MANDIANT

EBOOK

STRENGTHEN YOUR SECURITY TEAM

Add five critical capabilities at will

There are an estimated 3.5 million unfilled cyber security positions forecasted for 2021 and research suggests it's only getting worse.[1]

Introduction

Organizations of all sizes, shapes and industries across the globe are experiencing a chronic shortage of cyber security expertise. According to ESG research, 46% of organizations say they have a "problematic shortage" of cyber security talent at present.[2]

The result? While in-house security personnel keep up with alert volume and the latest threats, they must also juggle many other jobs without the opportunity to become experts in any given role. Many types of security expertise are simply difficult to maintain in-house. For example, it is expensive for organizations to hire, retain and support teams of intelligence and malware analysts and even more challenging to scale such teams.

This means many organizations are left to defend their networks and data without access to the cyber security expertise they need, ultimately leaving them more vulnerable to attack. Attackers, on the other hand, are growing increasingly skilled and resourceful, constantly adapting and innovating their tactics, techniques and procedures (TTPs) to avoid detection.

Mandiant Expertise On Demand is a new approach that provides flexible access to the breadth of specialized talent your security teams need to better secure your organization.

This ebook highlights which areas of expertise are often the hardest to find or build, outlines these kinds of skillsets and experience are critical to cyber security strategy and operations, and explains how Expertise On Demand can help supplement your organization's efforts to hunt for, prevent and respond to threats.

1 Cybersecurity Ventures (May 31, 2017). Cybersecurity Jobs Report 2018-2021.
2 Enterprise Strategy Group (February 2016). Cybersecurity Skills Shortage: A State of Emergency.

CAPABILITY #1

Threat Hunting

Summary

Threat hunting involves continuously and proactively looking for signs of compromise by combining a knowledge of the threat landscape, attackers, TTPs and indicators of compromise and quickly search through large amounts of data from those different sources.

Necessary tools and processes

- Network capture analysis
- Malware reversing
- Forensic artifact analysis
- Threat intelligence and analytics
- Sandbox environments
- External malware repositories
- Endpoint security analysis

Roles involved

- Incident responders
- Intelligence analysts
- Malware reverse engineers
- Technical research team
- Professionals and colleagues in the broader cyber security community

Desired outcome

Find intrusions (activity by new threats or known threats) in the fastest, most efficient way. In most cases, the time from detection to response is mere hours, drastically minimizing the scope, impact and cost of a breach.

How Expertise On Demand can help

Expertise On Demand can help security operations center (SOC) teams reduce the time and effort spent searching for new threats. Mandiant hunt analysts continuously discover patterns and trends across the entire Mandiant customer base, allowing greater visibility and ability to comprehend events difficult to understand in isolation.

The Ask An Analyst feature allows teams to request help analyzing threats and data, and applying knowledge about threat actor behavior to track attackers down fast. Threat hunting analysts can get access to the latest intelligence and analyst-driven techniques that can help detect intrusions early, investigate rapidly and access the in-depth behavioral insight needed for effective response.

CAPABILITY #2

Intelligence Analysis

Summary

Intelligence analysis considers threats and world events—including actions by nation states, strategic and military planning, cyber criminals and terrorists' movements—to provide warning of cyber attacks and weaknesses. In addition, intelligence analysis helps determine attribution for attacks, and the significance and sophistication of actors. This information is then correlated across other data sources and incorporated into intelligence assets and reporting.

Necessary tools and processes

- Network data
- Predictive analysis tools
- Databases on adversary best practices
- Native language research into adversary plans, doctrine, budgets and strategy

Roles involved

- Language-capable analysts
- Former intelligence or law enforcement experts
- Academics and economists
- Think tanks
- Political experts

Desired outcome

Improve the organization's ability to plan for and warn of upcoming known and unknown threats. Prepare defenses in advance and proactively manage risk.

How Expertise On Demand can help

Expertise On Demand can help intelligence teams on both short-and long-term analysis tasks and projects. From help translating foreign language content, to better understanding the tactics, techniques and procedures of known actors who may be targeting the organization.

The Ask An Analyst feature helps threat intelligence teams conduct proactive research with access to Mandiant experience regarding threats, adversary motivations and the ways in which cyber operations fit into a specific country's foreign policy. Expertise on Demand also makes the entire Mandiant Threat Intelligence portfolio available to clients, including finished intelligence pieces that highlight the cyber implications of world events, government announcements, terrorist or military actions and criminal activity.

CAPABILITY #3

Malware Reverse Engineering

Summary

Malware reverse engineering involves analyzing critical malware (such as viruses, backdoors and ransomware) identified by intelligence analysts, incident responders or technology. The work includes dissecting the malware, fighting through the attacker's anti-analysis code and figuring out everything the malware does from start to finish. Responders and analysts usually receive a detailed post-research report summarizing malware capabilities, persistence methods and network communication processes. This allows organizations to recognize, remediate and remove malware threats permanently.

Necessary tools and processes

- Malware analysis tools (custom, commercial and open source)
- Disassemblers and debuggers
- Forensic analysis platforms

Roles involved

- Intelligence analysts
- Incident responders
- Threat hunting analyst

Desired outcome

Identify behavior of malware to accelerate an incident response. Detect and prevent future attacks and impact future prevention strategies.

How Expertise On Demand can help

Expertise On Demand offers subscribers access to Mandiant intelligence and incident response experience that supports a much broader set of malware. Our malware analysts can quickly automate and correlate elements they've seen throughout the Mandiant customer base and in their extensive experience responding to incidents.

For those conducting reverse engineering, the clock starts when malware is found. Expertise On Demand can help these teams save time when time counts. The Ask An Analyst feature provides a lifeline for engineering teams, allowing them to request information on existing malware or have files scanned and analyzed.

CAPABILITY #4

Attack Simulation

Summary

Attack simulation involves conducting tests that closely resemble an attack, with objectives similar to real-world attackers, such as stealing or destroying sensitive data. It uses experience from the frontlines of cyber attacks and threat intelligence to simulate the tactics, techniques and procedures of real-world attackers that target your environment. This activity simulates and finds vulnerabilities by exploiting issues, escalating privileges and moving within the IT environment. Attack simulations, often called penetration testing, test the strength of security programs, including how well staff, processes and technology protect critical assets.

Necessary tools and processes

Open source, commercial and custom-developed tools (used to discover systems, obtain access, persist, escalate, move laterally and hunt users of interest, such as power admin users)

Roles involved

- Intelligence analysts
- Incident responders
- Industrial control systems (ICS) team
- Malware reverse engineers

Desired outcome

Enhance your ability to prevent, detect and respond to real-world incidents based on extensive experience with real-world breach attempts.

How Expertise On Demand can help

Mandiant experts know more about attackers than anyone, allowing us to test your security infrastructure based on the latest attacks, and inform you about opportunities to improve your organization's security posture. Expertise On Demand offers a wide range of resources and services to help security teams assess their capabilities, including threat intelligence and a wide range of Mandiant incident response and security assessment consulting services.

The Ask An Analyst feature can serve as an asset to security teams in any security situation, including simulations. Mandiant experts are engaged in the most consequential breach responses, so we know exactly how attackers operate during the most sophisticated attacks. We can also provide guidance on methodologies, tools and trends to help you stay ahead of attackers, simulated or otherwise.

CAPABILITY #5

Incident Response

Summary

Incident response (IR) refers broadly to handling security incidents, resolving specific or niche issues and putting solutions in place to address systemic causes of incidents. IR activities include performing host-, network- and log-based analyses, and triaging malware to support intrusion investigations.

The goal of Incident response is to quickly scope a compromise, identify what data was lost, catalog the tactics, techniques and procedures (TTPs) involved, plan and execute countermeasures and bolster the system's resilience to future attacks. To accomplish this, IR teams assess the situation, verify response objectives, collect evidence, perform analysis, provide management direction, develop remediation plans and potentially deliver an investigative report.

Necessary tools and processes

- Commercial and open-source forensic, malware and network analysis tools
- Log and structured data analysis frameworks
- Parsers, decoders and scripts to automate tasks
- Commercial and open-source intelligence platforms
- Office and productivity software
- Proprietary incident management tools

Roles involved

- Malware reverse engineers
- Application owners or administrators
- IT operations personnel
- Network engineers
- Intelligence analysts
- Internal and external legal counsel

Desired outcome

Minimize the impact of an incident and better prepare the organization to prevent, detect and respond to future intrusions.

How Expertise On Demand can help

Our large, highly trained team of elite incident responders can call upon more than a dozen years of victim intelligence and extensive knowledge of forensics and mitigation gleaned from across a broad ecosystem of experiences and evidence.

Expertise On Demand makes turnkey incident response capabilities available to subscribers through the Mandiant Incident Response Retainer. In addition, the Ask An Analyst feature, along with industry-leading threat intelligence, can bolster any response engagement and give your team the information and support needed to turn a worst-case scenario into a defeat for attackers.

Get Expertise On Demand to Build Security Capability

Many specialized cyber security capabilities—from threat hunting to intelligence analysis to incident response—are required to adequately protect an organization. Interplay among these disciplines is critical: the entirety of your security operation needs to work together to identify, analyze, contain and remediate threats and incidents, and ensure the organization is better prepared for the next event.

However, it isn't always possible to have top-shelf capabilities across the board. If you can even find the right talent (amid the worldwide talent shortage), it's expensive to bring these kinds of people, processes and technologies on board, not to mention retain and maintain them. And an in-house security team will often have to juggle competing priorities, rather than specialize in a single area. Finally, your in-house teams only have exposure to the incidents that face your organization, limiting the depth and breadth of their expertise.

Mandiant experts live, breathe and think about security all day, every day. Our security professionals have expansive and detailed cyber security knowledge and experience that can only come from exposure to thousands of the latest events, incidents, tactics and attackers. This experience is enhanced by machine-, victim- and adversary-based intelligence, so we can detect threats sooner, respond faster and secure your critical systems and data.

Whether your security team is a single person or a large operation, Expertise On Demand can fulfill, develop and supplement its capabilities to help you provide the world-class security your organization deserves.

Learn more at **www.mandiant.com/expertise**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT