GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Donlon, Meaghan

Title: "The Fundamentals of Building a Threat Detection and Response Program"

Website: Rapid 7 Blog

Organization: Rapid 7

Date: 17 September 2019

URL: https://blog.rapid7.com/2019/09/17/the-fundamentals-of-building-a-threat-detection-and-response-program/

Accessed: 19 Oct 2019

Synopsis: Last month, the Rapid7 team kicked off a learning series focused on building and ramping a threat detection and response program. Whether your organization is newly ready to evolve beyond just firewalls and antivirus, or actively investing in maturing SOC operations, this series has something for any business that wants to improve their ability to respond to threats.

In this post, we'll summarize some of the key takeaways for businesses looking to further their threat detection and response programs, as well as provide helpful resources that will help you along the way.

The Fundamentals of Building a Threat Detection & Response Program

Meaghan Donlon

Last month, the Rapid7 team kicked off a learning series focused on building and ramping a threat detection and response program. Whether your organization is newly ready to evolve beyond just firewalls and antivirus, or actively investing in maturing SOC operations, this series has something for any business that wants to improve their ability to respond to threats.

In this post, we'll summarize some of the key takeaways for businesses looking to further their threat detection and response programs, as well as provide helpful resources that will help you along the way.

What is threat detection and response?

Threat detection is an organization's ability to recognize when they are compromised, and "response" is everything that happens once that potential threat is identified.

Many organizations may not feel urgency to ramp up a threat detection and response program because they are confident in the prevention defenses they have in place to keep intruders out. Preparation and prevention are important pieces of any security program, but even with the best defenses, no organization is impenetrable. A strong threat detection and response program combines people, processes, and technology to recognize signs of breach as early as possible, and take the best possible action. As Rapid7 Principal Threat Researcher Wade Woolwine comments in our Threat Detection and Response 101 panel discussion, "Detection and response is where *people* join forces with *technology* to address a breach."

Find more of an introductory threat detection overview here.

With definitions out of the way, let's shift gears to talk about building an effective threat detection and response program.

Building a threat detection and response program

Step 1: Gaining full visibility of your environment and users

With the proliferation of data and toolsets in modern networks, compounded by the accelerated rate of change in these environments, getting visibility into your assets and user activity can be challenging. However, this is a crucial foundational step. Organizations can lose sight of this activity data when focusing too narrowly on compliance alone. While proving compliance is important, and requires appropriate log aggregation and retention, many of those same data sources can also be analyzed to find potential indicators of compromise.

> "Make processes that are applicable to what's happening in your day to day, what are you protecting, what's most important, and ensure you have good visibility ... and are able to paint a cohesive picture across these different technologies."
> — Hannah Coakley, Rapid7 Security Solutions Engineer

System logs, network data, and endpoint telemetry can help build that vivid picture of a network. This data is powerful, as it builds the foundation that will be analyzed to detect threats; it can also be utilized down the line for investigations or proactive threat hunting. That said, for organizations just starting out, the idea of trying to tackle ingestion of *all* of this data out of the gate may be a bit overwhelming. Going back to Hannah's previous comment, to help prioritize what data to focus on to start, organizations should understand what's most important to protect within their organization and what are the most likely entry points attackers might use. For example, the majority of breaches are initiated with compromised credentials, which makes visibility into user authentications and admin activity to find anomalous behavior a high priority for most organizations.

There are a number of frameworks that can help teams understand common attack techniques. The MITRE ATT&CK framework continues to grow in popularity because of its thoroughness in detailing the most prevalent tactics used by attackers. If you're interested in an even further prioritized list to start, the latest Rapid7 Quarterly Threat Report maps the most common threats identified across the Rapid7 Managed SOC, mapped to the ATT&CK framework.

With visibility into activity across your environment, the foundation is in place to put this data to work in helping detect potential threats.

Step 2: Building and responding to detections in your threat detection and response program

Because there are so many different types of potential attacks, strong threat detection needs to be multifaceted to be able to recognize both known and unknown threats. Known threats are those that are recognizable because the malware or attacker infrastructure has been identified as associated with malicious activity. Unknown threats are those that haven't been identified in the wild (or are ever-changing), but threat intelligence suggests that threat actors are targeting a swath of vulnerable assets, weak credentials, or a specific industry vertical. Let's look at a couple examples.

There are two ways to find threats: find anomalies across your infrastructure, and identify known-bad attacker techniques. In the first case, if a user logs in from Boston every morning and suddenly logs in from Moscow one afternoon, this is

certainly an activity of interest for your SOC team. User behavior analytics (UBA) are invaluable in helping identify this kind of anomalous behavior quickly. UBA tools establish a baseline for what is "normal" in a given environment, then leverage analytics (or in some cases, machine learning) to determine when behavior is straying from that baseline to signal that something may be wrong.

On the flip side, there are a finite number of ways attackers can gain an initial foothold onto the network, discover new assets, and move toward sensitive data. Attacker behavior analytics (ABA) can expose the various tactics, techniques, and procedures by which attackers can gain access—and profit—from your corporate network. This includes things like malware, cryptojacking (using your assets to mine cryptocurrency), and confidential data exfiltration.

During a breach, every moment an attacker is undetected is time for them to tunnel further into your environment. A combination of user and attacker behavior analytics offers a great starting point to ensure your SOC is getting alerted to potential threats as early as possible in the attack chain.

For more about threat detection, check out this interview with Rapid7's VP of Product, Sam Adams, about User Behavior Analytics, or this blog post about Attacker Behavior Analytics.

Step 3: Responding to security incidents

With visibility and detections in place, the last step is having the tools and processes in place to respond to incidents quickly, and with confidence. As a good starting point, Wade recommends a tabletop exercise (ideally with executive stakeholder visibility) to get everyone aligned on the current state of incident response in the organization.

Fundamental incident response questions include:

- Do teams know who is responsible at each phase of incident response?
- Is the proper chain of communications well understood?
- Do team members know when and how to escalate issues when needed?

A great incident response plan and playbook minimizes the impact of a breach and ensures things run smoothly, even in a stressful breach scenario. If you are just getting started, some important considerations include:

- Define roles and duties for handling incidents. These responsibilities, including contact information and backups, should be documented in a readily accessible channel (think an internal wiki or Confluence).
- Go beyond the IT and security teams to document which cross-functional or third party stakeholders (such as legal, PR, your board, or customers) should be looped in, and when. Knowing who owns these various communications and how they should be executed will help ensure response runs smoothly and expectations are met along the way.

Many organizations, in addition to mandated penetration tests, are conducting internal red team exercises to test their preventative controls, understand detection telemetry, and coordinate response.

[eBook] Prepare for Battle: Building an Incident Response Plan

Get Started

Ready, set, go!

If you're reading this post, it means your organization is thinking about threat detection and response, and that's a great start! The good news is, there are a lot of resources and tools in place to help you along the journey.

To learn how Rapid7 can help improve your detection and response program—or even possibly manage it for you—explore InsightIDR, our cloud SIEM, which enables SOC teams to efficiently tackle threat detection and response in their organization.

Start a free trial of InsightIDR today to start detecting and responding to threats targeting your environment and users

Get Started