PROACTIVE HUNTING

The Last Line of Defense Against the "Mega Breach"

Data breaches come in all shapes and sizes, as do the organizations that fall victim to these attacks. What constitutes a "mega breach" for one organization might resemble a common occurrence to another. The real measure of a breach's impact is its consequences for the victims. For example, extraction of even a small amount of crucial intellectual property data could be as devastating as a large-scale hemorrhage of personally identifiable information (PII), depending on how it affects the host organization.

That's why it's critical for every organization to identify its most sensitive and valuable data assets, and to construct a proactive defense strategy to protect them from a potential mega breach. Unfortunately, that process can be daunting -- in fact, it is overwhelming for most organizations, perhaps even impossible using their existing resources. Even if they succeed in identifying the data most at risk, it may be highly distributed within the organization. As a result, companies typically must mount a defense for their entire operation, but a single vulnerability on any endpoint in that system can allow intruders to strike with surgical precision. The odds are vastly in favor of the attacker.

Increasingly, organizations are realizing that deploying state-of-the-art technology is not enough. Even true next-generation endpoint protection -- which combines crowdsourced threat intelligence with innovative cloud-based architectures, machine learning, behavioral analysis and other advanced methodologies (**see CrowdStrike Next Generation Endpoint White Paper**) -- cannot provide 100 percent protection against concerted targeted intrusion efforts conducted by patient, persistent and skilled adversaries. In the final analysis, these types of attacks -- the ones that can culminate in a mega breach -- can only be averted when the best technology is paired with highly skilled and experienced human defenders.

The Role of **Proactive Hunting**

The old IT adage about "people, process and technology" is a good reminder that technology alone cannot solve security issues. Yet, many organizations' investment in the human capital portion of the equation has not kept pace with the sophistication of adversary activity. This underlines the need for an approach to security that fully embraces the human element. In practical terms, it means security teams must start augmenting their security technology with proactive hunting, using human-powered analysis to find clues about attacks before these incidents become full-blown mega breaches.

Proactive hunting puts dedicated analysts in charge of aggressively seeking out threat behaviors. These threat hunters look for evidence of potential malicious behavior that might exist in a detection technology's broad pool of behavioral data but which may be too subtle to warrant an automated response. From there, they can follow even the faintest suggestions of possible misdeeds to put together a picture of whether an attack is in progress, or if the behavior is irregular but does not represent malicious system activity.

You Can't Outspend the Problem

The assertion that technology alone can't solve the mega breach issue is well-documented. Multiple data sources indicate that security spending is rising at a rapid clip, but unfortunately, the river of green spent on cybersecurity seems to be flowing into a bottomless ocean of new threats. The modern paradox of cybersecurity -- falling farther and farther behind in effectiveness in spite of accelerated spending -- comes largely at the hands of nimble threat actors exploiting the asymmetrical nature of today's cyber battles: The attack surface area is simply too large to defend against 100 percent of attacks, particularly when adversaries use sophisticated methods to exploit small vulnerabilities with pinpoint accuracy. Consider these facts:

CYBER DEFENSE SPENDING IS ON THE UPTICK.

- The global cybersecurity market will equal $81.6 billion in 2016[1]
- That figure will rise to $170 billion by 2020[2]

Looking for Trouble:
The Fundamentals of Proactive Hunting

According to research firm Gartner, triggers for proactive threat hunting typically fall into three major investigation initiator categories.[7] The first is hypothesis-driven investigation, such as knowledge of a new threat actor's campaign based on threat intelligence gleaned from a large pool of crowdsourced attack data. In these cases, threat hunters will look into currently unknown attack details and try to find those behaviors within their specific environment. The second category involves investigations that are based on known IOC (Indicator of Compromise) triggers, which spur threat hunters to look deeper into a specific system's activities to find potential compromise or ongoing malicious activity. Finally, there are analytics-driven investigations where threat hunters pursue potential leads based on advanced analytics and machine learning.

- More than 43% of organizations spend $1 million or more on their IT security budgets[3]

....BUT IT NEVER SEEMS TO BE ENOUGH

- 73% of organizations don't feel their organization has enough staff to defend itself against current threats[4]
- 22% of organizations say their security departments are "completely underwater" with work[5]
- 74% of large enterprises regularly ignore security alerts[5]
- The average time it takes to detect attackers is 229 days[6]

Regardless of how the hunting is initiated, the process typically follows a three-step course of action:

Trigger: Some form of advanced tooling helps focus the threat hunting analyst on a specific system or area of the network to investigate further. Often, a hypothesis about a new detection method can be a trigger for proactive hunting.

Investigation: This step requires technology such as EDR (Endpoint Detection and Response). Using EDR, skilled threat hunters will utilize analytical frameworks to take a deep dive into potential malicious behavior and associated activity on a system. The investigation will continue until either the behavior is deemed non-malicious or a complete picture of malicious behavior and/or compromise has been developed.

Resolution: Threat hunters will pass on relevant malicious behavior intelligence to their operations and security counterparts to perform incident response and achieve appropriate mitigation of threats. When done correctly, data gathered by threat hunters about both malicious and non-malicious behavior can be fed back into automated technology to further its effectiveness without human intervention.

The Experts Weigh In

"At least half of all cyber hunting expeditions typically uncover the kinds of stealthy, targeted malware that antivirus will never detect and that presents real and imminent danger to the enterprise. Hunting methodologies sniff out smokescreens intended to mask more sophisticated social engineering exploits that give attackers ongoing access to networks for future compromise."

-Richard Stotts & Scot Lippenholz, Booz Allen Hamilton[9]

Experts agree that proactive hunting requires a tremendous amount of dedication and resources to operate effectively. Some of the most important components necessary for successful proactive hunting include:

Data

- Absolute visibility into endpoints and network assets
- The ability to gather and store granular system events data across the enterprise
- Scalable cloud infrastructure to aggregate and perform real-time analysis on these large data sets

Analytics

- Threat intelligence to cross reference organizational data with external threat trends
- Sophisticated tools to effectively analyze and correlate behavior
- Adequate time for threat hunters to dedicate to analysis processes

The Experts Weigh In

"Proactive threat hunting and investigation is used to detect unknown and advanced threats. Hunting entails analyst-driven investigation rather than relying on signature or rule-based detection mechanisms. In addition, hunting and investigating is proactive, seeking out IOCs and incidents rather than waiting to be alerted and reacting."

-Oliver Rochford & Neil MacDonald, Gartner[9]

Human Capital

- Highly skilled intrusion analysts with expertise advanced enough to identify sophisticated targeted attacks

- The security resources necessary to respond to the findings once they've been delivered

This last category -- human expertise -- is absolutely crucial. Because so much of proactive hunting depends on human interaction and intervention, the success of these efforts depends as much on who is hunting through the data, as it does on the tools they're using to hunt with. As SANS Institute put it in a recent study on proactive hunting:

> "Hunters are curious. They are passionate. They are skilled at leveraging multiple tools and understanding and pushing the limits of those tools. Most important, hunters are innovative analysts who understand their threat landscape and their organization well enough to ask the right questions and find the answers."[11]

It's a tall task, but the rewards are there for organizations that find a way to integrate proactive hunting capabilities with their security

The Experts Weigh In

"Persistent and focused adversaries are already in many enterprises. They present a security challenge that requires dedicated and empowered threat hunters who know what adversaries are capable of, so they can sniff them out of the network as early as possible, close the gaps and create repeatable processes that can be followed for future hunts."

-Robert M. Lee, SANS Institute[10]

operations. According to a recent survey, 74% of organizations who have implemented proactive hunting have reduced their attack surfaces, and 59% have enhanced the speed and accuracy of their security response through its use.[12]

Facing the Realities of Proactive Hunting

While the benefits of proactive hunting are clear, achieving a truly effective in-house threat hunting capability lies beyond the reach of most organizations. "Effective threat hunting remains the domain of the well-resourced, super-security-mature, extra-skilled security 'one percent-ers,'" says Gartner's Anton Chuvakin.[13]

In the vast majority of organizations, mounting an effective proactive hunting program would siphon off resources that are sorely needed to carry out existing security operations center (SOC) and incident response capabilities.

> "44% of organizations say that the number of networking or security staffers they have with strong knowledge in both security and networking technology is inadequate."[15]

In fact, among those early adopters who have ventured into proactive hunting on their own, very few would say they're doing it well. Approximately 88 percent of organizations say their threat-hunting programs need to be improved, and 56 percent

don't like how long it takes them to hunt for threats in-house. Furthermore, 53 percent of organizations say that their hunting isn't invisible to adversaries, meaning their hunting activities may be tipping off the attackers and making detection even harder in the future.[12]

One of the biggest challenges facing organizations trying to build out a proactive hunting program is that of recruiting suitable talent. In spite of rising budgets, security executives are painfully aware of not being able to attract and retain talent to fill even their most basic cybersecurity positions. Proactive hunting requires a much more advanced level of expertise than the average cybersecurity analyst possesses, which means that this growing skills shortage is felt even more acutely when trying to establish a hunting program in-house.

> "Even when budgets aren't an issue, you can't buy the experience of continuous 24/7 battle-hardened hunters -- and even if you get someone great, you can't keep their edge sharp when you are not experiencing a breach every day. Those people will either get bored and leave, or their skills will atrophy. Our hunters respond to a breach every two hours so their skills are always honed."
>
> — **DMITRI ALPEROVITCH**, CTO CrowdStrike

Managed Hunting Solves the Problem

With so many challenges making proactive hunting a nonstarter within the typical security program, security leaders may need to look for an alternative route to plug proactive hunting into their existing infrastructure. For operations as specialized as this, it often makes sense to augment existing security functions with managed threat hunting services.

The idea is to place trust in an outside organization with the right resources -- tools, data and people -- to effectively manage a proactive hunting capability, and then feed the results of the managed hunting team directly into the organization's in-house security operations to quickly mitigate advanced threats as they are exposed by the hunting team. Such a coordinated effort can play a key role in thwarting attacks while they are still in their early stages, avoiding a mega breach situation.

This is exactly the role that Falcon Overwatch plays for CrowdStrike customers today. Built around an advanced and strategically focused 24/7 global operation center, Overwatch directly integrates a dedicated threat hunting team with an organization's existing security resources, without the cost and overhead associated with fielding such a team in-house.

How CrowdStrike Does It

CrowdStrike Falcon Overwatch offers organizations the capability to proactively search for threats above and beyond the automated detection offered by the company's Falcon Host next-generation endpoint protection technology. The global Overwatch

team sifts through endpoint event data telemetry from all across CrowdStrike's worldwide customer community to find "smoking guns" that point to highly sophisticated attacks that would otherwise go undetected.

To power their hunting activities, the Overwatch team uses the CrowdStrike Threat Graph™, a specialized cloud-based graph database designed by CrowdStrike to enable its Falcon Platform to solve complex security challenges. Threat Graph is able to sift through tens of billions of events per day and query petabytes of information in seconds, providing the Overwatch team with a level of scalability and full visibility that most incident hunters can only dream of.

Putting the elite Overwatch team to work looking for the most evolved threats makes it possible to find damaging attacks days, weeks or even months before they would have been detected using conventional automated-only methods. This type of proactive managed hunting can effectively close the windows of opportunity that attackers need to coordinate sophisticated data exfiltration operations that ultimately lead to mega breaches.

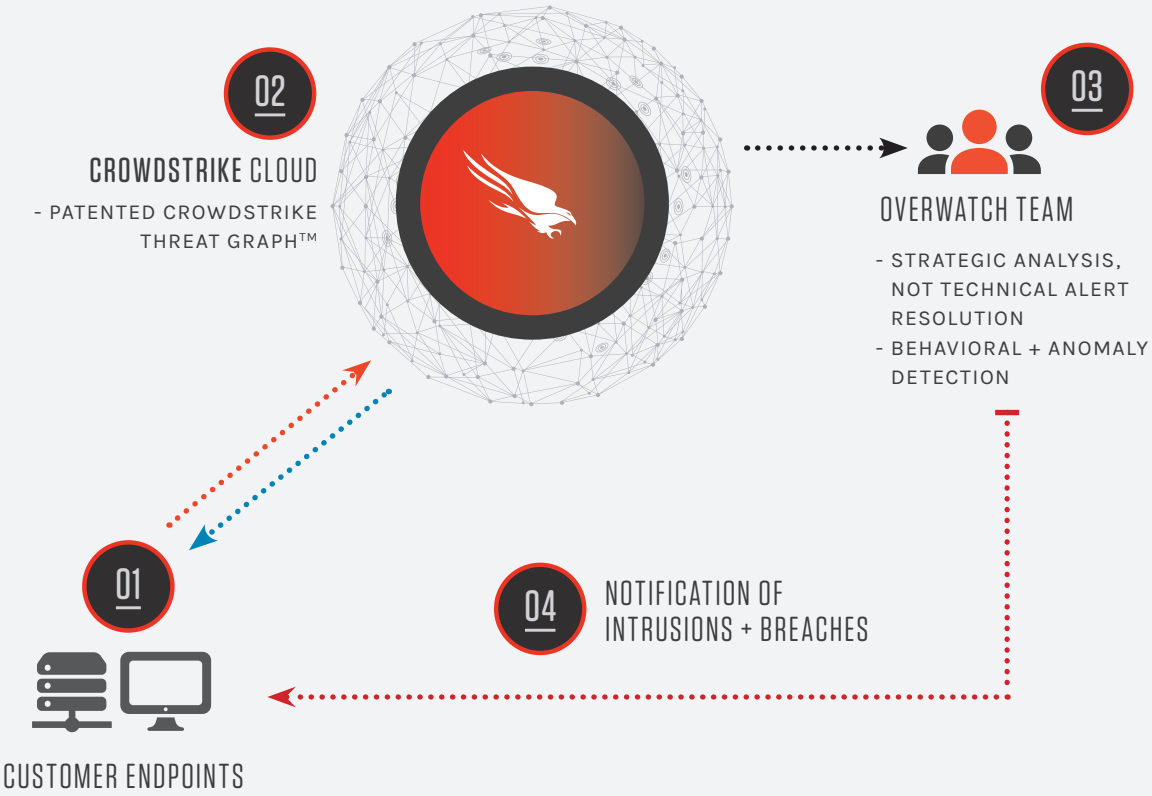

Figure 1: How Falcon Overwatch Works

There are four major elements at work in the Overwatch managed hunting service:

1. Host Sensors: Extremely lightweight (<5MB) Falcon Host sensors capture endpoint events and send relevant data to the CrowdStrike Cloud, where it can be aggregated with crowdsource data and subjected to CrowdStrike Threat Graph analysis, then further examined by the Falcon Overwatch team.

2. CrowdStrike Cloud and CrowdStrike Threat Graph™ Analysis: The CrowdStrike Cloud provides a powerful and highly scalable repository in which to store and analyze information generated by the host sensors. The CrowdStrike Threat Graph correlates these billions of sensor events in real time. The Overwatch team benefits from -- as well as augments -- the capabilities of Threat Graph to draw links between security events across the global Falcon Host sensor community, spotting anomalies that indicate previously unknown and undetectable attacks, whether they use malware or not.

3. Falcon Overwatch Human Intelligence: The Overwatch team performs strategic analysis on the data samples to determine what, if any, adversarial activity is taking place. This means they'll examine the footprints of potential malicious activities within an endpoint or strung across multiple connected assets, and compare those results against threat intelligence throughout CrowdStrike's entire customer base.

4. Notification of Intrusion and Breach: If a possible attack or breach is confirmed, the Overwatch team notifies the customer immediately, providing detailed and actionable information rather than simply generating a standard tactical alert -- the type of perfunctory response you'd expect from an automated system.

All of these elements work together to achieve the fastest, most accurate and comprehensive response to stealthy attacks that typically elude traditional automated, malware-centric security analysis. The synergy between CrowdStrike's advanced technology, coupled with some of the world's most skilled and experienced cyber threat hunters, provides Overwatch customers with a strategic advantage in the fight to detect determined adversaries and prevent a mega breach.

> "We only have highly experienced analysts -- and their expertise comes from years of experience in threat intelligence, malware analysis, and deep network and endpoint analysis and forensics."
>
> -- CHRISTOPHER WITTER, Manager, Falcon Overwatch

Falcon Overwatch in Action

Here's what a typical Overwatch analysis might look like in action:

1. The Falcon Overwatch hunters are alerted by triggers that could potentially indicate malicious behavior. It could be a detection that has too low a level of criticality for Falcon Host to act on independently, such as a firewall being disabled. This behavior could be a standard practice used by an administrator to temporarily get a job done, or it could be an adversary carrying out an attack. By tracking the context, the Overwatch team can understand whether it's an adversary or a legitimate user.

2. Based on that trigger, Overwatch will conduct an in-depth forensic analysis. For example, they will examine how many times that action took place in the entire environment. In this example, if it was run by 450 out of 500 machines, then the likelihood is high that it was normal administrative behavior. But if it was run on only a handful of machines, Overwatch hunters might dig further.

3. At that point, Overwatch analysts might also look into the "ancestry" of the activity. This could involve examining the main process that triggered the detection, and looking up a level to see what system process initiated that activity, to find indications as to whether it was a standard process or something that looks suspicious. If it does appear potentially malicious, they'll keep moving up the chain of activity to find the initial point of origin.

4. If it was a malicious file at the heart of the activity, the team will start dissecting it to see what other behaviors might be associated, whether it involves password or credential dumping, or something more complex. The team will gather a full spectrum of information about the attack, including time of day and conditions when it was executed, and compare that against data pulled from CrowdStrike's entire threat intelligence data pool. That data is then compiled into a comprehensive report that is sent both to the customer's Falcon Host dashboard and via an alert email direct to the customer's security team.

Customers utilizing Overwatch benefit greatly from the comprehensive analysis, speed and agility offered by managed hunting. These benefits include:

- Faster reaction time and reduced "dwell time" for threats
- Reduced alert fatigue
- Detection of malware-free attacks and other sophisticated stealth techniques
- Cutting-edge defense without the cost or the difficulty of assembling and operating an in-house proactive hunting team

The benefits of Falcon Overwatch not only apply to organizations with small teams, or those with limited proactive hunting skills and experience, but also to larger mature organizations looking for extra capabilities and skilled personnel to augment their existing SOC and incident response teams.

Here are some additional examples of how Overwatch has delivered.

Breaking the Pen Test

In one very large financial organization, a security team reported that a Falcon Overwatch alert allowed them to shut down a particularly pernicious attack within minutes. In the report sent to the customer, the Falcon Overwatch team noted that the attack looked like it could have been part of a penetration test. However, the security team hadn't been informed of any such test and immediately took action to remediate. They later learned that the attack actually had come from a penetration test -- one that had been ordered by upper-level executives to test the mettle of their security investments. The penetration testing firm reported not only that the Overwatch response ranked among the fastest detections they had ever encountered, but also that they had never before been so thoroughly locked out of an environment.

Keeping Ongoing Attacks at Bay

In this instance, CrowdStrike was working with a customer that had been plagued by a persistent adversary that continued to repeatedly probe and attack some of the organization’s most valuable IT assets. The customer’s small and inexperienced security team came to depend on Overwatch to provide visibility and notify them each time the adversary attacked a new server or network asset. Over a period of many months, Overwatch has been able to help the customer escalate remediation, adapt defensive capabilities and keep attackers locked out of prioritized assets on a continuous basis.

Making Sure Isolated Incidents Stay Isolated

In another incident, a multinational firm experienced an attack on assets in Europe. The attack itself occurred on Christmas Day, while many of the firm's security team members were on vacation. Investigations showed that the new attack came as a result of adversaries using credentials stolen during a previous attack, which took place many months earlier against a different division of the firm based in Asia. The Overwatch team spotted malicious lateral movement as attackers used those initial credentials to dump more passwords and bring additional tools into the environment to further compromise machines within the European network. The Overwatch team was able to gather all of the necessary information the customer needed to block the attack and take affected machines offline for further forensic analysis.

> "It's really the complete package that CrowdStrike brings to a company like ours that amplifies the value," says Brian Kelly, CSO for Rackspace (NYSE: RAX), a $2.9B managed cloud provider. "They're with you at 3 o'clock in the morning, they're subject matter experts around all topics -- forensics analysis, incident response, technology, root cause analysis. It's just everything together that makes this something unique, and a key part of my strategy going forward."

Conclusion

The frequency of mega breaches continues to rise at an alarming rate. While an initial compromise can take place within a matter of minutes, the average time it takes for organizations to detect attackers on a given endpoint or network currently stands at seven to eight months.[6] The results are self-evident: Mega breaches involving tens of millions of customer records have become commonplace, along with reports of intellectual property thefts that can severely impact competitiveness and threaten an organization's future revenue.

Many of these breaches could be prevented by deploying next-generation endpoint protection technology in concert with an aggressive proactive hunting strategy. This potent combination is by far the most effective means of defending against advanced adversaries -- adversaries that Robert M. Lee of the SANS Institute defines as having the "ability to understand the target, have consistency across their actions and possess the logistics and coordination to carry out long-term campaigns."

Such adversaries cannot be controlled by simply deploying technology, regardless of how advanced it may be. By pitting elite analysts against these adversaries to proactively hunt for malicious activity in their environment, organizations can finally level the playing field and protect their most precious assets. Fortunately, this can be accomplished quickly and affordably by taking advantage of the managed hunting services offered by CrowdStrike Overwatch. With Overwatch on their team, organizations can significantly increase their odds of avoiding a mega breach.

To learn more about how Overwatch can help your organization meet threats head-on, visit https://www.crowdstrike.com/products/falcon-overwatch

ABOUT **CROWDSTRIKE**

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. CrowdStrike's core technology, the CrowdStrike Falcon™ platform, stops breaches by preventing and responding to all attack types – both malware and malware-free.

CrowdStrike has revolutionized endpoint protection by being the first and only company to unify three crucial elements: next-generation AV, endpoint detection and response (EDR), and a 24/7 managed hunting service — all powered by intelligence and uniquely delivered via the cloud in a single integrated solution.

Falcon uses the patent-pending CrowdStrike Threat Graph™ to analyze and correlate billions of events in real time, providing complete protection and five-second visibility across all endpoints. Many of the world's largest organizations already put their trust in CrowdStrike, including three of the 10 largest global companies by revenue, five of the 10 largest financial institutions, three of the top 10 health care providers, and three of the top 10 energy companies. CrowdStrike Falcon is currently deployed in more than 176 countries.

We Stop Breaches. Learn more: **www.crowdstrike.com**

[1] http://www.gartner.com/newsroom/id/3404817

[2] http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#627a0da72191

[3] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[4] http://www.darkreading.com/vulnerabilities---threats/poor-priorities-lack-of-resources-put-enterprises-at-risk-security-pros-say/d/d-id/1321308

[5] http://www.securityweek.com/incident-response-becoming-more-difficult-survey

[6] https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094wwen/SEL03094WWEN.PDF

[7] http://www.ciosummits.com/Online_Assets_Intel_Security_Gartner.pdf

[8] http://www.infoworld.com/article/2980341/security/for-discerning-hackers-malware-is-so-last-year.html

[9] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

[10] http://www.eweek.com/security/businesses-see-sharp-rise-in-targeted-attacks.html

[11] http://www.boozallen.com/insights/2013/03/cyber-hunting-proactively-track-anomalies-to-inform-risk-decisions

[12] https://www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785

[13] https://www.sans.org/reading-room/whitepapers/analyst/threat-hunting-open-season-adversary-36882

[14] http://blogs.gartner.com/anton-chuvakin/2016/03/21/antons-favorite-threat-hunting-links/

[15] http://www.networkworld.com/article/2687381/cisco-subnet/more-data-on-the-cybersecurity-skills-shortage.html

CROWDSTRIKE

crowdstrike.com

15440 Laguna Canyon Road, Suite 250, Irvine, CA 92618

VER. 09.13.16