CounterTack®

CounterTack Case Study

Cyber Security Provider Case Study

COMPANY PROFILE:
Asia's Leading Cyber Security Provider

HEADQUARTERS:
Singapore

EMPLOYEES:
Over 26,000

OBJECTIVE:
Detect highly sophisticated cyber-attacks and provide rapid incident response

SOLUTION:
Countertack Active Defense™ and Responder® PRO with Digital DNA®

KEY BENEFIT:
"Responder PRO allows us to determine quickly if a certain host has been compromised and begin the process of reverse engineering."

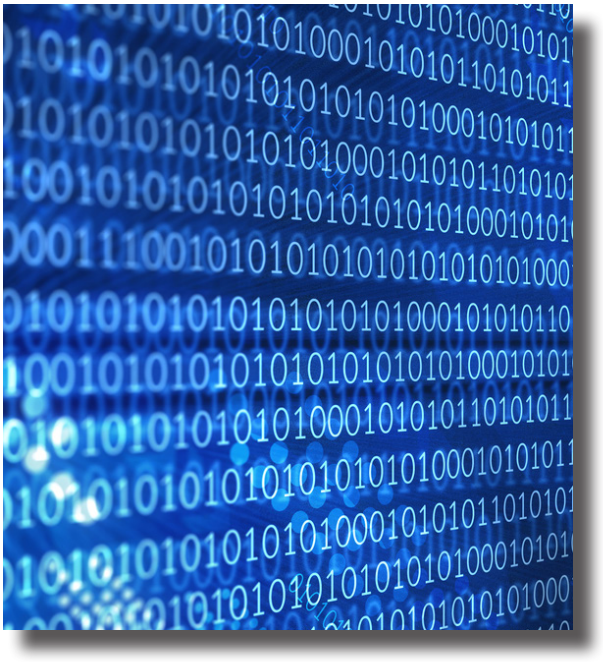
"CounterTack's product support is one of the best we have experienced – Any support required, from technical training to troubleshooting of issues, was efficiently attended to."

"WITH COUNTERTACK, OUR INCIDENT RESPONDERS ARE EMPOWERED TO REACT RAPIDLY AND QUICKLY FIND ANSWERS TO SECURITY INCIDENTS."

SECURITY CHALLENGE:
The security provider needed a comprehensive solution to quickly analyze and respond to security incidents they deemed as advanced persistent threats across multiple sites including remote locations.

DEPLOYMENT:
Incident handlers were equipped with Responder PRO and Digital DNA. Active Defense was used for emergency deployment when traveling to the remote site was not possible.

APT SOLUTION SELECTION PROCESS:
The key challenge was minimizing the time required for a small team of incident handlers to triage incidents. Given the nature of the threat, rapid triaging was required as there was a potential risk of multiple incidents happening before a full response could be administered. Digital DNA reduced the triage time while memory analysis of suspected hosts aided incident responders. The console of Responder PRO showed disassembled suspicious files making it extremely convenient to work on cases. Active Defense provided remote data extraction to facilitate urgent responses.



Cyber Security Provider Case Study

"Digital DNA allowed us to zoom into suspicious artifacts quickly and gave us an independent assessment of them so that our incident handlers could grasp the situation quickly."

WHY ACTIVE DEFENSE WITH DIGITAL DNA?

PRODUCT TRAINING AND SUPPORT:

CounterTack's Advanced Malware Analysis training class provides organizations an opportunity to analyze real malware in memory using Responder® PRO to strengthen their forensic skills. Common malware is used to replicate realistic everyday situations.

ACTIVE DEFENSE WITH DIGITAL DNA:

Active Defense is powered by CounterTack's patented Digital DNA® technology that identifies specific behavioral traits of every process running in memory. Digital DNA has been proven to help security teams detect a large variety of new malware including zero-days, rootkits, and targeted attacks that signature-based methods simply cannot.

RESPONDER PRO WITH DIGITAL DNA:

Responder PRO, with patented Digital DNA, automatically reverse engineers all code in memory and examines it for potentially malicious capabilities. Observed behavioral traits are matched against CounterTack's Malware Genome database to classify digital objects as good, bad or neutral. Rules and Weighting are applied to compute the overall severity score, which is presented as part of a comprehensive threat profile.

CounterTack®

100 5th Ave, First Floor
Waltham, MA 02451-1208
855.893.5428
www.countertack.com