bfore.ai

Case Study

PreEmpt Active Defense

How Bfore.Ai helped a leading investment firm stop an attack in under seven minutes

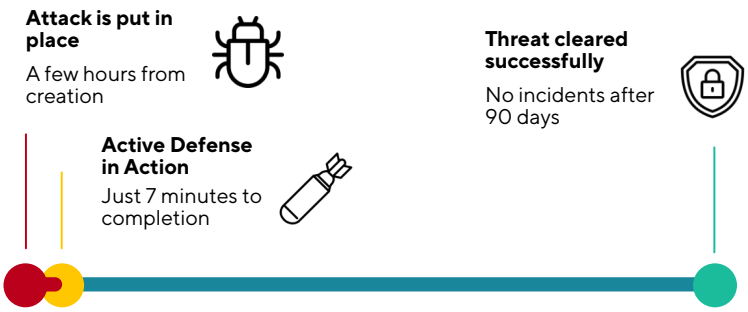
A global financial services firm specializing in institutional trading, investment banking, research and related brokerage services stopped an attack in its tracks with PreEmpt Active Defense

The challenge

In 2022, the CISO of the firm was alerted to the presence of an expertly engineered spear phishing impersonation domain.

"When our team was alerted to this domain, we viewed it as a ticking time bomb," the CISO said. "It was clear that these criminals had done serious homework. The illusion of legitimacy they'd conjured up was extremely compelling–if we weren't able to shut the threat down immediately, it could have been a crisis situation potentially costing the firm upwards of $200k."

Remediation Timeline



> *"...a crisis situation potentially costing the firm upwards of $200k"*
>
> *Chief Information Security Officer*

Book a demo now - sales@bfore.ai

bfore.ai

The solution

Due to Bfore.Ai's reputation, the CISO reached out for help with domain takedown. It took Bfore.Ai's team seven minutes from being alerted to neutralize and take down the domain–exponentially quicker than the industry average of 72 hours.

> *"I was utterly blown away... PreEmpt Active Defense and PreCrime Brand were clearly the leading solutions for anticipating and eliminating threats in the fastest possible way."*
>
> *Chief Information Security Officer*

"I don't know which was bigger, my disbelief or relief at how quickly Bfore.Ai was able to resolve this issue–I was utterly blown away," the CISO added. "We were considering different partners to help us automate aspects of our cybersecurity process, but the results Bfore.Ai gave won us over immediately. We realized straightaway that PreEmpt Active Defense and PreCrime Brand were clearly the leading solutions for anticipating and eliminating threats in the fastest possible way."

The results

Bfore.Ai PreEmpt Active Defense now handles all evidence collection, request follow up, domain disabling, outreach and documentation of every process step. This is followed by 90-days of monitoring to ensure no mistaken domain reactivation. The solution has yielded $1.5 million monthly savings due to proactive threat neutralization and has freed up 20 hours a week that the infosec team can now dedicate to other high-value initiatives.

Impact in metrics

10%
Workload reduction for CISO team

60%
Increase in threat identification

98%
Reduction in false alerts