code42

CROWDSTRIKE

CASE STUDY

CrowdStrike and Code42 vs. External Threat and Insider Risk

CrowdStrike is a cybersecurity company that provides cloud-based endpoint and workload protection against cyberattacks.

INDUSTRY	HEADQUARTERS	NUMBER OF EMPLOYEES	GLOBAL REACH
Technology	Sunnyvale, CA	1,683	13 offices across 7 countries

After working on security teams at large retail organizations, I'm now in the unique, and fortunate, position to be the Principal Security Researcher and Engineer at Code42, an organization that makes one of the products that my team uses daily. This gives us direct access to Code42's latest product features, beta testing, and the opportunity to network with organizations like CrowdStrike both as peers and as customers of each other's products.

Code42's Incydr solution is an incredibly helpful tool to have in the toolkit. I'm proud of how my company is innovating to help fill a critical need in data security, particularly around protecting data from Insider Risk. But as any savvy security professional knows, there's no one silver bullet to address all of an organization's data security needs. For this, I rely on different products to protect Code42's data from an ever-present array of threats.

One of the key solutions we use at Code42 is CrowdStrike's Falcon, the fastest-growing endpoint detection and response solution on the market. Some of the things I love about CrowdStrike are its high-fidelity rate and its low rate of false positives; how it has a lot of searchable, granular event data; and its Falcon OverWatch service, which provides a "second set of eyes" to alert us to unusual activity in our environment.

CrowdStrike and Code42 work shoulder-to-shoulder to protect our data. Falcon protects our organizations from external threats such as malware, while Incydr accelerates our detection of and response to Insider Risk, like departing employees taking company IP.

As you can tell, I'm a huge advocate for CrowdStrike, which made it particularly cool to meet with Tim Briggs, CrowdStrike's director of incident response and eDiscovery investigations, at our Evolution19 conference in Denver. I learned a lot from

Tim, and even got a few tips from the trenches about how he uses Code42 and CrowdStrike in their environment. For example, Tim shared a story about a recent incident when their security team received an alert from Falcon that was related to torrent activity in their system. Torrent activity could be extremely malicious, in that an employee may be exfiltrating valuable IP, or it could simply mean an employee was misusing company assets.

With the alert in hand, the CrowdStrike security team was able to use Incydr to look at the files and download the history of the employee in question. They quickly figured out that the employee was downloading movies onto their device. With that context, the CrowdStrike team was able to ascertain that while the employee was misusing company assets, he wasn't behaving maliciously or exfiltrating data. The security team was then able to report that to their executive team.

While the threat landscape is in a constant state of flux, two things will never change. Breaches will happen, and employees will take data when they leave. It is that simple. Together, CrowdStrike and Code42 are dedicated to making it faster and easier for our respective customers to detect and respond to insider and external threats.

UPDATE: WITH HOW MUCH HAS CHANGED IN THE WORLD OF WORK IN 2020, I RECONNECTED WITH TIM TO DISCUSS HOW HIS USAGE OF CROWDSTRIKE'S FALCON IN TANDEM WITH CODE42'S INCYDR HAS EVOLVED. HERE ARE HIS RESPONSES:

How do you use Falcon and Incydr together today?

"We use Falcon to alert us to threats from outside our organization and to potentially risky exfiltration events, and Incydr gives us the details we need to verify what's actually happening within our organization so we can investigate and respond with confidence. To put it simply, Falcon alerts on an event and Incydr has proof of the files involved."

Something we've found really important and should really be best practice for anyone working in Insider Risk – is having multiple sources of information so you can verify what has happened and understand the details of each event. When you're dealing with Insider Risk, a lot of these incidents may not be intentional or malicious, but they can still affect someone's life in a very serious way. It's critical that you verify that an alert reflects what actually happened and that you have validation to back up what you're seeing and help you determine the next steps."

> "CrowdStrike and Code42 work shoulder-to-shoulder to protect our data. Falcon protects our organizations from external threats such as malware, while Incydr accelerates our detection of and response to Insider Risk, like departing employees taking company IP."
>
> - Nathan Hunstad, Principal Security Researcher & Engineer, Code42

CASE STUDY

What’s your favorite part of using CrowdStrike Falcon and Code42 Incydr together?

“Both solutions are so simple to use – it’s clear that simplification is a priority in both tools and it really pays off. I’ve used nearly every DLP solution out there and they’re often so complex, they make your life harder, not easier. But Falcon and Incydr work really nicely together so you can figure out what’s happening very quickly and respond right away.

For example, if we have an employee leaving the organization, we can make sure they’re in the Incydr Departing Employee Lens to monitor file movement closely. From there it’s easy for us to jump into Falcon and block USB ports or take other necessary steps to protect our data if we identify something suspicious. The ease of use is great on its own, but where it really helps is with enabling our team to work faster. Employees can get up to speed really quickly and jump right in without needing a whole lot of training on using the tools.”

From our latest conversation with Tim, it’s clear that an evolving Insider Risk landscape hasn’t slowed his team down. From their powerful tech stack to their understanding of the human side of Insider Risk, they’re well set up to continue detecting Insider Risk and determining the right-sized response as fast as ever.

About Code42

Code42 is the Insider Risk Management leader. Native to the cloud, the Code42® Incydr™ solution rapidly detects data loss, leak and theft as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. The Code42© Instructor™ solution helps enterprises rapidly mature their Insider Risk Management programs by incorporating holistic, hyper-relevant Insider Risk education for end-users to reduce risk events due to accidental and negligent behavior.

With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, the Code42 Incydr solution is FedRAMP authorized and can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and is backed by Accel Partners, JMI Equity, NewView Capital and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America’s best workplaces in 2020 and 2021. For more information, visit code42.com or join the conversation on our blog, LinkedIn, Twitter and YouTube.

Corporate Headquarters
100 Washington Avenue South,
Minneapolis, MN 55401
612.333.4242

Code42.com

CS2107281