Hyperion Gray, LLC | www.hyperiongray.com | contact@hyperiongray.com
3036 Westmoreland Farm Rd| Davidson NC, 28036| 304-989-1431

Hyperion Gray Incident Response

Executive Summary

Hyperion Gray's strong incident response capability comes from years of on-the-ground experience from the perspective of a hacker. We do not provide cookie-cutter incident response and basic monitoring as other companies but provide an unparalleled introspective view of hackers' methodology. If you would like a lesser standard, we are happy to refer you to some of our competitors. Our mix of computer forensics, continuous monitoring, and penetration testing experience provides our customers with end-to-end solutions for responding to incidents and ensuring that they do not continue to occur. We use US Department of Defense standards to ensure your business' security [1]. However, we understand that security cannot be the only priority of a company –business operations must continue as we perform our assessments and fixes. We provide a tiered approach such that costs can be kept to a minimum. We integrate with your currently available tools and provide a detailed plan before approaching each engagement to ensure business continuity during our incident response efforts. Hyperion Gray is an elite team of well-known hackers who have not only conducted research into computer security, we have worked with the most advanced research organizations in the world, such as the Defense Advanced Research Projects Agency (DARPA) [2] [3] and the US intelligence community's counterpart IARPA [4] on never-before seen incident prediction and response technology.

Initial Incident Response

At Hyperion Gray we understand that responding to an incident can be a daunting task. First, know that we are here for you and your organization every step of the way. Having familiarity in both securing and breaking into massive US Department of Defense and corporate networks, no task is too large for our team. For large organizations or Federal governments this often means attempting to stop a hacker from persisting within a network of tens or even hundreds of thousands of assets. Persistence occurs when a hacker maintains their foothold in a network without the knowledge of incident responders. By knowing the latest and developing techniques hackers are using, Hyperion Gray can provide guidance to stop hackers in their tracks.

The initial phase of our incident response focuses solely on information gathering efforts. By asking the right questions from the start, we work effectively and efficiently within your organization and offer bespoke, custom solutions for only what you need and none of what you do not. Many reading this may be thinking – "where do we even start? I don't even know how many assets are on my network!" We at Hyperion Gray would like you to know that you are not alone. It is common in large-scale networks to lose track of even the most basic attributes of your network, such as the number of workstations or the number of servers hosted on a network. Not to worry, this is common, and we are well-versed in asset discovery of even the largest and most complex networks.

Therefore, our initial incident response consists of **a deep understanding** of your network. A small sample of some questions we ask before we perform any hands-on work:

How many network segments appear to be affected? Approximately how many assets are on these networks?

What appears to be the hackers' goal(s)? For example, is a hacker attempting to deface your company's web presence? Are they looking for financial systems? Is it unknown at the time?

Is there a pattern in the affected assets? Are hackers focusing on Windows workstations in order to attack your users? Are they focusing on your Linux servers? These can be very telling, as individual hackers or even teams of hackers may be using 0-days (as-of-yet undiscovered) vulnerabilities to traverse your network.

What current security tools/technologies are currently in use on your network?
In short, we begin with a simple conversation with your IT and networking teams, along with any relevant security teams.

Stopping the Hacker(s)

Once we understand the basics of your network and the hackers' goals, our primary action item is to *stop the damage*. When a hacker enters a network their first goal is almost always to persist within the network. Typically, hackers backdoor your network in such a way that is difficult to detect. Moreover, there are often multiple points of persistence, and multiple methodologies of persistence. If they are good at what they do, an adversary can remain undetected to even the most sophisticated state-of-the-art tools. Therefore, Hyperion Gray focuses not on expensive tools, but by performing in-depth analysis of a sample set of affected assets. A hacker typically has spent weeks, months, or even years within your network before being detected, and it may be difficult or even impossible to analyze every single asset. To mitigate this, we sample your assets by type (e.g., Linux web server, Windows workstation, Windows server, etc.) and attempt to gain an understanding of the basics of how the hacker maintains persistence in your network. This is not always possible, but by using our expertise we can at least gain a basic understanding of a hacker's methodology, the tools they use, and the skill level of an attacker.

After gaining an understanding of the adversary, we move to the next phase – stopping them in their tracks. We use well-known, industry standard methods of stopping hackers – this is not complicated but somewhat tedious. We never solely rely on anti-viruses, nor on intrusion detection/prevention systems. Instead, we rely on common sense and expertise. Although these tools are important components of a thorough incident response plan and continued security posture, we first work with your organization to develop a comprehensive plan to sanitize your assets of any malicious software that a hacker relies on to persist within your network. Practically speaking, this means discovering troublesome assets and reinstalling many operating systems along with verifying that base images have not been infected with malicious code. Many vendors will attempt to "clean up" your systems using tools such as anti-virus, but several academic studies and hacker conference talks show how easy it is to evade such tools. Therefore, the only solution is a full reinstall of the operating system of an asset. We understand that this can be disruptive to

your organization, which is why we work with your organization to ensure business continuity throughout this process. We do not simply make up these steps as we go along, but instead one of our proudest assets as a company is that **we are hackers.** We know how a hacker thinks, the methodologies a hacker uses, and the ways in which they can avoid detection. By using a mix of common tools and some dirty tricks, we make your network a hotbed of detection for a short amount of time. By using intrusion detection/prevention tools (we can recommend some or use current tools owned by your organization), honey token/honeypot tools (fake assets that if attacked give us alerts), and centralizing the information given using a Security Information Event Manager (SIEM), we immediately detect any attacker activity. We monitor this closely in parallel with re-imaging and cleansing your assets to ensure that we are, in fact, stopping the hack from progressing. In short, we become hunters and the hacker(s) the prey. Incidentally, these security introspection tools can remain in your network, allowing your security/IT team or Hyperion Gray to continue monitoring the network even after the incident response has ended.

We use standards set out by the US Government and Department of Defense, in particular US-CERT's National Incident Response Guidelines customized to fit your organization's needs. In other words – we provide nation-state level security to companies of any size. We maintain these standards as we gain an understanding of your network, the following steps are performed in parallel.

Implementing Immediate Detection Methods & Supplementing with Threat Intelligence

Threat intelligence is a relatively new field in the information security community. It involves using large databases of known attacker attributes known as **indicators.** These vary widely and can be anything from known malicious IP address ranges to known email addresses to attack organizations. By performing threat intelligence in parallel with detection methods and asset cleansing we can better understand the adversary. This aims to answer the question – who is attacking, and more importantly, how sophisticated are they? An attack by teenagers looking to have fun is far different than a Chinese government sponsored attack, and we must tailor our response accordingly. It is rare that the real identity of an attacker is achieved, as even moderately skilled attackers can hide their true identity. However, attacks can be correlated with other attacks, allowing us to understand the goals and skill level of an attacker.

Monitoring and Testing

The systems that we implement or ensure are already implemented within your environment are not taken offline. Instead, we attempt to turn your negative incident into a positive outcome for your organization. We provide or ensure that your internal security team provides unparalleled and continued introspection to your environment. Without after-action care, it is possible that the hack on your network will simply happen again, wasting much of your business' precious time and capital. Therefore, the aforementioned tooling and threat intelligence information continues to be used in your environment. We at Hyperion Gray provide end-to-end solutions to accomplish

this either ourselves or by training your security team to perform sophisticated monitoring. In short, we leave you in a much better state than you were before.

Validating or Implementing Scanning and Testing

We highly recommend that after the comprehensive review of your network that you scan and perform various regular security tests against your networks – especially those affected by the incident. This involves two kinds of testing, which Hyperion Gray specializes in. The first is vulnerability scanning. This type of scanning automates security testing of a large number of assets and provides information on assets' security posture. This type of testing is **broad but not deep**. It covers many assets but can only provide so much insight into each asset. This is why we recommend a **penetration test** against your organization. As opposed to being an automated and broad test, we become the hackers and attempt to break into your network(s). This type of test is **deep but not broad** comprised of highly manual methodologies which are dependent on the skillset of the simulated attacker. At Hyperion Gray we hire only the best of the best hackers with the most elite qualifications. All our hackers are certified as ethical hackers and are skilled nation-state level attackers. In short: we're better than anyone that has attempted to break into your network, and we provide unparalleled capabilities - from finding undiscovered vulnerabilities in major products to breaking into customized web applications. We recommend performing regular, automated vulnerability scanning and a penetration test at least twice per year. We at Hyperion Gray are glad to either validate testing from third party vendors or perform these tasks ourselves. Of course, we recommend ourselves, but we are somewhat biased.

Pricing

From the beginning we like to make clear that we are not the cheapest shop. We are the elite of the elite, and we provide highly sophisticated capabilities. This is not ego, it is simply taken from the fact that we work with the most advanced research organizations in the world and have staffed many US Department of Defense, Federal, and international corporate networks successfully. Our track record speaks for itself – in a network penetration test we have **never failed** to break into a network.

Our pricing provides flexibility for organizations with pieces of the aforementioned items, such that we can integrate with your existing solutions, or implement ones that your organization may be missing. Our cost structure works with **price caps**- amounts that we do not exceed. It is not rare that a piece of work takes us less time, in which case we do not charge the customer the full amount. Price is determined by the number of assets owned by a company *and* the level of introspection requested. We provide Basic, Professional, and Ultimate packages along with piece-meal testing should you only need a portion of our capabilities. Below is our pricing sheet divided into the various tiers we provide:

Our **Basic Tier**:

- **Initial Incident Response**
- **Implementing Immediate Detection Methods**
- **Stopping the Hackers**
- **Validating or Implementing Immediate Scanning**

Number of Assets	*Tier*	*Total Price*

1,000 or less	Basic	$10,000 USD
1,000-5,000	Basic	$20,000 USD
5,000-10,000	Basic	$30,000 USD
10,000+	Basic	$40,000 USD

Our **Professional Tier:**
Everything our Basic Tier provides
2 years of biannual penetration testing (4 total penetration tests)

Number of Assets	*Tier*	*Total Price*
1,000 or less	Professional	$35,000 USD
1,000-5,000	Professional	$44,000 USD
5,000-10,000	Professional	$56,000 USD
10,000+	Professional	$68,000 USD

Our **Ultimate Tier:**
Everything our Professional Tier
4 years of biannual penetration testing (8 total penetration tests)
Supplementing engagement with threat intelligence

Number of Assets	*Tier*	*Total Price*
1,000 or less	Ultimate	$42,000 USD
1,000-5,000	Ultimate	$56,000 USD
5,000-10,000	Ultimate	$70,000 USD
10,000+	Ultimate	$87,000 USD

You may choose from the following tasks:

Number of Assets	*Task*	*Total Price*
1,000 or less	Penetration Test (2/yrs.)	$30,000 USD
1,000-5,000	Penetration Test (2/yrs.)	$40,000 USD
5,000-10,000	Penetration Test (2/yrs.)	$55,000 USD
10,000+	Penetration Test (2/yrs.)	$60,000 USD

Number of Assets	*Task*	*Total Price*
1,000 or less	Simple Incident Response*	$8,000 USD
1,000-5,000	Simple Incident Response*	$13,000 USD
5,000-10,000	Simple Incident Response*	$23,000 USD
10,000+	Simple Incident Response*	$31,000 USD

* No after-action testing, No threat intelligence

[1] https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[2] https://www.forbes.com/sites/thomasbrewster/2018/03/13/dark-web-map-6000-webpages/?sh=a01530618e73

[3] https://www.forbes.com/sites/thomasbrewster/2015/05/06/punkspider-google-for-all-web-vulnerabilities/?sh=2313aab024af

[4] https://www.forbes.com/sites/thomasbrewster/2019/03/29/omnisense-us-intelligence-funded-startup-claims-it-can-predict-cyberattacks-days-before-they-happen/?sh=22a57b402766