CrowdStrike Products

CROWDSTRIKE

FALCON X: INTELLIGENCE AUTOMATION

ACTIONABLE THREAT INTELLIGENCE IS THE NEXT STEP IN SOC EVOLUTION

EXECUTIVE SUMMARY

Implementing threat intelligence has the potential to profoundly transform an organization's security posture, but it has proven too complex and costly for many organizations to adopt and operationalize. Traditional threat intelligence feeds suffer in quality and relevance, consuming and distracting scarce resources and skills, making it even more difficult for security teams to identify the threats that truly require their attention. The cybersecurity staffing and skills necessary to conduct further investigations are substantial for the largest organizations and simply out of reach for smaller ones.

As a result, many organizations have not successfully implemented a threat intelligence program, let alone a global threat intelligence strategy. These organizations remain slow to respond and constantly react to the onslaught of new attacks instead of confidently deploying proactive countermeasures and getting ahead of the attacker's next move.

CrowdStrike® has automated threat intelligence with Falcon X™, fully integrating threat intelligence into the Falcon endpoint protection platform. Falcon X takes directly from your endpoints, so there's no development effort needed to correlate data from your own systems with a threat intelligence system. Your data is automatically operationalized with no human intervention at all.

While many endpoint protection products utilize artificial intelligence and machine learning to prevent malicious files from executing, they do not automatically provide the context you need to decide how to quickly remediate the problem.

Falcon X gives you the information you need to prioritize your efforts accurately. Smaller companies gain visibility into information that would have remained out of reach, while large enterprises are able to slash their response times exponentially.

All intelligence is actionable, but it's up to each business to figure out how they can put their intelligence to work. What businesses are really seeking is the ability to operationalize their intelligence.

INTRODUCTION

Security Operations Centers are drowning in data, overwhelmed by a huge number of security alerts on a daily basis. Threat Intelligence has the potential to enable teams to work smarter, not harder. But Is intelligence really better than data? This question may sound like heresy to security professionals who are constantly reminded that raw data, while easy to produce, is just numbers but intelligence is actionable. The problem is that last word: actionable. All intelligence is actionable, but it's up to each business to figure out how they can put their intelligence to work. What businesses are really seeking is the ability to operationalize their intelligence.

That's where organizations struggle. They lack the manpower or the time to operationalize intelligence manually, and their automated tools struggle to put alerts into context within the organization. Because security teams have to deal with many inputs and many alerts, they are unable to investigate the vast majority or to determine the best ways to respond to the alerts they do investigate. This is a problem for organizations of any size, and it's a problem that is going to become more critical as the next evolution of advanced threats takes shape around 5G, unsecured IoT devices, connected services, and other technologies that are rapidly gaining traction.

THE THREAT INTELLIGENCE SPECTRUM

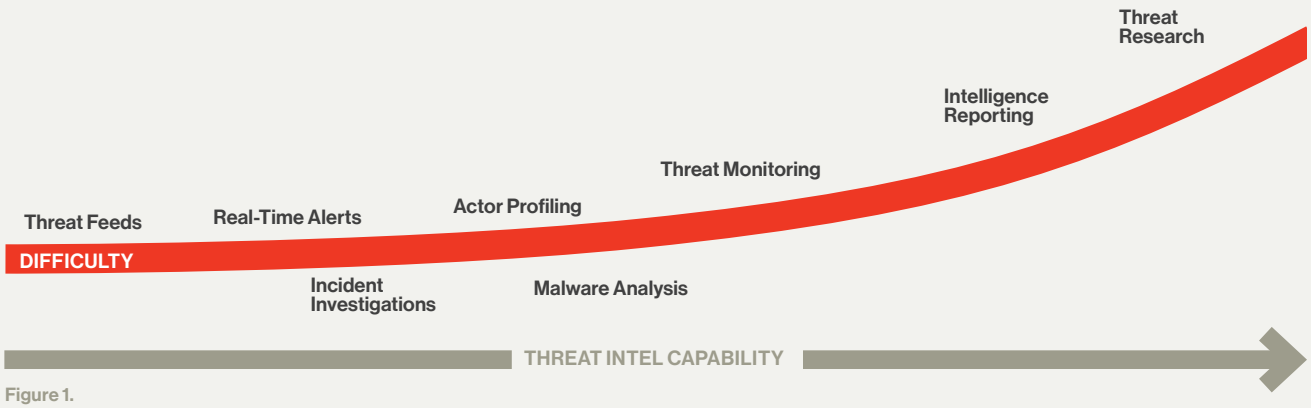


Figure 1.

The first challenge businesses face is defining what intelligence means to them. Is intelligence a threat feed, a research report, threat monitoring or a mixed bag depending on an organization's specific needs? Is a little threat intelligence good enough for Company A while Company B needs more? Not really. While not all businesses are equally attractive targets to attackers, any business that is breached will suffer the painful consequences of lost data, whether that company is a global enterprise or a local store. The stakes are the same for everyone.

Threat intelligence capabilities fall along a spectrum. In a perfect world, all organizations would work with exactly the right amount and quality of threat intelligence for their particular needs. But few organizations work along the entire spectrum because some capabilities demand significant investment and are harder to achieve than others. In the real world, security teams use whatever capabilities they have the resources to implement. Their focus is determined by where their organization is located on the "security maturity curve."

Organizations with limited security capabilities — and those limits may be due to staffing, budget, or other internal considerations — tend to focus on the threats most relevant to their situations in the moment. These are the organizations on the left end of the spectrum, as illustrated in Fig. 1. Companies working on this end of the spectrum are forced into a reactive posture, battling threats as they emerge. They are boiling the ocean in hopes of finding relevant threats, but this is a numbers game they're not well-positioned to win.

Organizations with more security resources strive to achieve a proactive stance by adding threat monitoring, intelligence reporting, threat research and other advanced capabilities into their activities. This level of intelligence not only exposes the threats that are truly targeting an organization, but also exposes global threats that haven't hit an organization yet but may do so in the future. In reality, few companies are able to devote the extremely costly, specialized resources that are necessary for these types of proactive threat intelligence.

A better approach is to focus first on threats relevant to your organization — the threats that are actually on your endpoints, not just those on a general blacklist.

FOCUS ON THE THREATS THAT MATTER TO YOU

Today, most security teams use threat feeds from a variety of sources that provide a blacklist of IP addresses, URLs, or hashes to block. Security teams integrate this data into their own systems. Then they wait for one of their users to perform an action that corresponds to an item on one of the blacklists.

Organizations spend time and money to collect these feeds, but a lot of the data isn't applicable to their unique needs and environments. Industry threat feeds are available, but even those don't lower the noise level enough because businesses within the same industry will have different security concerns.

These activities align with the left side of the spectrum, which is the lower end of the security maturity curve. Organizations on this end of the spectrum react to many inputs and many alerts equally, investing large chunks of their security budgets in investigating false positives and legitimate traffic.

A better approach is to focus first on threats relevant to your organization — the threats that are actually on your endpoints, not just those on a general blacklist. Then global threats can be added into the mix as needed. Organizations able to operate on this end of the spectrum have developed greater security maturity than most, as detailed on the right side of Fig. 1.

OBSTACLES TO OPERATIONALIZING THREAT INTELLIGENCE

IN THE MID-SIZED COMPANY

This security team is typically relying on an endpoint product or tool to secure the network. They might have an early-stage security operations center (SOC) or an incident response(IR) team.

And they are overwhelmed. According to a study, "The Cost of Malware Containment" by the Ponemon institute, mid-sized companies average 17,000 security alerts a week, and only 19 percent of those are reliable. Because the workload is so much greater than the team's capacity, only 4 percent of those suspicious alerts are investigated.

All the team can do is triage the most critical alerts and hope they didn't miss the one that mattered.

IN THE ENTERPRISE

Bigger businesses have full SOCs, but their security teams lack visibility because alerts take too long to investigate. The investigation cycle looks like this:

- Receive an alert from an endpoint
- Decide if it requires investigation or not
- Run the alert through a file analysis in a sandbox
- Get information from the sandbox based on the behavior of the file
- Interpret and decipher the results, which requires high-level technical knowledge
- Determine whether to continue

THE INVESTIGATION CYCLE IS TYPICALLY TEN HOURS. ENTERPRISE SECURITY TEAMS NEED IT TO TAKE MINUTES.

CrowdStrike research has revealed it only takes 1 hour and 58 minutes for an adversary to move from the first compromised server to other systems in the environment. This is known as breakout time.

Breakout time is important because adversaries are rarely targeting the first system they breach. The valuable assets they really want are elsewhere, so the adversary must move laterally to burrow deeper into the network in search of the true target.

CrowdStrike recommends using the 1:10:60 rule.

- 1 minute to detect
- 10 minutes to investigate
- 60 minutes to remediate and contain

ADVERSARIES ARE ABLE TO MOVE SWIFTLY. SO MUST YOU.

TO PREVENT, PREDICT. TO PREDICT, PROFILE.

There are human beings behind every attack who have reasons for targeting specific regions, companies and industries. If you can understand your adversaries' motivations, skill sets and tradecraft, you can predict — and prevent — their next moves by updating patches, performing remediation or taking other steps to counter their known techniques.

Individual companies lack the resources to track adversaries. There are simply so many attackers out there that tracking them, analyzing their technical approaches and documenting their activities requires a massive effort. To collect this type of data requires a significant team with global reach and a great deal of expertise in the realms of technology, human collection and even culture: for example, the CrowdStrike global Falcon Intelligence™ team speaks over 40 languages. The expense required to support security efforts at this scale is beyond the reach of most organizations .

Organizations that are unable to track their attackers cannot know which of their adversaries are likely to strike next or what techniques they'll employ to do so. This knowledge gap leaves businesses stuck on the tactical end of the threat intelligence spectrum, only able to respond to threats as they emerge instead of preventing them from occurring in the first place.

The CrowdStrike global Falcon Intelligence team speaks over

40 languages

THE NEXT-GEN SOC

Traditional security practices are based on prevention and policy-based controls. A typical security stack includes products such as antivirus software, intrusion prevention and detection solutions and firewalls. But with the advent of digital transformation, 5G networks and interconnected sets of services, the nature of threats is changing — and the potential for attacks more devastating than any we've seen before is on the near horizon. Organizations are hungry for better ways to defend their assets.

Gartner is advising security architects to shift their security mindset from incident response to continuous response. Continuous response is based on a feedback loop that uses intelligence, learning and improving to adapt to threats as they evolve. The takeaway for security architects is to treat their systems as if they are already compromised and require continuous monitoring and remediation.

CRITICAL CAPABILITIES OF GARTNER'S ADAPTIVE SECURITY ARCHITECTURE

Source: Gartner (February 2014)

Managing a continuous loop using legacy software would require larger security staffs than most businesses can attract or retain. The only way to implement an adaptive security architecture in the real world is to utilize intelligent automation.

Gartner forecasts that by 2021, endpoint protection platforms will provide automated, orchestrated incident investigation and breach response. But you don't have to wait three years for that level of protection. CrowdStrike is delivering it right now.

INTRODUCING FALCON X

Falcon X is built for organizations that are struggling to respond to cybersecurity alerts and don't have the time or expertise to get ahead of emerging threats. CrowdStrike Falcon X delivers the critical intelligence you need, while eliminating the resource-draining complexity of incident investigations. Falcon X solves this problem by automating threat intelligence and delivering customized and actionable IOCs, enabling organizations to implement proactive defenses.

With the unique cloud-native CrowdStrike Falcon® platform as a foundation, cybersecurity teams can now automatically analyze malware found on endpoints, find related samples from the industry's largest malware search engine and enrich the results with customized threat intelligence. As a result of this closed-loop system, security teams immediately receive a unique combination of customized indicators of compromise (IOCs) and threat intelligence designed to help prevent threats faced by the organization now and in the future.

TURN THE TABLE ON ATTACKERS WITH ACTOR PROFILES

Attackers are studying your business. They create sophisticated victim profiles about your organization long before they try to break into your networks. They know your weaknesses, your technologies, and they even know who belongs to your IT staff and what technical questions those employees are asking on public IT forums.

Now you can turn the tables on attackers by gaining knowledge about them before they come knocking.

Falcon X tracks more than 110 adversaries in cyber espionage, cybercrime, hacktivism, and other corners of the dark web. The information gained about these malicious actors is used to create actor profiles of adversaries' motivation, capabilities, and tradecraft—the why, what, and how of a potential attacker.

You can quickly discover whether an attack is a commodity attack you will deal with just one time, or a targeted attack you can expect to persist. When you understand an adversary's methods, you can predict and prevent their activities in the future.

Falcon X operationalizes actor profiles through strategic analysis and clear documentation that clarifies the preventative steps you can take to stop an attack before it's launched against you. You can see the techniques an attacker uses so you can apply relevant patches, or you can block the servers your attackers use to transmit malicious communications.

With the unique cloud-native CrowdStrike Falcon® platform as a foundation, cybersecurity teams can now automatically analyze malware found on endpoints, find related samples from the industry's largest malware search engine and enrich the results with customized threat intelligence.

FROM VICTIM TO VICTOR IN SECONDS

When CrowdStrike Falcon blocks a threat, it is automatically analyzed by Falcon X. The threat is processed in an safe and secure environment, and is compared to massive databases in order to find related samples of that threat. Here is an example of what Falcon X looks like in action:

• A piece of ransomware is blocked by CrowdStrike, then sent to Falcon X to detonate in a safe sandbox environment.

• The results of the detonation are delivered in a complete report outlining the behavior of the malware, as if it had run in your environment. In the report, you will see that the ransomware would have notified you that the attacker had just encrypted all your data and you must pay up to a bitcoin wallet or lose your assets

• In just a few seconds, Falcon X checks its database of over 1.2 billion malware samples to see if any other attackers are using the same bitcoin wallet.

•When a match is found, your attacker's previous attacks are exposed, perhaps even the identity of the attacker

•Now you can broaden your protection against all similar threats and protect yourself from future attacks.

Falcon X automatically investigates everything, sends it all to file analysis and finds related samples in its massive library. This all happens in minutes, not hours.

HOW FALCON X MAKES THREAT INTELLIGENCE AS EASY AS 1-2-3

1 DEEP ANALYSIS OF THE FILE

Deep analysis reveals what the file would have done if it executed.

Falcon X provides a risk score and outlines steps to respond. In addition, the platform harvests IOCs making it easy for your team to deploy proactive countermeasures against future attacks.

2 FIND SIMILAR THREATS

Falcon X finds threats similar to the one being investigated. This is important because adversaries reuse code and that leaves artifacts that reveal a great deal of information about malware authors and malware campaigns. Knowing who or why a malware attack was launched helps you take the right steps to block all related threats.

3 CONTEXT ENABLES ACTION

Falcon X incorporates threat intelligence that has been enriched by the Crowdstrike team

You gain visibility into more than just bad indicators. You can also see additional context you can use to prioritize your next steps, such as:

- Confidence level
- First/last seen
- Actor attribution
- Related reporting
- And more

LOOK, NO HANDS

Each of these steps is done for you with no human intervention. It takes less than 10 minutes. The results are integrated into other tools your team is using, so if you see Falcon X prevent a file from running, you can see other information about the file as well.

You also have the option to see all indicators, which are updated in real time and that you can integrate into your SIEM/TIP infrastructure if you choose.

HOW FALCON X HELPS YOU PREVENT FUTURE ATTACKS

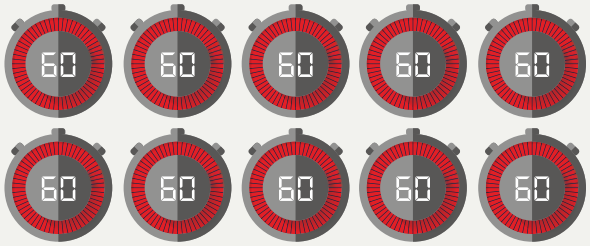
Organizations using legacy security solutions usually try to prevent future attacks by using indicators of compromise. Maybe they update their perimeter by blocking IPs or domains, or they may create Snort or Suricata rules. However, any of those actions still must be tested to be sure the changes aren't stopping legitimate traffic with false positives. But performing those checks requires too much time and too many skills, and test results are prone to errors because tools are disjointed.

Falcon X automatically investigates everything, sends it all to file analysis and finds related samples in its massive library. This all happens in minutes, not hours — and speed is everything, because attackers only need two hours from the time they breach your system to the time they can make a jump toward the assets they really want.

You are protected against future attacks because you have context, attribution and information on how to stop the actor or malware campaign the next time they try to breach you. Falcon X does this by exposing known attack vectors, identifying related malware and malware techniques that have been seen in the past or predicted for the future, and sharing this information throughout all security devices.

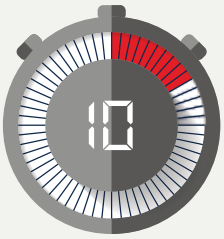
All of this investigation and analysis happens without the need for you to do anything except review the results. You've saved time, you know your priorities, and you can trust your changes to be free of errors.

YOUR INVESTIGATION CYCLE TODAY



10 HOURS

YOUR INVESTIGATION CYCLE WITH FALCON X



10 MINUTES

PREDICTIVE SECURITY TAILORS & OPERATIONALIZES YOUR INTELLIGENCE

Falcon X addresses the entire threat intelligence spectrum. The platform provides context at the endpoint using intelligence automation and the results can be shared with other security elements, like firewall rules, to make them more intelligent. Falcon X includes a global set of indicators of compromise (IOCs), and enables a local and global view of intelligence. Actor profiles provide additional context behind attacks, threat monitoring and intelligence reporting.

The use of intelligent automation solves the operationalization problem all the way along the spectrum. Smaller companies gain access to threat intelligence capabilities they couldn't otherwise acquire, and enterprise security teams are freed from trying to squeeze rote activities into their overscheduled days. Falcon X supplies rich intelligence in a fully automated package.

For more information visit www.crowdstrike.com/products/falconx/.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyber attack types, using sophisticated signatureless AI and Indicator-of-Attack (IOA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates over 1 trillion security events per week from across the globe to immediately prevent and detect threats.

Learn more at www.crowdstrike.com