The Need for Threat Intelligence in Endpoint Protection

In the past several years, we've seen a disturbing trend: Attackers are innovating much faster than defenders are. We've seen the “productization” of malware, with commercial attack kits available on underground forums for anyone who wants to perpetrate a variety of attacks. Large botnets are available for rent, allowing attackers to send spam or launch DDoS attacks at will. Many attackers reuse malware, command-and-control protocols and methods, adapting their “products” over time to keep ahead of the anti-malware industry and security professionals. As more and more attacks occur, however, the likelihood increases that other organizations or groups have seen the attacks before; after all, no organization is immune from attack. The idea behind cyber threat intelligence revolves around this: We can benefit from someone else seeing indicators of attacks and compromise scenarios, hopefully in time to prevent the known attacks or at least detect them more rapidly.

The total “campaign” involved in an advanced threat scenario has many areas where we’ll want to answer questions such as, “Who is targeting us?” and, “What methods are they using?” among others. Understanding what you want to know about threat actors, their methods and how to prevent or detect attacks can help shape your threat intelligence strategy immensely. The better intelligence we have, the more rapidly we can detect and respond.
Overview of CrowdStrike Falcon

CrowdStrike’s Falcon platform seeks to provide a complete replacement for traditional endpoint anti-malware and attack prevention and detection tools. There are several major aspects to the architecture and deployment model that warrant mention, as well as key features that will be highlighted in this review, with a particular emphasis on Falcon X’s threat intelligence capabilities and how they integrate with endpoint protection.

CrowdStrike Falcon has an extremely lightweight agent. Installation is fast, and when the agent is running, it adds negligible overhead to the endpoint. This is critical for operations teams that need to properly secure systems without adding so much overhead that they effectively cripple performance. For systems running in the cloud, every bit of overhead counts even more, because additional overhead increases cloud service provider (CSP) costs.

Another key aspect of the Falcon deployment is its cloud-based monitoring console. Being housed in the cloud helps to alleviate the operational burden of deploying an in-house management server. It can also make deployment more flexible in mixed and hybrid environments, where some systems are on premises while others are in various cloud environments such as Amazon Web Services (AWS) or Microsoft Azure. Next, the Falcon platform captures detailed forensic information about attempted and thwarted attacks, allowing defenders to examine evidence and learn from the attacks to better investigate and prepare for future incidents. Finally, and most specific to our review, Falcon benefits from a large intelligence processing engine within the CrowdStrike cloud, leveraging machine-learning technology built on detection and prevention events spotted in the wild by agent deployments. Any CrowdStrike customer can benefit from the crowd-source model of intelligence developed in this manner.

Falcon X takes this further by adding specific and enhanced threat intelligence capabilities into the platform that help security teams get more in-depth intelligence data, as well as automatic indicators of compromise and intelligence automation driven by the CrowdStrike AI model. Detailed reports on specific actors and campaigns are also available from the CrowdStrike Falcon Intelligence team. This is completely integrated into the Falcon platform and makes threat intelligence readily accessible and usable for all types of analysts when working within the CrowdStrike console.

Getting Started with Falcon X

For the CrowdStrike Falcon X review environment, we used a testbed set up in the CloudShare testing environment with Windows target systems (Mac and Linux sensors are also available). We first installed the Falcon sensor agent, which supports all of the Falcon modules, on the Windows target virtual machine. The system also had a number of malware samples and other exploits available for testing. Installation was simple and very fast (less than one minute), and did not require a reboot.
The online CrowdStrike Falcon console was simple to navigate. The dashboard screen showed us the main detection events and activity that had occurred recently, as well as recent changes and news from the CrowdStrike team (see Figure 1).

By clicking on any of the detected events, we went to the Detections screen, which shows more in-depth information about the threats, actions taken by Falcon and more. One of the more powerful features of the Falcon console is the filtering and investigations feature. At the top of the main console is the Filter bar, where you can choose the range and type of events you want to view in the main console. Analysts can simply click in the Filter bar and be presented with the types of filters to apply (examples include agent version, host type and hostname, severity, time and user account, among others). The “Tactic & Technique” assigned to each threat is also shown. In Figure 2 our top result in the listing is derived from Intelligence Indicators, and is also identified as Fancy Bear.

This example is interesting, because we see two types of intelligence detections in play. The first is a detection type of “Falcon Intel via Intelligence Indicator,” which means that Falcon has automatically correlated this detection with indicators delivered, vetted and enriched by the CrowdStrike threat intelligence team. The second is intel via machine learning (ML), where a file was prevented from executing and was automatically quarantined; it is after this quarantine that Falcon X investigations kick off and provide the intelligence. This is a great example of intelligence generated based on global threats that the CrowdStrike team has seen in the wild mixed with intel that was generated from a threat discovered at the endpoint.

Before diving into the investigation of malware on the affected endpoint, we took a look at the Quarantined Files section of the console, available from the main menu. Falcon X analyzes every quarantined file automatically to assess whether various intelligence indicators apply to it, and the console allows analysts to quickly click the files to see...
a number of file details, which can help to tune SIEMs, firewalls and other infrastructure controls. The details provided in this pane include but are not limited to:

- **Behavioral threat scoring**—Risk analysis of the threat based on all factors assessed by CrowdStrike

- **Strict indicators of compromise (IoCs)**—Indicators detected based on sandbox detonation of the file

- **Broad IoCs**—Indicators from sandbox analysis combined with CrowdStrike threat intelligence (includes data from more than 1 billion malware files assessed over time)

- **Severity and actions taken**—Overall threat ranking and actions taken by the Falcon sensor on the endpoint

The most valuable and in-depth threat intelligence information can be accessed in the associated Falcon X Report, which is found by clicking the icon next to the Behavioral Threat Score. This report is designed for all audiences; where simple actions are expanded upon (e.g., threat level and score, attribution, ability to download IoCs), and detailed process trees and sophisticated analysis breakdowns are also available by clicking into details in the report. Anyone from a Tier 1 analyst to a dedicated cyber threat intelligence analyst can gain value from this report. This report is shown in Figure 3.

The online CrowdStrike Falcon console was simple to navigate. The dashboard screen showed us the main detection events and activity that had occurred recently, as well as recent changes and news from the CrowdStrike team.
All IoCs are downloadable directly from the Falcon console in CSV format, too, which makes importing them into a broader internal threat intelligence platform much simpler. Based on the information seen in the Falcon X report discussed earlier, security operations teams (or any type of analyst) can easily get intelligence data from the console almost immediately. Some of the details included are illustrated in Figure 4.

CrowdStrike Falcon submits quarantined files automatically to expedite full sandbox analysis of the possible malware or exploit, but the platform also enables user submission of non-quarantined files to enable more in-depth analysis from CrowdStrike Falcon X. Falcon X performs a rigorous assessment of each sample to look for correlation in other campaigns seen globally, as well as relationships with other malware or exploits noted in the wild. Falcon X customers can submit files through a form when they discover files that are suspicious (perhaps on systems not running CrowdStrike), and Falcon X Premium users can escalate any sample to CrowdStrike experts for human analysis to provide more in-depth analysis and correlation. The submission form screen for files/malware not yet quarantined is shown in Figure 5.
Investigations with CrowdStrike Falcon X

After reviewing the malware analysis and submission components of the platform, we returned to the console to look at what an analyst might leverage most frequently during a real investigation. There are many locations where an analyst can begin an investigation. The most likely starting point is the Detections pane or the main dashboard. In the Detections pane, we clicked the malware detection event that corresponded to the alert derived from CrowdStrike Intelligence indicators (identified as Fancy Bear). In the Detections detail pane, we can break down a detailed timeline of the malicious behavior, including event types, process names, attributes of malicious files and processes, and hashes and other indicators. See Figure 6.

One of the most valuable features available within the detection event pane is the Sandbox Report for analyzed malware. This report provides a significant amount of detail that includes the threat behavior of the malware, a threat score, threat indicators noted, network activity and process details, and even screenshots of the detonation within the sandbox environment. A screenshot of several sandbox analysis results is shown in Figure 7.

---

**Figure 6. Detailed Malware Detection Timeline**

---

**Figure 7. Details from the CrowdStrike Sandbox Reports**
In the Details pane for a specific detection event, CrowdStrike also has a tab assigned for the profile of this malware and campaign, and we selected the Fancy Bear profile, as seen in Figure 8.

The detailed adversary reports from the CrowdStrike team include access to a plethora of additional threat reports published by the team, as well as alerts issued over time for elements of the campaign; note that many of these more advanced reports and rules are available only to Falcon X Premium customers. These alerts often include immediate notification of emerging threats, malware, campaigns and actors and are intended to be timely, relevant and actionable. Strategic reports look at trends and activities on a longer-term basis (monthly, quarterly and yearly). Another type of report, Tippers, provides in-depth analysis of specific malware and campaigns as applicable (covered shortly). The reports include IoC, YARA and Suricata rules to identify the threats, which are immediately usable by analysts.

In an investigation, analysts should review the common vulnerabilities and exposures (CVEs) in use by actors and patch accordingly, read about the latest attacks seen by known actors and campaigns, and use the YARA, IoC and some of the broad IoCs to help detect or prevent future attacks where possible. Some of these features are available only with the Falcon X Premium service, although Falcon X includes weekly threat updates.

CrowdStrike's intelligence data associated with malware and attack stages is thorough and in-depth, and includes contextual intelligence associated with environmental factors and industry information, analysis and threat intelligence from the CrowdStrike Falcon Intelligence team, and additional useful details, when available. These might include actor attribution, environment context for specific verticals and industries, global IoCs seen across numerous environments and from other intelligence sources, weekly intelligence summary reports and more.
It’s easy to search for related malware as part of an analysis exercise through the MalQuery service within Falcon. The search capability allows analysts to look for hashes and other indicators, as well as any ASCII, Hex or other strings of interest (see Figure 9).

Additionally, the MalQuery hunt feature allows analysts to create YARA rules that break down malware by more complex combinations of patterns, including string pattern matches, conditions where more than one pattern may be required, and metadata describing the rules and malware families involved. More advanced security operations center (SOC) teams and malware analysts will likely develop a catalog of YARA rules they can leverage to find advanced and sophisticated actors, and minimize false positives. An example YARA rule for the Pico ransomware is shown in Figure 10.

CrowdStrike’s hunt feature allows an analyst to query the specific YARA function across the entire spectrum of known intelligence (more than 1.2 billion malware samples gathered during a five-year period by Falcon globally) and return data that can help in determining whether these indicators are present in the protected environment.

Additionally, all CrowdStrike Intelligence IoCs are available within the Falcon Portal and through the Falcon Indicator API for hunting and integration into SIEM or other SOC platforms, as well.

```
rule pico_ransomware {
    meta:
    description = "Rule to detect Pico Ransomware"
    author = "Marc Rivero | @seifreed"
    reference = "https://twitter.com/sirii_uz/status/103513857934355184"

    strings:
    $s1 = "C:\\Users\\rikfe\\Desktop\\Ransomware\\ThanatosSource\\Release\\Ransomware.pdf" fullword ascii
    $s2 = "\\Downloads\\README.txt" fullword ascii
    $s3 = "\\Music\\README.txt" fullword ascii
    $s4 = "\\Videos\\README.txt" fullword ascii
    $s5 = "\\Pictures\\README.txt" fullword ascii
    $s6 = "\\Desktop\\README.txt" fullword ascii
    $s7 = "\\Documents\\README.txt" fullword ascii
    $s8 = "/c taskkill /im " fullword ascii
    $s9 = "\\AppData\\Roaming\\" fullword ascii
    $s10 = "Mozilla/5.0 (Windows NT 6.1) Thanatos/1.1" fullword wide
    $s11 = "AppData\\Roaming" fullword ascii
    $s12 = "\\Downloads" fullword ascii
    $s13 = "operator co_wait" fullword ascii

    condition: ( uint16(0) == 0x5a4d and filesize < 700KB ) and all of them
}
```

Figure 9. Malware Search Functionality

Figure 10. Pico Ransomware YARA Rule

Falcon X Premium Features

To sum up some of the benefits of using Falcon X for threat intelligence and analysis, the service offers:

- Automatic analysis for quarantined files
- Complete actor profile information and threat intelligence that includes kill chain information, targets, CVEs in use and indicators
- IoC generation for any threat detected (or related threats) that can be downloaded and imported into existing threat intelligence platforms or hunting toolkits
- Malware searches for related IoCs and YARA rules
- Weekly threat intelligence reporting and information from the CrowdStrike team
- APIs and integration with SIEM and other tools

While these features were extensive, we also reviewed some of the capabilities included in the Falcon X Premium product. The CrowdStrike Falcon Intelligence dashboard includes a basic level of intelligence information broken down by country, reports and intelligence detection events. Alerts coming from CrowdStrike are also shown (see Figure 11).

We can click into detection events here and see the same details as we can from the normal Detections dashboard (in fact, we’re taken there directly from this event list upon clicking an event), and we could also access threat intelligence reports easily. The Intel Reports menu also allowed for more granular selection of reports, as well as much more ready access to data from feeds such as Snort, Suricata, YARA and others maintained and released by the community. CrowdStrike analysts also produce tailored and customized YARA and Suricata rules. A Snort/Suricata feed sample is shown in Figure 12.
Falcon X Premium allows organizations to use what CrowdStrike calls “Tailored Intelligence” rules, where the CrowdStrike Falcon Intelligence team and the Falcon analysis engine can monitor any keywords and pattern matches noted on social media and Pastebin. Falcon X Premium also covers vertical-specific threats, regional threats, organizational threats and many more levels of reporting. This intelligence reporting includes numerous levels of human intelligence (HUMINT) reporting, expert malware analysis, daily updates for active campaigns, and tailored intelligence for countries and various actor motivations (crime, espionage, etc.). Another report type available with the Premium offering is a set of pointers about noted activity related to malware or campaigns—called Tippers—that may prove useful in adding context and timelines to intelligence efforts. Abstracts of the Tipper documents are listed in association with detected actors and campaigns, with links to the full reports. See Figure 13 for examples of both the abstract and the full report content detail.
Wrapping Up: Final Impressions

As the threat landscape continues to change, and with more advanced attackers than ever, security teams need all the help they can get to more effectively prevent, detect and respond to threats. Incorporating threat intelligence into the detection and response workflow of numerous security operations teams could help to significantly enhance the speed and efficiency (not to mention the accuracy) of investigations. Given attackers’ emphasis on the endpoint today, rapidly detecting and stopping malware and exploits is critical; we need as much information as we can get to determine whether we’re being targeted, whether others have already seen the same issues, and whether there are indicators we can use for hunting and searching across the environment. Those types of information are also important to help when organizations are looking for guidance from experts and the intelligence community in general.

CrowdStrike’s Falcon X solution can help SOC teams in many ways. As an additional layer of contextual information, the data provided in the Falcon console from malware detection events, suspect files not quarantined and industry expertise can be invaluable for analysts trying to dig deeper into events and incidents they’re investigating in their environments. We found the solution intuitive and easy to use. It added a wealth of detail to the malware and attack scenarios we ran against the Falcon sensor in our test environment. As previous reviews have found, the console was packed with data that was easily sorted and analyzed, and pivoting from one data point to another was a seamless exercise throughout.

Dave Shackleford, a SANS analyst, instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

SANS would like to thank this paper’s sponsor:

CrowdStrike