FORTINET

Top 5 Critical Capabilities of a Detection and Response Platform

Table of Contents

Executive Summary

The sophistication of today's cybercriminals and their campaigns presents a critical challenge and opportunity for security operations teams. While a successful cyber defense requires the ability to monitor many avenues of attack and various signs of malicious activity, which can be complicated and time-consuming for even the most seasoned security practitioners, deploying the right technologies plays a pivotal role in helping your team see the larger picture and effectively respond before any damage occurs. When evaluating detection and response platforms, you should consider several critical questions before purchasing.

Introduction

When making cybersecurity investments, most organizations have historically focused on prevention. But as stated in a Gartner research note, "Given the complexity of threat detection, the age of buying a single best-of-breed threat prevention product is mostly behind us. What is needed is a detection stack capable of gathering enough telemetry using various methods, including APIs, and analyzing it correctly to find the attack needle in the data haystack."[1]

That said, business leaders increasingly recognize that the complexity of security infrastructure and alert management presents an ongoing challenge. The good news is that 75% of organizations are pursuing cybersecurity vendor consolidation, preferring platforms over an array of point products.[2]

However, not all platforms provide the right level of coverage. Attack surface and campaign-stage coverage, detection technology, and degree of integration can vary greatly. Finally, while technology receives the most attention, people and processes remain essential to an effective defense. As Gartner rightly acknowledges, "The stack that is best for you is the one that most efficiently and (cost) effectively meets your monitoring objectives."[3]

Five Considerations for Threat Detection and Response Investments

Suppose you're considering adopting a platform approach to detection and response or need to adjust your approach to risk management. In that case, there are five critical questions to consider before making new investments.

1. What can you inspect?

There are many ways threat actors attempt to enter your organization (email, internet download, external-facing applications and assets, enterprise services, and more), many destinations within it (end-user devices, application servers, IoT and OT systems and more), not to mention additional targets outside the organization (Software-as-a-Service and public cloud infrastructure, for example).

As a recent Gartner brief noted, "The more POVs [points of view] a stack has is directly related to the quantity and type of threat it can detect, and/or the quality of the alert it produces.

At the least, the stack should have a strategic POV to the type of threats that are of most interest."[4] You can't detect what you don't inspect, so be sure that you have all your bases (or attack vectors and targeted infrastructure, in this case) covered.

2. Are all stages covered?

Many attacks today progress through multiple stages to bypass prevention-oriented controls, remain hidden for extended periods, and maximize their impact and return on investment. The MITRE ATT&CK framework and Lockheed Martin's Cyber Kill Chain reflect the common stages and regularly used tactics, which span pre-attack preparation, attack delivery, and post-infection and post-intrusion activity. Fortunately, the more stages the threat actor executes ahead of achieving their ultimate objective, the more chances the organization has to detect and disrupt the attack before it succeeds.

Gartner mentions: "In general, it's best to find a detection stack that works at the attack stage that yields the highest quality alerts for your monitoring objectives."[5] To do so, a security operations platform must cover all avenues of attack and expansion and all stages of the cyber kill chain. These include reconnaissance, weaponization, delivery, exploitation, installation, command and control communication, and further actions on the objective.

3. Which technologies are used to detect?

Of course, just because you are inspecting activity across attack vectors and along the cyber kill chain doesn't automatically mean you can detect attacks, as they are increasingly engineered to look like or even utilize legitimate services or actions. According to Gartner, "Some methods are very simple to the point of deterministic, others are dependent on extensive knowledge of threats, while others might require complex data analysis. There is no best method, yet some methods are more conducive to being effective for certain threats over others."[6]

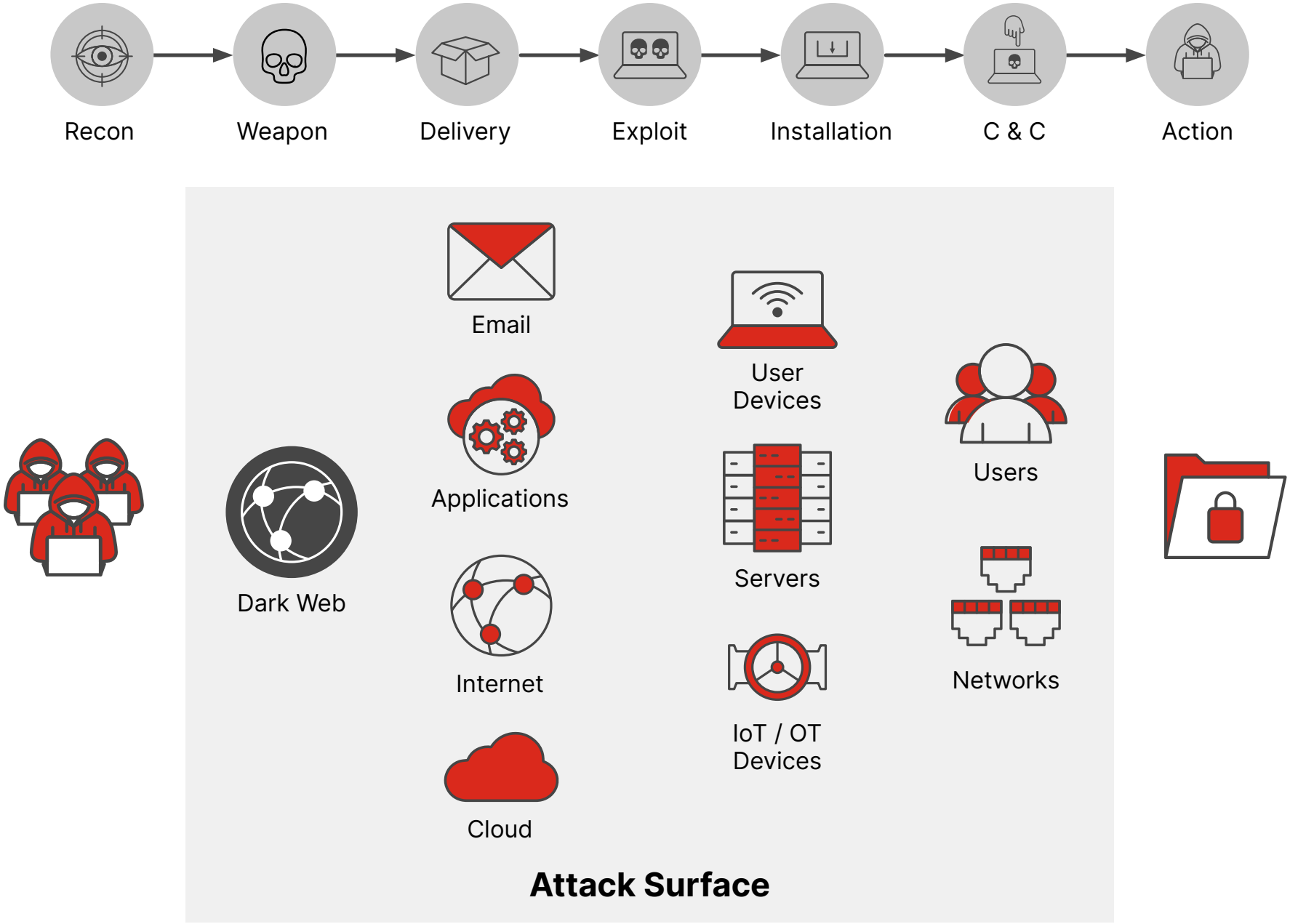

Figure 1: Required attack surface and Cyber Kill Chain coverage

Threat intelligence and indicators of compromise are highly accurate but not very predictive. Rules and heuristics are more predictive but also often produce false positives. Static machine or deep learning models are much more predictive but usually offer a probability that can initially be difficult to trust and challenging to maintain over time. Behavior analysis offers some of the best predictors, but only if these processes can accurately identify known tactics, techniques, or procedures. Identifying anomalous activity that may be unauthorized or legitimate is time-consuming for security teams. Consider the right mix of detection technologies suitable for your organization and team.

4. Who (or what) is expected to respond?

Detection is just the first step. Incident validation and containment are necessary to limit risk, and a comprehensive investigation and remediation process are needed to return to safe operations.

Traditionally, this function has been handled manually by experienced security professionals. And make no mistake—these professionals remain an essential part of the process. However, according to Gartner, "Response SOPs [standard operating procedures] are

good for laying out the objectives, processes and activities. However, they will not be able to cover the prescriptive level of what exactly needs to be done on each object involved in the attack; based on the specific type of attack that just happened."[7]

Organizations need to decide how much to rely on the institutional knowledge of the security team versus building that knowledge into documented processes that can be orchestrated and automated by a platform. A strong security operations strategy typically relies on both, and organizations must determine the proper balance to strike.

5. Can your team run it?

Of course, even the most finely tooled, orchestrated, and automated system will not run itself. As Gartner notes: "The last, and often the hardest challenge is operations... A lot of the work involved isn't break/fix related, but rather take the form of expert-level critical thinking and investigations."[8]

Determine whether the detection and response platform you select is one your team can run or whether you need to rely on outsourced experts. When it comes to outsourcing, you have many options. Outsourcing can be done ad hoc or on an ongoing basis, and you can decide whether you need support for all activities or specialized coverage for certain tasks. In any case, outsourcing does not absolve the organization of cyber risk. It simply utilizes skills and staff from other providers, so if you choose to outsource, make sure you're selecting a platform that can be supported by a reliable partner with the necessary expertise.

Summary

The sophistication of today's threat actors and the complexity of their attacks is both a challenge and an opportunity. Ensuring you have an effective detection system covering the entire attack surface and cyber kill chain with high-fidelity technology that enables an efficient response can greatly reduce your cyber risk.

[1] The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations, Gartner, December 19, 2022.
[2] Gartner Survey Shows 75% of Organizations are Pursuing Security Vendor Consolidation in 2022, Gartner, September 13, 2022.
[3] The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations, Gartner, December 19, 2022.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.

FORTINET

www.fortinet.com

February 2, 2024 4:57 PM
2504903-0-0-EN