat data to create a cohesive, prioritized, and actionable path for addressing immediate risks. Mandiant will evaluate risk severity, exploitability, and business impact to logically sequence efforts, ensuring technical fixes align with strategic business goals. You will receive an integrated Remediation Strategy Document and an actionable Execution Roadmap, which outlines phased remediation tasks across code, infrastructure, and defensive posture.

Cyber Defense Enablement

Organizations can significantly strengthen their entire defense-in-depth and proactive blocking capabilities through the Cyber Defense area, which utilizes threat intelligence-driven attack emulations to uncover real-world attack paths to crown jewels. By collaborating directly with Mandiant Operators and Incident Responders to test defenses against live threat actor scenarios, organizations gain increased detection visibility, and actionable strategic recommendations to operationalize automated defensive capabilities for long-term security enhancements.

Threat Modeling

Through Threat Modeling, organizations can gain the ability to systematically identify and prioritize vulnerabilities and strategic, design and architectural risks across mission-critical applications, hybrid IT infrastructure, and third-party dependencies to prevent scalable exploitation. This is achieved by implementing threat modeling directly into your developer workflows to evaluate application components and their connections from a threat actor's perspective to understand the full attack surface. The methodology involves interactive discovery workshops to review architecture and business logic, decomposing components, and applying STRIDE analysis to identify design flaws. This process concludes with the evaluation of attack paths, specifically focusing on 'attack chains' where minor, isolated vulnerabilities can be rapidly linked for successful exploitation. A final report is delivered containing finalized threat modeling diagrams, visualized attack paths, a detailed breakdown of identified threats, and actionable, prioritized strategic mitigations for improving application design and architecture.

Application Code Review

By engaging in an Application Code Review, organizations can gain the capability for rapid, AI-accelerated secure code review of exposed crown-jewel and mission-critical applications, enabling the discovery of complex, zero-day vulnerabilities in your source code. This exercise utilizes custom, agentic tools to autonomously scan codebases and automate codebase fingerprinting and vulnerability hypothesis generation. Specialized agents perform in-depth analysis and provide findings, which Mandiant testers then manually validate to demonstrate exploitability, and help prioritize based on the established threat modeling profile . The deliverables include technical details of the vulnerabilities discovered, a written report featuring risk ratings, context, and actionable recommendations, and a prioritized remediation roadmap for improving your Secure Software Development Lifecycle (SDLC).

Platform Hardening

By proactively identifying and resolving platform misconfigurations before they can be exploited, organizations can secure their entire software development lifecycle across source code and CI/CD environments. This comprehensive evaluation includes verifying MFA enforcement, validating branch security, secrets scanning and rotation, and analyzing pipeline-as-code files for script injection risks and third-party dependencies. Mandiant provides a prioritized remediation roadmap, detection improvement recommendations, and a detailed risk report to ensure robust protection for software supply-chain attack paths that target development and deployment processes.

Vulnerability Management Program Enhancement

By strengthening and scaling vulnerability management capabilities through expert program design and optimization, organizations can identify critical capability gaps and optimize their program architecture to handle the anticipated AI-enabled surge in vulnerability discovery. By automating workflows and developing centralized metrics for continuous measurement, Mandiant delivers a customized, actionable roadmap to elevate your program, providing strategic recommendations with hands-on assistance to replace human-speed patching protocols with a modern, automated defensive operating model and a tailored Zero Day Response Playbook.

The threat landscape is shifting as adversaries continue to operationalize AI to compress exploitation timelines.

Don't wait for the next breach to uncover your gaps. Partner with Mandiant to implement the Accelerated Vulnerability Readiness Program, modernizing your defensive architecture and securing your applications, infrastructure, and people against machine-speed threats. Contact a Mandiant expert now to schedule a consultation on your vulnerability readiness.