Mandiant

Datasheet

High Value Asset (HVA) Protection Program

Benefits

- **Unified 360 degree cyber-physical defense:** Securing the executive's total environment through a bespoke approach that bridges the gap between digital and physical security
- **Intelligence-led preemption:** Neutralizing risks before they manifest by using proactive, person-specific intelligence to identify and disrupt the threat vectors most relevant to the individual
- **Frictionless security:** Delivering elite security that scales to the individual's specific comfort level, ensuring uncompromising protection while strictly adhering to personal privacy requirements

Why Mandiant?

- **For over two decades**, Mandiant has served as a trusted advisor to thousands of organizations. We combine our frontline expertise and deep understanding of global attacker behavior to help organizations prepare and defend their cyber defenses against compromise
- **Organizations worldwide** use our services to improve their security posture, gain a deeper understanding of threat activity, and assess their defenses against real threats

Cyber defense expertise designed to protect executives at home, work, online and on global travel

As the boundary between digital and physical threats disappears, siloed defenses are no longer sufficient. This service delivers a unique approach to high value asset (HVA) protection. An HVA represents the human attack surface: the leaders whose influence and access make them primary targets for multi-vector threats. Mandiant protects not just the individual, but the personnel and reputation that surround them.

Drawing on Mandiant's world-class frontline intelligence and incident response expertise, we provide custom insights and proactive guidance to help reduce the probability of an attack and to provide a highly effective response to executive threats.

Overview

A high-value asset (HVA) includes the most visible highest ranking executive personnel at an organization as well as their direct supporting personnel, that can be uniquely targeted by attackers due to an HVA's influence, reputation, and level of access.

Mandiant's proactive approach to executive security enables the rapid identification and effective response to emerging threats against HVAs. We integrate cybersecurity into the existing security programs, demonstrating the nexus between the two programs as it pertains to protecting an HVA.

Our world-class Mandiant cybersecurity experts collaborate with your team to embed specific capabilities such as cybersecurity best practices, custom threat intelligence and offensive testing within your organization's executive protection suite to better protect HVAs from threats.

Our methodology

As threats against HVAs escalate, organizations must evolve their security posture to protect key personnel with the same rigor as core information and physical infrastructure. True resilience requires a unified defense across the four critical domains of an executive's life: the **office**, the **home**, during **travel**, and **online**. By closing the security gaps between these environments with a holistic/unified approach, organizations neutralize the multi-vector threats that specifically target their most vital leadership assets.

Seamless integration

In this custom program, Mandiant specialists can seamlessly integrate with existing protective details to help identify and prioritize the individuals most at risk. We don't just observe; we operationalize threat intelligence. Our Analysts pinpoint the specific risk profiles relevant to each executive and their household to ensure a highly personalized layer of protection. From executing offensive security drills at private residences to hardening the communication networks of private aviation assets, we bridge the gap between traditional bodyguards and cybersecurity disruption.

A dedicated HVA advisor

Our personalized programs are designed to balance **uncompromising security** with the **stringent privacy requirements** of Tier 1 HVAs. We understand that the higher the profile, the more sensitive the personal boundaries. Mandiant deploys a **dedicated HVA advisor** to navigate these complexities, ensuring that even the most restrictive environments are hardened against sophisticated attacks without disrupting the executive's operational or personal life.

Integrated security information flow



Protective Security

We empower protective details with world-class threat intelligence, enabling a comprehensive threat profile and proactive stance against complex, multi-vector threats targeting high-profile individuals.

Cyber Security

Mandiant modernizes executive safety by positioning cyber defense as a primary pillar of the protection program, rather than an afterthought. Ensuring digital vulnerabilities are defended with the same rigor as kinetic ones.

Physical Security

We bridge the gap for physical security teams by securing the "digital-physical" overlap—identifying and addressing security vulnerabilities within home networks and smart technologies to ensure they do not become entry points for physical threats.

Tiered model for defining and managing HVAs



1 HVA Tier 1: Executive personnel with decision making authority and high public visibility, such as **CEO** and **C-Suite**.

2 HVA Tier 2: Supporting personnel that have a high level of access to Tier 1 HVAs, such as **executive assistants, advisors,** or **family members.**

Examples of HVA program deliverables

	Strategic Services	Offensive Security Services (OSS)	Threat Intelligence
Home	**Residential Security Blueprint:** A bespoke architecture balancing privacy controls with seamless usability for the HVA and family.	**Residential Attack Simulation:** Active validation of network, IoT, and physical perimeter controls with specific hardening protocols for all home devices.	**Residential Security Footprint Analysis:** Advanced OSINT analysis of the residence to identify physical/ digital vulnerabilities and execute the removal of exposed data.
Office	**Corporate Perimeter Optimization:** Strategic review and enhancement of existing workplace protection to ensure seamless executive safety within the firm and offices.	**Penetration Testing (Integrated Control Validation):** Stress-testing of the office's cyber-physical defenses to verify the effectiveness of current executive security measures.	**Corporate-Executive Nexus Profile:** Detailed analysis of how the executive's personal threat profile impacts corporate risk and brand integrity.
Online	**Digital Security Roadmap and Training:** Tailored, high-touch guidance for securing the HVA's digital life, including social media, private comms, and dark web exposure.	**Digital Identity Exploitation Analysis:** Simulating adversary techniques to target the executive's digital identity, followed by hardening of online accounts.	**Digital Monitoring:** Persistent dark web and OSINT surveillance to identify and neutralize leaked personal info and emerging digital threats.
Travel	**End to end travel security:** Dynamic security requirements and geo-specific protocols tailored to the HVA's global travel footprint.	**Aviation/Vehicle security Testing:** Vulnerability testing of private aviation, maritime, and vehicular networks to secure onboard control systems and comms.	**Itinerary Threat Intelligence:** Intelligence overlays and adversary simulations to identify and mitigate risks along specific travel corridors.

Contact us today to discuss how we can help you achieve your program goals.

Google Cloud

For more information visit
cloud.google.com