EXPERTISE ON DEMAND
How to enhance your security team
There is a chronic shortage of qualified candidates. According to ESG research, 46% of organizations say they have a “problematic shortage” of cyber security talent at present. Even if you are able to recruit in-house staff, they probably won’t get to focus on all aspects of security all day, every day — because you’ll also need them to wear multiple hats (for example, threat monitoring, intelligence gathering, incident response or even managing IT or business operations). The result? In-house security personnel tend to be stretched thin, juggling many jobs, without the opportunity to become experts in any given role. Many types of security roles are just hard to maintain in house. Supporting a deeply embedded team of intelligence and malware analysts is expensive for any organization and scaling such a team is even more challenging. Without scale, however, it is difficult to achieve the macro visibility across industries, regions and different attacker techniques that allows analysts to connect the dots between observed activities.

So, if your organization is like most others, you’re left trying to defend your networks without access to the cyber security talent you need—leaving you ultimately vulnerable to attack. But while companies struggle to find the right talent, the bad actors remain busy. Attackers are increasingly skilled and funded, constantly morphing their tactics, techniques and procedures (TTPs) to avoid detection. Your team must be sufficiently skilled and landscape-aware to support a robust security strategy.

You may decide to engage with a company that provides an entire security program tailored to your industry and business needs. Expertise On Demand provides the ultimate flexibility to access the breadth of specialized talent you need to secure your organization.

In the following pages, you’ll learn about some of the expert roles that are often the hardest to find or are only required in specific situations. This paper details these roles, their responsibilities and the cross-functional processes that are required to successfully hunt for, respond to and prevent threats as part of a world-class security organization.

---

Threat Hunting Analyst

Responsibilities
The threat hunting analyst continuously and proactively looks for signs of compromise by combining a knowledge of the threat landscape, attackers, TTPs and indicators of compromise to quickly search through the large amounts of data sources.

Tools and processes used
- Network capture analysis
- Malware reversing
- Forensic artifact analysis
- Threat Intelligence and analytics
- Sandbox environments
- External malware repositories
- Endpoint security analysis

Experts consulted with
- Incident responders
- Intelligence analysts
- Malware reverse engineers
- Technical research team
- Professionals and colleagues in the broader cybersecurity 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 a breach's scope, impact and cost.

ROLE

Typical day
A typical day is spent searching for new threats. Threat hunting analysts use the latest intelligence and analyst-driven techniques to detect intrusions early, investigate rapidly and provide the in-depth behavioral insight needed for effective response. They retrieve and analyze data from network traffic recordings, security device logs and every endpoint in the environment. They compile evidence, build an event timeline and apply knowledge about threat actor behavior to track attackers down fast. Finally, they provide regular updates on investigation progress and definitive, action-oriented reports. In addition to active hunting, threat hunting analysts also study attackers and predict their actions — incorporating this knowledge into future investigations. Analysts gather organize and prioritize available data, then apply analytic tools and methodology to see if the results warrant further investigation. In response to an intrusion, hunt analysts support the investigation by providing evidence gathered during their analysis so that responders and forensic analysts have a thread to pull further.

Without it, then what?
You’ll be in a reactive mode and experience higher attack dwell times — the amount of time the attacker is in an organization’s environment before being discovered. You’ll intensify the risk of missing a breach. And consequently the impact of the breach is likely to be much larger.

FireEye advantage
FireEye hunt analysts continuously discover patterns and trends across the entire FireEye customer base, allowing greater visibility and ability to comprehend events difficult to understand in isolation. FireEye also uses these experts to look for non-malware and other threats that are hard to detect using just technology solutions — for example, threat actors who spread within the environment using standard operating system tools such as the Remote Desktop Protocol.
# Intelligence Analyst

## Responsibilities

The intelligence analyst analyzes world events — including actions by nation states, strategic and military planning, cyber criminals and terrorists’ movements — to provide warning of upcoming cyber threats. They determine attribution for attacks (such as petty criminal vs. nation state). They also determine early on if the threat is significant and sophisticated — for example, a nation state could be masquerading as a lower-skilled adversary to fly under the radar.

This information is then correlated across other data sources and incorporated into intelligence assets.

## Tools and processes used

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

## Experts consulted with

- 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.

## Typical day

Intelligence analysts spend a typical day on both short- and long-term projects. They translate foreign language statements, major announcements and internal or external propaganda. They write complete intelligence pieces that highlight the cyber implications of world events, government announcements, terrorist or military actions and criminal activity. They also conduct their own proactive, independent original research with deep dives into threats, adversary plans and intentions and ways in which cyber operations fit into a specific country’s foreign policy.

## Without it, then what?

Without robust intelligence and analysis you’ll know little or nothing about your adversary, making it difficult to combat threats. If you rely solely on technical solutions for gauging geopolitical risk, you’ll be in a reactive state. But, with a deep understanding of why you are being targeted and what your adversary is likely to do next, you can get ahead of the game.

## FireEye advantage

FireEye intelligence analysts track threats across industries, borders and targets and apply lessons learned to future targets. This tracking identifies not only the victim profile, but also how the attacker operates once inside a network and the techniques they use to spread internally, target data and more.
Malware Reverse Engineer

**Responsibilities**

The malware reverse engineer analyzes critical malware (viruses, backdoors, ransomware, etc.) identified by intelligence analysts, incident responders or technology. They dissect the malware, fight through the attacker’s anti-analysis code and figure out everything the malware does from start to finish. They provide a detailed report back to the responders and analysts that includes information on how the malware tries to persist, in what way the malware communicates on a network and all of its capabilities. This report allows organizations to recognize, remediate and remove threats permanently.

**Tools and processes used**

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

**Experts consulted with**

- 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.

**Typical day**

In a malware reverse engineer’s typical day, the clock starts when malware is found. The engineer uses a variety of techniques, monitoring the malware in a safe environment, analyzing it statically with state-of-the-art tools to get answers to the most critical questions. Then, the engineer dives deep, reverse engineering the malware by studying its compiled machine code. Finally, the engineer writes up and delivers a report detailing the findings. These findings drive how responders and analysts act — for example, findings could steer analysts to study other locations on the file system or network for related artifacts and take the investigation in a new direction.

**Without it, then what?**

You’ll lack a true understanding of the threat. Without a deep dive into the malware, you limit your ability to permanently remove the threat, limit its spread or identify the same threat on other systems. You won’t understand the full malware family capabilities and will mistakenly focus on finding the exact same piece of malware (which almost never shows up again), wasting precious time and resources.

**FireEye advantage**

FireEye intelligence and incident response experience supports a much broader set of malware. Our malware analysts can quickly automate and correlate elements they’ve seen previously throughout the FireEye customer base and in their extensive experience responding to incidents.
# Attack Simulation Specialist

## Responsibilities

The attack simulation specialist conducts tests in your production environments that closely resemble an attack and have objectives similar to real world attackers, such as stealing or destroying sensitive data. This specialist leverages experience from the front lines of cyber attacks and other threat intelligence to simulate the tactics, techniques and procedures (TTPs) of real-world attackers that target your environment. They simulate and find vulnerabilities by exploiting issues, escalating privileges and moving within the IT environment. They test the strength of security program, including how well staff, processes and technology protect the most critical assets.

## Tools and processes used

- 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)

## Experts consulted with

- 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 dealing with real-world breach attempts.

## Typical day

Throughout a typical day an attack simulation specialist will usually be engaged in different test phases — for example, trying to gain access from the outside while another specialist has a foothold and another is moving laterally throughout a network. In addition, the team is constantly working to stay current on tools, trends and defensive technology.

## Without it, then what?

You don’t know where you’re vulnerable and can’t tell if your defenses work because you haven’t verified or tested them. You’ll lack an understanding of how attacks play out, which could hinder your ability to respond effectively to a real-world incident.

## FireEye advantage

FireEye will test your security infrastructure and tell you about your security flaws. We are engaged in the most consequential breach responses, so we know how attackers operate and can simulate the most sophisticated attacks. We can also provide guidance on methodologies, tools and trends to help you stay ahead of attackers.
# Incident Responder

## Responsibilities

The incident responder handles security incidents, resolves specific or niche issues and puts solutions in place to address systemic causes of incidents. They perform host-, network- and log-based analyses in addition to malware triage to support intrusion investigations. They aim to quickly scope compromises including what data was lost, identify the tactics, techniques and procedures (TTPs) of the attacker, plan and execute countermeasures and bolster the system’s resilience to future attacks.

## Tools and processes used

- Commercial and open-source forensic analysis tools
- Commercial and open-source malware analysis tools
- Commercial and open-source 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

## Experts consulted with

- 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.

## Typical day

The typical day of an incident responder starts with a check for new activity within the ongoing investigation. With each incident, the incident responder will assess the situation, verify response objectives, collect evidence, perform analysis, provide management direction, develop remediation plans and create an investigative report. The responder will review status reports and assess acute need, reprioritize based on project objectives, communicate status updates and work on containment and validation.

## Without it, then what?

You’ll have no designated person to respond to and remediate attacks. Your organization will be unlikely to develop or maintain institutional knowledge about the environment, intrusions or response methodology. Time between detection and response will be longer, increasing the likelihood of stolen data, disrupted systems and future threats.

## FireEye advantage

FireEye provides a large, highly trained team of incident responders. They can pull from a historic library of incident response engagements, rely on 12+ years of victimology data and possess extensive — often leading edge — knowledge of forensic artifacts – gleaned from across a broad ecosystem of experiences and evidence.
# Security Threat Protection Analyst

## Responsibilities
Collects, stores and analyzes raw data coming from discovery systems, sensor networks and human visibility to create actionable intelligence that highlights how the threat landscape is changing – including identification of new threat actors, new campaigns and new and changing techniques. New and refined detection algorithms are generated and pushed back into the security technologies being used for real-time protection.

## Tools and processes used
- Custom and proprietary discovery and automation tools
- Machine learning technology, including custom algorithms for large-scale application
- Big data analytics technology
- Data visualization tools

## Experts consulted with
- Malware reverse engineers
- Data scientists
- Intelligence analysts
- Researchers

## Desired outcome
Precise threat detection, which includes protecting the organization in real time to all emerging threats. Detect all attacks, block attacks without false positives and alert the organization to advance attacks that are high risk.

## Typical day
In a typical day, a security threat protection analyst monitors the state of the operations, including searching for new techniques being used by attackers including mechanisms they use to evade detection. This information is then codified into technology that protects the organization. The analyst evaluates different challenges that the systems and organization are experiencing, putting together plans to mitigate. Analysts also validate adequate short-, medium- and long-term protection strategies.

## Without it, then what?
Your environment will be at risk for a breach (loss of customer info, sensitive data) if you miss detecting something important. If the detection is not precise enough and you have a false alert, you could end up with a denial of service and unnecessarily block a key business process or create a lot of busy work for your analysts.

## FireEye advantage
The security threat protection analysts working in FireEye Labs are constantly scanning for patterns and threats across our entire customer base. This visibility along with our tremendous depth and breadth of experience, allows us to make sense of complex events quickly. FireEye works with researchers to codify results, benefitting all customers through new product-level features and enhancements.
## Security Program Analyst

### Responsibilities
The security program analyst monitors, analyzes, measures and balances business risk based on cyber threats. They assess threat risk and exposure and build roadmaps to close security gaps.

- Traditional preventative technology (such as IPS, proxies, firewalls, VPN)
- Access management control mechanisms (such as privileged access tools)
- Monitoring of network traffic, email and host space
- Analytics and intelligence platforms for detection and control

### Tools and processes used

### Experts consulted with
- Business stakeholders — such as CFO or COO — to help evaluate business risk
- Legal and compliance professionals
- IT professionals

### Desired outcome
Properly analyze, measure and balance business risk based on cyber threats. Help to establish an accurate understanding of current cyber risks and where to invest to close gaps based on high-risk threats.

### Typical day
In a typical day, a security program analyst focuses on aligning the company’s overall security posture with the threats they are likely to face. They identify events of interest, gather alert data and correlate all available information with threat intelligence. They prioritize events for deeper analysis and determine how to manage the risks that arise.

### Without it, then what?
Without an experienced security professional overseeing your security program, you’ll underestimate cyber risk and put your organization at unnecessary operational, financial, legal or reputational risk.

### FireEye advantage
FireEye professionals have a deep understanding of the threat landscape specific to your industry and geographic region. We can assess your risk and recommend a security strategy that balances exposure and expense.
Expertise On Demand

There are many unique, specialized cyber-security roles to be filled in order to adequately protect an organization — from a threat hunting analyst to an intelligence analyst to a more strategic security program analyst. In addition, the interplay among these roles is key — the entire security team works together to identify, analyze, contain and remediate incidents, ensuring the organization is better prepared for the next intrusion.

However, it isn’t always feasible — or the best solution — for companies to have all of these high-specialized experts in-house. If you can even find the right talent (amid the worldwide talent shortage), it’s expensive to bring them on board and retain 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 experience.

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

Whether your security team is a single-person or large operation, FireEye can provide Expertise On Demand you need to complement and complete your security team, helping you to provide the world-class security your organization deserves.

To learn more about FireEye, visit: www.FireEye.com