sixgill

Empowering security teams with an agile threat intelligence methodology for the modern threatscape.

Continuous Investigations/Continuous Protection™ (CI/CP)

The only way for today's security teams to effectively manage the huge amount of data points they need to digest is by implementing a modern methodology, which is continuous, fast, iterative and smart. The cornerstone of the CI/CP framework lies in quickly and intuitively connecting the dots between a singular tactical incident and the broader strategic landscape.

Sixgill pioneers the Continuous Investigations /Continuous ProtectionTM (CI/CP) approach to security. CI/CP uses automation tools that empower security teams to collect, analyze, research, and respond after each intel development as seamlessly as possible. Focusing on maximum security readiness at any given time, Continuous Protection naturally leads to Continuous Investigation.

Real-time

Real-time collection that enriches your data lake and enables swift response.

Contextual

Any data point is processed, structured and correlated with other data sets in order to connect the dots and complete the bigger picture.

Provides synergistic value

Any data point that is collected is processed, structured and correlated with other data sets in order to connect the dots and complete the bigger intelligence picture.

Iterative and continuous

Gain a full-cycle of agile responses as soon as a new data point reaches the data lake, trigger the appropriate response, rinse, and repeat with new insights.

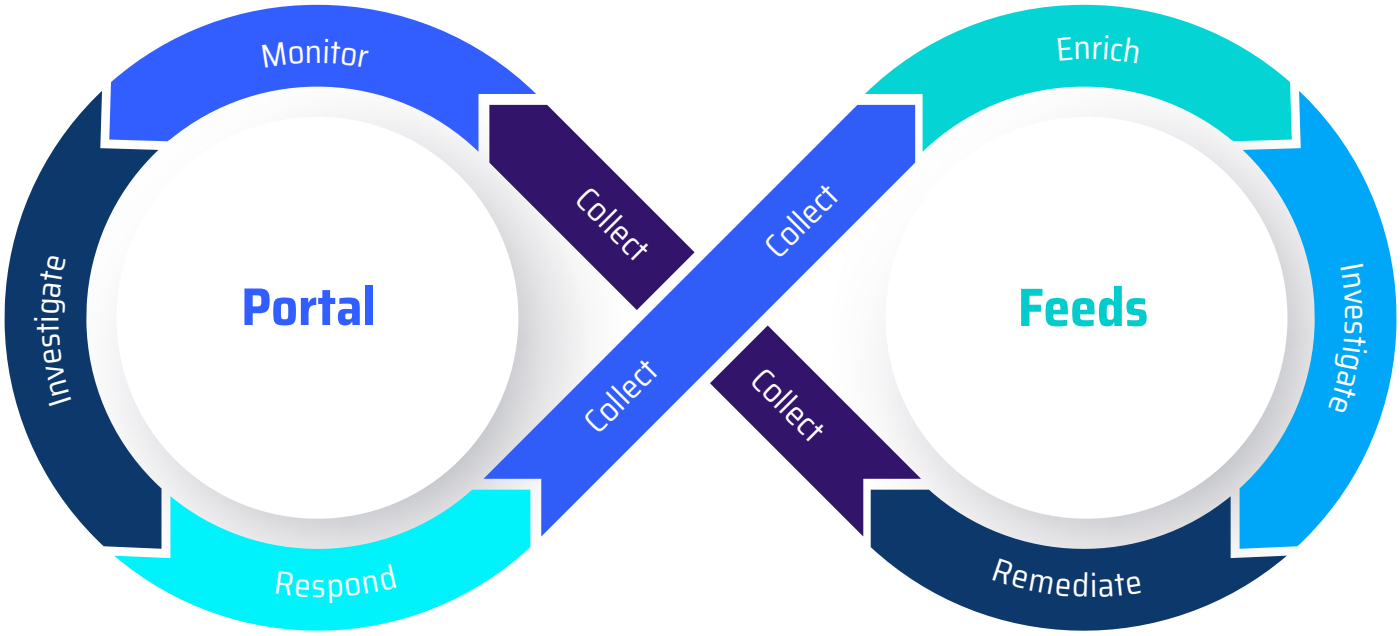
Visibility into a threat actor's mindset

Better understand a threat actor's mindset; from connections, through expertise, all the way to what motivates them.

Seamless protection

With CI/CP, security teams are constantly and proactively responding to the most updated intelligence picture, generating fresh, relevant intel.

Continuous Investigations/Continuous Protection™ (CI/CP)



Advantages

Nothing is faster than real-time

Real-time collection that enriches your data lake. In order to support a continuous CI/CP process, you must ensure there is a continuous stream of valuable data from the darkest corners of the underground. It is vital that these collection mechanisms be agile enough to seamlessly adjust themselves to the changing nature of the threat actors' ways of communications.

CI/CP is all about context

Data, even in a raw form, is never collected in a vacuum. Every IP has a "story". Every post has an author. Every product that is sold on the dark web has a customer base. These details matter when you want to create CI/CP driven processes. Any data point that is being collected should be processed, structured and correlated with other data sets in order to connect the dots and complete the bigger picture.

Provides synergistic value

When implementing CI/CP, you have to make sure that the data enables you to respond seamlessly with each intel development. CI/CP advocates integrating threat intelligence feeds with your security platform- - whether it is a SIEM, SOAR, EPP or VM - in a way that every meaningful data point will trigger an action on your end to mitigate the threat.

Iterative and continuous

Implementing CI/CP driven threat intelligence processes empowers you to have a full cycle of agile responses . As soon as a new data point reaches the data lake, it is pushed to your security platform and is correlated with other indicators you already have. The data is aggregated, and the appropriate playbooks are triggered. After preventing the initial threat, you should now circle back to the data point that triggered the incident and thoroughly investigate it to understand the causes of the incident, and take actions to improve your security posture. CI/CP leverages an investigative portal that allows you to effortlessly deep dive, slice and dice the data and accelerate time-to-insights.

Visibility into a threat actor's mindset.

By implementing CI/CP, security teams can better understand a threat actor's mindset; from connections, through expertise, all the way to what motivates them. This deep understanding of threat actors' M.O.s enables security teams to better anticipate, intercept and respond to incoming threats.

An investigative portal should enable you to discover:

- If they are a human or a Bot
- Expertise - Are they a script-kiddie, a novice, or a pro
- What tools they use
- Related IPs and Domains
- TTPs
- Targets - Financial organizations, healthcare, gaming, federal entities
- Trends in references - Timeline reference analysis
- Social network - Who are their friends, co-workers, rivals
- Motivations - Is it money, ideology, or state-directive
- Contact information

Seamless protection

Implementing CI/CP threat intelligence means teams are constantly and proactively responding to the most updated intelligence picture, generating fresh, relevant intel to take incident detection, prevention and response to the next level, with minimum business interruption, breaking security silos and maximizing performance of security teams, platforms and processes.

The world is shifting left. It's time threat intelligence does the same.

Sixgill's fully automated threat intelligence solutions help organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response - in real-time. Sixgill's investigative portal empowers security teams with contextual and actionable alerts along with the ability to conduct real-time, covert investigations. Rich intelligence streams such as DarkfeedTM harness Sixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems to help proactively block threats before they are deployed in the wild. Current customers include enterprises, financial services, MSSPs, government and law enforcement entities.

SECURITY We treat security of data with the highest standards. Sixgill's security-first approach leverages the best and most advanced technologies to make sure that your data stays safe and private. Our service undergoes rigorous audits and employs the latest best practices to ensure the integrity of the data as well as its authenticity, security and compliance.

sixgill

Sixgill is a fully automated threat intelligence solution that helps organizations protect their critical assets, reduce fraud and data breaches, protect their brand and minimize attack surface. The portal empowers security teams with contextual and actionable alerts as well as the ability to conduct real-time investigations. Rich intelligence streams such as Darkfeed harness Sixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems to help proactively block threats. Current customers include enterprises, financial services, MSSPs, government and law enforcement entities.

www.cybersixgill.com