CrowdStrike Services

CROWDSTRIKE

REDUCING LOSSES RELATED TO CYBER CLAIMS

The need for speed in endpoint recovery and forensic investigation

STOPPING BREACHES IS CROWDSTRIKE'S FOCUS

The CrowdStrike® Services team is at its strongest when investigating advanced persistent threats by leveraging a combination of highly skilled forensic consultants, in-depth threat intelligence and exceptional technology. This approach allows the Services team to efficiently investigate and contain large-scale attacks across highly distributed enterprises.

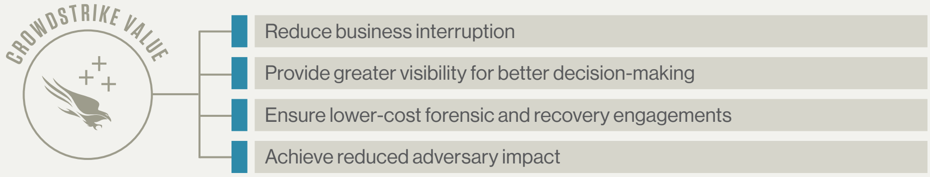
CrowdStrike responds to and protects your clients with the utmost expertise and professionalism, ensuring ease of engagement and speed to visibility and containment, with the goal of returning your client to "business as usual" as quickly as possible. The Services team strives to reduce the duration and manage the cost of forensic and recovery engagements with speed and precision.

TRADITIONAL INCIDENT RESPONSE (IR) APPROACH

MANY DAYS	WEEKS	MONTHS
• Ship servers • Load software • Fly in consultants	• Run system scan (single snapshot) • Analyze results • Repeat until activity is seen	• Plug holes as they are found • Rerun scans to look for more activity • Analyze additional scans and plug holes • Repeat until consultant feels there is no more activity

CROWDSTRIKE APPROACH

HOURS	HOURS	DAYS/WEEKS
• Deploy cloud-based sensors	• Conduct computer and human analysis of real-time activity	• Identify/contain adversary • Remove adversary access • Analyze forensic artifacts • Plug holes



Reduce business interruption

Provide greater visibility for better decision-making

Ensure lower-cost forensic and recovery engagements

Achieve reduced adversary impact

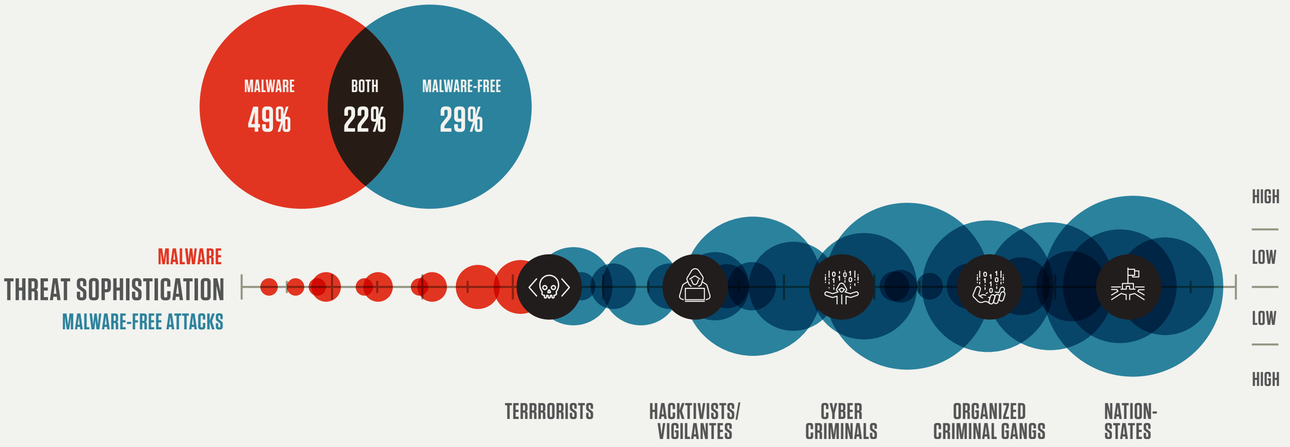
WHY CHOOSE CROWDSTRIKE?

SPEED OF DEPLOYMENT: The CrowdStrike Falcon® platform leverages cloud-based technology to deploy endpoint sensors to gain visibility across your client's entire network within hours. Other vendors can take days or weeks to ship servers, load software and fly in consultants.

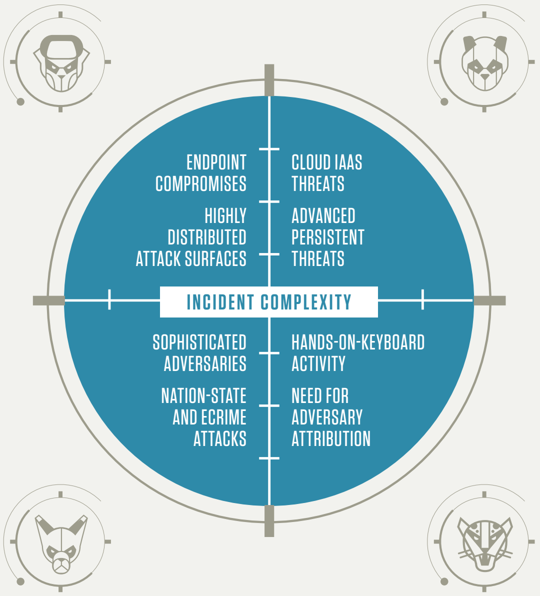
REAL-TIME VISIBILITY: The sensors provide real-time visibility of activity within the environment, allowing the CrowdStrike Services team to detect, analyze and contain adversary activity far faster than the traditional approach of analyzing a scan (a single snapshot in time) of the environment.

INTELLIGENCE-LED REMEDIATION: Threat intelligence powers everything CrowdStrike does. The Services team is able to immediately analyze indicators of attack (IOAs), enabling it to identify the adversaries and anticipate their next move. This information helps the team quickly expel the adversary.

THE RIGHT TEAM, TOOLS AND APPROACH TO ADDRESS THE MOST SOPHISTICATED BREACHES



WORLDS MOST ADVANCED CLOUD-NATIVE PLATFORM	GROUND BREAKING THREAT INTELLIGENCE	POWERED BY THE CROWDSTRIKE SECURITY CLOUD	WORLDS LARGEST UNIFIED, THREAT-CENTRIC DATA FABRIC	POWERING THE NEXT GENERATION OF PROTECTION AND THREAT HUNTING


ENDPOINT COMPROMISES
CLOUD IAAS THREATS
HIGHLY DISTRIBUTED ATTACK SURFACES
ADVANCED PERSISTENT THREATS
INCIDENT COMPLEXITY
SOPHISTICATED ADVERSARIES
HANDS-ON-KEYBOARD ACTIVITY
NATION-STATE AND ECRIME ATTACKS
NEED FOR ADVERSARY ATTRIBUTION

NATION-STATE ADVERSARIES

- Espionage and theft of intellectual property
- Large-scale and enterprise-wide targeted attacks
- Targeted destructive attacks (e.g., Shamoon, NotPetya, Dustman)

ECRIME ADVERSARIES

- Enterprise-wide, large-scale breaches by eCrime actors such as MUMMY SPIDER, WIZARD SPIDER, INDRIK SPIDER and more
- Highly persistent malware used to gain and sell access, such as Emotet
- Ransomware such as REvil, Ryuk, BitPaymer and DopplePaymer
- Banking Trojans such TrickBot, DanaBot, BokBot and Dridex

CONTACTS

BREACH HOTLINE	GLOBAL	NORTH AMERICA	EMEA	APJ
1-855-276-9347 services@crowdstrike.com	Charlie Groves +1 303 887-0506	Adam Cottini +1 917 797-7510	Marko Polunic +49 1590 440-1631	Paul Byrne +614 3233-2931

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services delivers Incident Response, Technical Assessments, Training, and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks, and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of our Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: **We stop breaches.**

Learn more at **www.crowdstrike.com/services/**
Email: **services@crowdstrike.com**