The Defender's Advantage

Solutions Guide: Financial

Mandiant

Google Cloud Security

The Defender's Advantage, developed by Mandiant, part of Google Cloud, emphasizes a proactive and intelligence-driven approach to cybersecurity. Google Cloud's comprehensive suite of security products and consulting aligns seamlessly with this methodology, enabling organizations to gain a decisive advantage over adversaries. This document outlines how Google Cloud Security can help you achieve your defender's advantage.

The latest M-Trends report shows that in 2023 the number one industry targeted for cyber instructions was financial services. These businesses have access to various sensitive information, including proprietary business information, personally identifiable information (PII), and obviously financial data. Attackers can gain access through direct assault or can abuse service providers and technology organizations to facilitate third-party compromises. The top malware targeting the financial sector was Beacon, a backdoor written in C/C++ that is part of the Cobalt Strike framework.

Mandiant/Google organizes the Cyber Defense domain in six critical functions to achieve the mission of allowing financial services organizations to continue to operate in the face of threats. The functions of the Cyber Defense domain are Intelligence, Detect, Respond, Validate, Hunt, and Mission Control. These functions work together to provide a common front against attackers.

Intelligence provides a guiding light

Intelligence is a cornerstone of a strong Cyber Defense program. It provides the forward knowledge of threat actors, their tactics, techniques, and procedures. Through collecting, analyzing and disseminating threat actors' indicators of compromise, the other Cyber Defense functions operate from a position of knowledge. This allows prioritization of actions across the entire Cyber Defense program.

Financial clients often come to Mandiant/Google with the need to improve the quality of their threat intelligence. There are many providers touting the quality of their intelligence, but Google can provide customized threat intelligence tailored to financial sector threats and identified advanced persistent threats (APTs). We also provide detailed threat profiles and allow companies with more mature resources adopt a proactive cybersecurity posture.

Google Threat Intelligence combines the depth of Mandiant frontline intelligence, the global reach of VirusTotal crowdsourced intelligence, and the breadth of Google's unmatched visibility into attacks targeting billions of users to provide an industry-leading view into the threats that matter. Cybersecurity and threat intelligence experts can help organizations optimize their use of threat intelligence by developing a threat intelligence function, understanding the threats that matter most to their organizations, and/or utilizing resources to help operationalize the intelligence into Cyber Defense programs.

Detecting and investigating malicious activity

Many of the traditional elements seen in security operations, or security operations centers (SOCs), are performed in the **Detect** function. This function also includes enhancing contextualization, providing detection analytics, increasing visibility to give an organization a clearer picture of threats to the environment, and a more comprehensive view of the environment itself.

Frequently clients ask Mandiant/Google to review existing detection frameworks and perform a gap analysis based on specific financial services threats. We help client prioritize the most critical vulnerabilities, and in some cases perform a documentation of their threat logic, for both end point detection (EDR) and their security information and event management (SIEM).

Google Security Operations analyzes the wealth of security telemetry in real-time to surface potentially malicious activity. The rich investigative views help analysts get to the root cause by automatically surfacing and prioritizing findings including rich context about threat actors and campaigns from applied threat intelligence.

AI-generated summaries of what's happening in cases, along with recommendations on how to respond, allow analysts to investigate more efficiently. Additionally, AI can be used to run searches, create detection rules, and analysts can use AI to access the latest threat intelligence from Mandiant directly in-line—including any indicators of compromise found in their environment—and navigate to the most relevant pages in the integrated platform for deeper investigation.

Google Cloud Security also offers managed threat detection, investigation, and response services through Mandiant Managed Defense to provide 24x7 security operations coverage from Mandiant's team of seasoned defenders, analysts, and threat hunters.

Responding to compromise

The **Respond** function focuses on capabilities such as investigation and containment, and includes automation and orchestration, which drives faster remediation of incidents to minimize impact. This function is dedicated to minimizing the impact of any compromise, ensuring rapid recovery to normal operations, and relaying information to the other functions to increase resiliency across the program.

Mandiant responds to the largest and most impactful breaches around the world. Setting up a Mandiant Retainer to put incident response experts on speed dial is a great way to make sure that if your organization faces a breach, Mandiant experts can begin triage within two hours of you notifying them of an incident. The retainer also provides flexible access to proactive services to mitigate risk, identify gaps in cyber defense capabilities, and ready your organization for a breach.

We support clients well after the initial incursion with a detailed post mortem methodology. Mandiant provides recommendations on staffing and additional resources to improve a client's security posture, defining and implementing improvements that can turn an under resourced SOC into an effective cyber defense center.

Google Cloud Security offers a centralized platform for managing security incidents. It provides security specific case management that allows security operations center (SOC) teams to manage, assign, and track the progress of investigations, as well as collaborate on response efforts. The platform can also help speed up and drive consistency in response processes with flexible playbooks that automate repetitive tasks and orchestrate the tools required to contain and remediate threats.

Targeted testing and validation of controls and operations

The continuous management of threat exposures within an organization is the purpose of the **Validate** function. In addition to providing assurance that the security control ecosystem is operating as designed throughout changes to the environment, the Validate function also manages the program's readiness to respond, uncovers vulnerabilities in the environment, and the capabilities of its resources.

Recently a financial services client needed support in validating their EDR detections. Mandiant was asked to build this content with the validation platform so that all EDR detections with their SIEM were being detected correctly and consistently.

Mandiant's Validation Services team associated the content with over 50 high-profile detections relating to high-frequency, high-impact tactics, techniques and procedures (TTPs). This was then imported into the client's environment for execution and testing.

Mandiant Attack Surface Management offers the adversary's view of your organization's attack surface by collecting asset and exposure information like an attacker would. This understanding of your attack surface and potential entry points that malicious actors could exploit can provide a starting point for validation activities.

Validation of existing controls and operations can be achieved with Red Teaming performed by Mandiant experts. These experts will use real-world attacks to see if attacks are caught by existing controls and assess how security analysts handle the alerts generated. Penetration testing also provides targeted validation of controls protecting crown jewels including web application reviews and cloud architecture assessments.

To simulate attempts to reach and compromise cloud resources, Security Command Center provides continuous virtual red teaming. Millions of attack permutations run against a digital twin model of your cloud environment to predict where an external attacker could strike, identify cloud resources that could be exposed, and determine the possible blast radius of an attack.

Mandiant Academy provides instructor-led and on-demand training to enhance the cyber defense team's knowledge in the areas of intelligence, incident response, malware analysis, and more. For hands-on experiential learning, the ThreatSpace Cyber Range allows security analysts to practice responding to attack scenarios in a safe and controlled environment.

Hunting for active threats

The **Hunt** function expands the detection capabilities of the Cyber Defense program by becoming proactive as it examines the environment for active compromises. It helps to ensure defense controls are operating as designed and provides defenders with the opportunity to identify weaknesses in their controls or undesired activity. Hunt activities provide a very practical complement to the Validate function.

Financial services firms often wish to begin threat hunting as part of adopting a more proactive cybersecurity posture. Mandiant helps to build a foundation and get them started. For example, we recently worked with a client to build out the tooling and hunting notebooks necessary to perform threat hunting at scale. These notebooks consisted of:

- Malicious Powershell usage
- QakBot
- IOC-drive hunt
- Lateral movement

Mandiant Hunt delivers expert-led continual threat hunting, leveraging your Google Security Operations and Security Command Center data to expose attacker activity missed by other security telemetry.

A Mandiant Custom Threat Hunt complements continuous Mandiant Hunt as a point-in-time threat hunt to help organizations uncover ongoing or past threat actor activity in their environment while improving their ability to effectively detect future threats. Some common drivers for a Mandiant expert-led targeted threat hunt include an increased targeting by specific threat actors in your industry or vertical; implementation of new technologies, cloud platforms, or SaaS solutions; business partners or supply chain impacted by an incident or breach; and planned or recent mergers and acquisitions.

Coordinating Cyber Defenses through Mission Control

The **Mission Control** function provides the connective tissue that holds the other Cyber Defense functions together and drives coordination and unified management across the program. It also ensures that the functions are connected to the organization's business goals and values. This function is focused on Cyber Defense program management and establishes formal processes for resources management, communications, metrics, and crisis management. Additionally, Mission Control ensures coordination with non-cybersecurity teams across an organization. This program management ensures that the Cyber Defense capabilities remain resilient and aligned to changes within an organization and threat landscape.

For a recent financial services client we supplied a full-time SOC advisor to fill a critical senior role. This advisor conducted a review to determine how to raise the client's procedures and practices up to industry standards. As part of the program the advisor mentored more junior SOC staff and worked with detection engineers to improve the client's logging, alerting and security, orchestration, and response (SOAR).

Google Cloud Security can help develop and enhance your cyber defenses, including processes and procedures utilizing Google Security Operations as well as non-Google technologies. The first step is often to evaluate the maturity of your security program across the four core domains: security governance, architecture, Cyber Defense, and risk management.

If your Cyber Defenses are established, Mandiant experts offer technical and executive tabletop exercises to evaluate how personnel and partners will interact when responding to various breach scenarios, and identify gaps in incident response plans. These scenarios can include crisis communications as well to inform, engage, and safeguard stakeholders during a cyber incident.

Get started

Google Cloud's security offers a full portfolio of products and services to help financial institutions gain a decisive advantage over adversaries. By leveraging these tools and services, organizations can gain deep visibility into their environment, build proactive defenses, and respond effectively to security incidents, ultimately achieving a position of strength in the ongoing battle against cyber threats.

Learn more about The Defender's Advantage at
https://cloud.google.com/security/resources/defenders-advantage