SOLUTION BRIEF

FortiEDR Threat Hunting Capabilities

Introduction

As one of the most valuable tools of EDR, threat hunting helps identify bad actors that have otherwise circumvented the first line of defense. It achieves this by proactively identifying threat indicators and vulnerabilities that lurk undetected while also assisting with post-attack investigation, especially with ransomware.

Fortinet FortiEDR is a powerful threat hunting tool that provides benefits earlier and later in the cyber kill chain. Let's examine both aspects.

Threat Hunting Early in the Kill Chain

While FortiEDR pre- and post-infection engines offer protection at multiple stages of the cyber kill chain, how can you proactively scan endpoints for tactics, techniques, and procedures (TTPs) that could indicate a *potential* attack? How can you search for threats that may have otherwise slipped through the net?

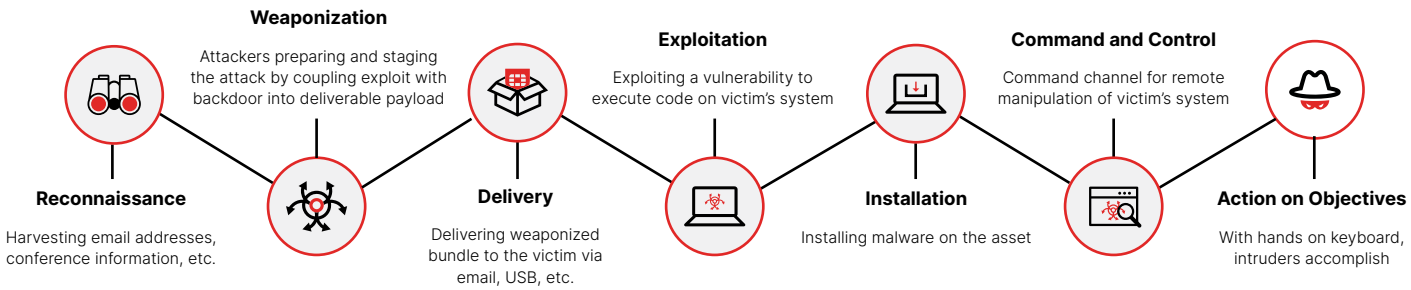

Figure 1: Cyber kill chain.

Threat hunting enables the SOC analyst to proactively scan their environment for metadata that could correspond to a potential attack. FortiEDR collects a plethora of metadata across multiple operating systems, which can be queried. A subset of this is illustrated in Figure 2. While FortiEDR provides extensive data retention by default, it can be extended even further, if necessary.

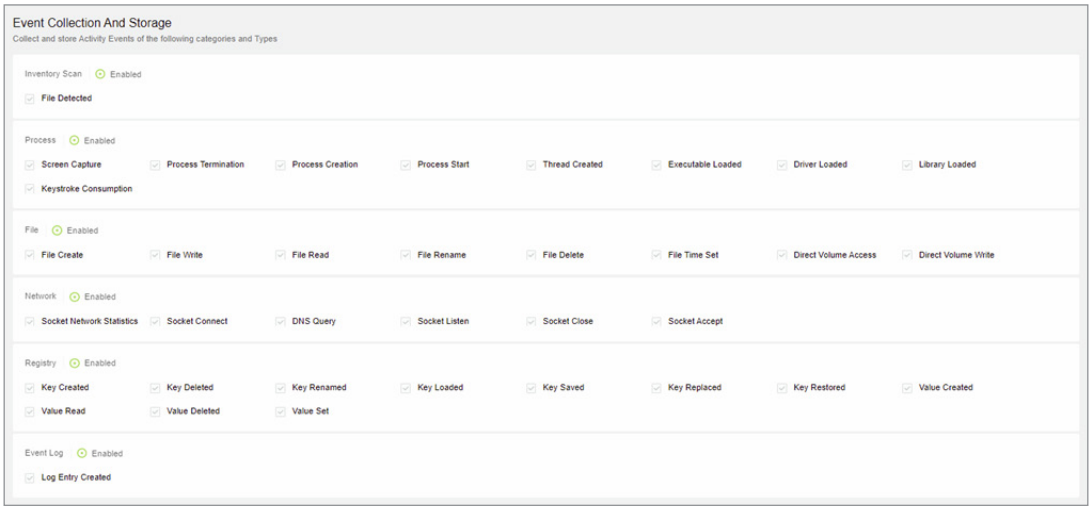

Figure 2: FortiEDR threat hunting collection profile.

Each of these data points (or a combination) could reflect TTPs. This empowers the SOC analyst to better understand their attack surface and pinpoint potential attack vectors within their organization *before* the Delivery or Exploitation phases. Let's look at a practical example with Log4j.

Threat hunting Log4j

Apache Log4j is a Java-based logging audit framework. Apache Log4j 2.1.14.1 and below are susceptible to a remote code execution vulnerability where an attacker can leverage this vulnerability to take full control of a machine.

This module is a prerequisite for other software, which means it can be found in many products and is trivial to exploit. It is critical that organizations inventory their systems and prioritize remediation.

Detection of exploitable systems is possible via FortiEDR threat hunting by searching for the loading of vulnerable Log4j versions. This is an example of a vulnerable Log4j library being loaded by an Apache Tomcat Server.

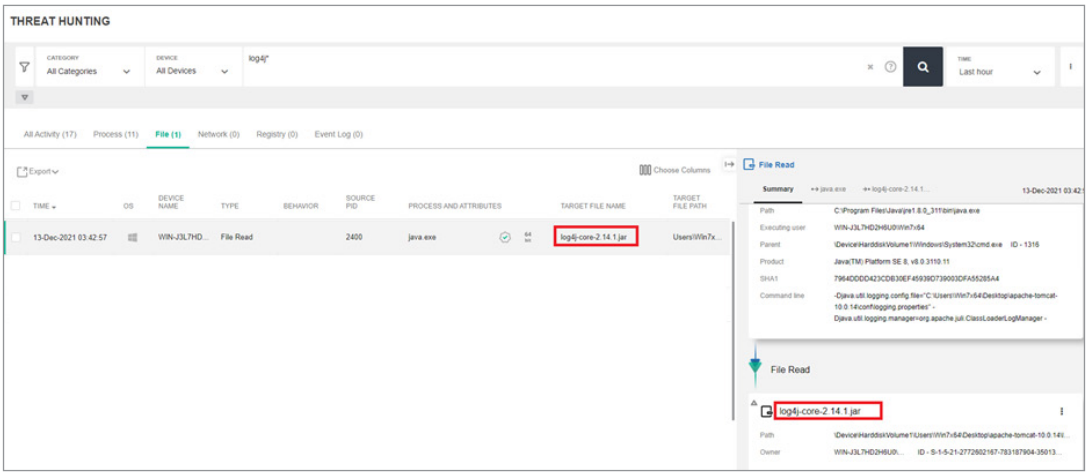

Figure 3: Vulnerable Log4j library being loaded by an Apache Tomcat Server.

With this information, it is possible to intervene *before* an attack is carried out.

Read more about how FortiEDR protects against this Log4j vulnerability.

What about searching for TTPs? While it is often possible to correlate suspicious behaviors with threat hunting tools, it can often be time-consuming and cumbersome unless the solution implements some sort of automated behavioral correlation. FortiEDR is such a solution.

Behavior Correlation Aligned to the MITRE ATT&CK Matrix

With MITRE ATT&CK Matrix alignment, FortiEDR uses sophisticated algorithms to identify behavioral traits in collected metadata and align these to MITRE TTPs. For example: discovery, lateral movement, and reconnaissance.

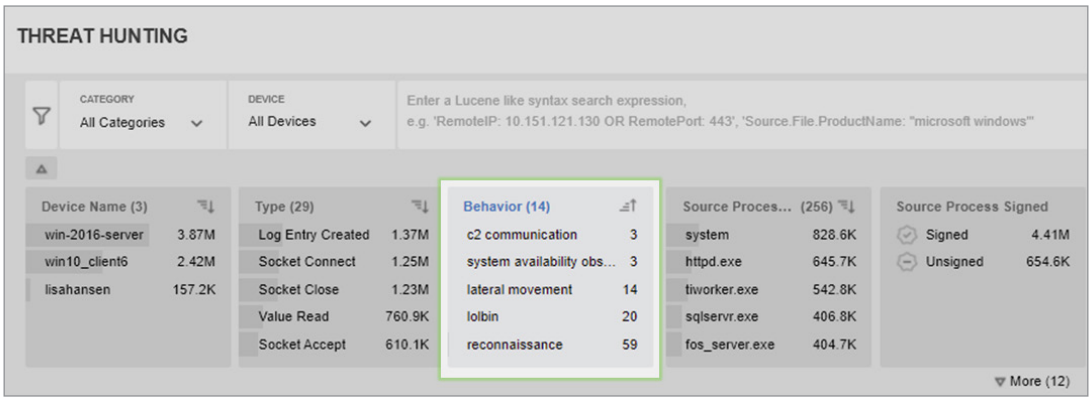

Figure 4: Threat hunting behavioral TTPs aligned to MITRE ATT&CK Matrix.

This enables the SOC analyst to easily identify suspicious behavior that points to TTPs earlier in the kill chain without having to manually sift through the vast amounts of collected data.

While this capability is undoubtably useful, it still requires the SOC analyst to manually search for said behaviors. What if the desire is to be more proactive?

Scheduled Queries

Scheduled Queries are used to automatically run predefined threat hunting searches at recurring intervals. For example: scan all endpoints for reconnaissance behavior every 15 minutes. If this behavior is identified, generate a “Suspicious” event and notify the SOC team.

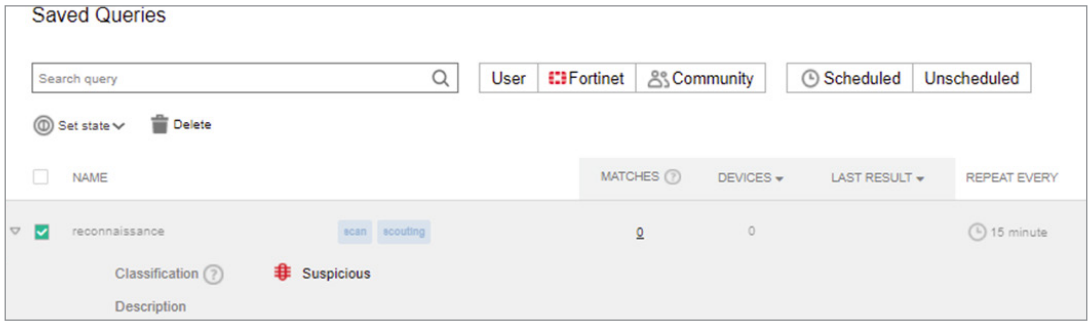

Figure 5: Threat hunting Scheduled Queries.

When fully utilized, these features enable SOC teams to identify potential attacks earlier in the kill chain and greatly reduce the mean time to detection (MTTD). What about post-attack? How does threat hunting help with incident investigation and reducing mean time to remediation (MTTR)?

Threat Hunting Later in the Kill Chain

Post-attack, threat hunting can assist in “following the breadcrumbs” and identifying patient zero, peering back days, weeks, or even months. While the FortiEDR Forensics suite provides much of the answer with patented code-tracing technology, threat hunting is also an essential component.

While investigating an event, FortiEDR provides an intuitive experience with contextualized threat hunting hyperlinks, enabling the SOC analyst to quickly retrieve the information required.

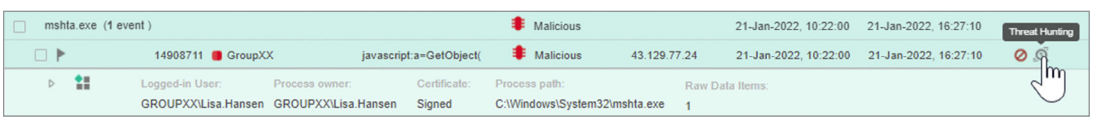

Figure 6: Contextualized threat hunting, Events view.

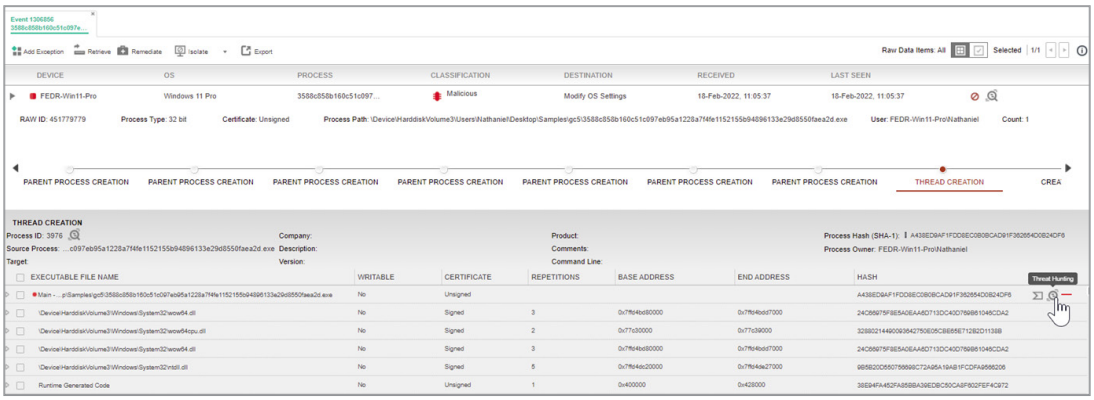

Figure 7: Contextualized threat hunting, Forensics view.

It is also possible to scan all (or selected) endpoints for specific traces of an attack—detonated samples, encryption activity, command and control (C2) communication, etc. These can all be used to trace back to the point of origin: patient zero.

In the following example, an identified threat has been traced back to the use of Mimikatz, a tool commonly used by threat actors to steal credentials and elevate privileges. Using threat hunting, all uses of Mimikatz can be queried while sorting by date and time.

In this case, the first use of mimikatz.exe is quickly identified with a “File Create” activity. This search also indicates the machine and user originally compromised.

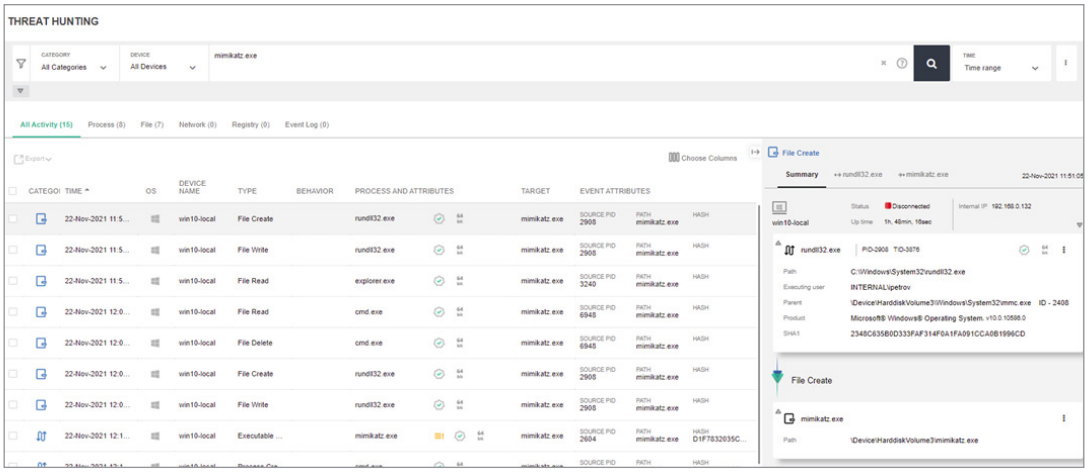

Figure 8: Using threat hunting to find patient zero.

Upon stumbling across a suspicious file, it is also possible to either remediate (delete) or retrieve it for further analysis offline.

Figure 9: Threat hunting retrieve and remediate options.

Shifting focus from file activity to network activity, FortiEDR threat hunting can be used to search for potentially malicious network communication, including C2.

While it is possible to perform searches using contextual GUI-driven workflows, some prefer to construct queries using the flexible Lucene syntax. In this example, it is used to identify all network connections to known bad IPs associated with Kinsing cryptomining.

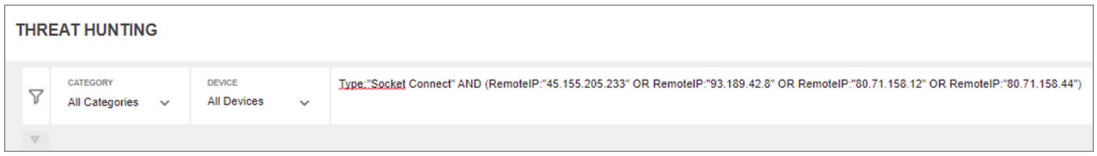

Figure 10: Using threat hunting Lucene syntax.

While this query can be conducted as a one-off search to identify historical indicators, the same query can be scheduled so that notifications are generated on future occurrences.

The flexibility and breadth of these threat hunting features mean that performing post-attack investigations with FortiEDR enables organizations to respond to incidents more effectively and reduce MTTR.

Summary

While traditional endpoint security solutions have operated from the mindset of "lay in wait," threat hunting enables a new way of thinking to reduce MTTD and identify threats earlier in the kill chain. It enables SOC teams to be proactive, and ensures that even *if* something slips through the net, they have the necessary tools to protect the organization. Threat hunting also serves as an essential tool to reduce MTTR when an attack has already occurred.

FortiEDR threat hunting delivers a non-compromising solution combining comprehensive data collection for multiple operating systems with automation and intuitive workflows. It ensures SOC teams do not become overwhelmed thanks to behavioral analysis aligned to the MITRE ATT&CK Matrix and scheduled queries enabling proactive notification of suspicious behavior.

While threat hunting is a powerful tool for SOC analysts, what if your organization doesn't have a SOC team? Fortinet's Managed EDR service, FortiResponder, includes managed threat hunting.

While threat hunting is a key component of what makes FortiEDR an essential solution to protect organizations from the latest cybersecurity threats, it is but one of many components. With many legacy endpoint protection platform (EPP) solutions on the market today rebranding themselves as an EDR solution, it is important for buyers to list the problems they are facing in their organization and aligning a true EDR solution and its components to meet those needs.

March 5, 2022 5:37 AM
1507301-0-0-EN