



CROWDSTRIKE

# CROWDSTRIKE REDUCES LOSSES FOR INSURANCE CARRIERS ON CYBER CLAIMS

When a breach occurs, speed to remediation is critical. CrowdStrike’s incident response (IR) methodology provides many advantages over traditional IR approaches. CrowdStrike gets your clients back to business faster and reduces cyber-related claims:

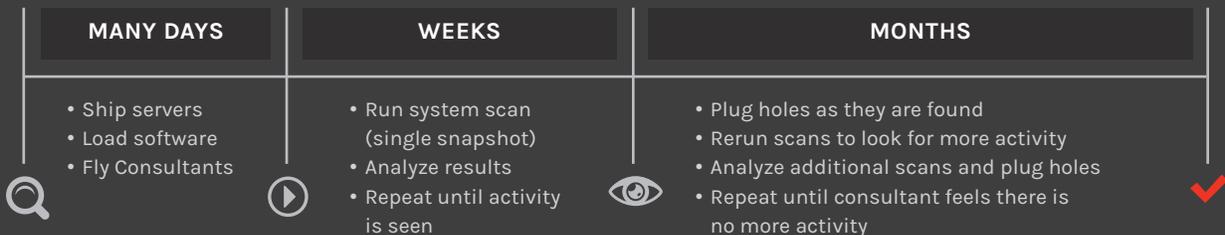
- Faster time to visibility and remediation means less expensive forensic costs
- Reducing business interruption losses by getting your client back to business faster
- Minimizing adversary impact by limiting adversary dwell time

**Speed of deployment:** Our Falcon Platform leverages cloud-based technology to deploy endpoint sensors to gain visibility across the insured’s entire network within hours—other vendors can take days or weeks to ship servers, load software and fly consultants.

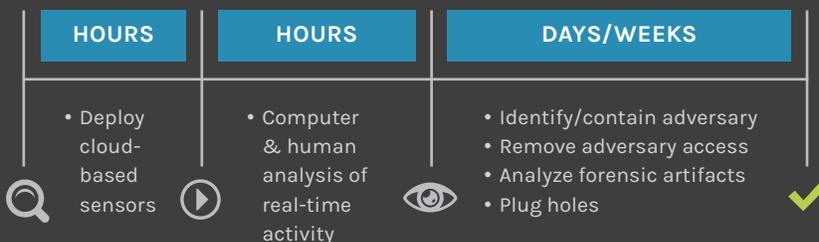
**Real-time visibility:** The sensors provide real-time visibility of activity within the environment, allowing our Professional Services team to detect, analyze and contain adversary activity far faster than the traditional approach of analyzing a scan (snapshot in time) of the environment.

**Intelligence-led remediation:** Threat intelligence powers everything we do at CrowdStrike. Our team is able to immediately analyze indicators of attack, enabling us to identify the adversaries and anticipate their next move. This information helps our team quickly expel the adversary.

## TRADITIONAL IR APPROACH



## CROWDSTRIKE APPROACH



## CROWDSTRIKE VALUE

- Reduce business interruption
- Greater visibility for better decision making
- Less expensive forensic engagement
- Reduced adversary impact

# Case Study:

## EXPELLING THE RUSSIANS — RESPONDING TO THE DNC CYBER CRISIS

CrowdStrike's success on behalf of the Democratic National Committee (DNC) is a perfect example of the speed and expertise of our incident response process.

Our Professional Services team and the DNC had complete visibility across the DNC's environment within hours. Armed with critical information, the client was able to make key decisions and drive a coherent strategy for crisis management.

By leveraging our deep intelligence on adversary groups, we were able to identify and attribute the intrusion to specific Russian adversaries: COZY BEAR and FANCY BEAR. Our knowledge of the adversaries' attack patterns allowed us to quickly identify, contain and expel them from the DNC's environment.

### CERTIFICATION AND ACCREDITATION

External validation and accreditation is critically important as organizations assess providers to secure their technical environments. Our Professional Services team is one of the few in the security consulting industry to attain such certifications:

- CrowdStrike is one of 12 organizations that is PFI-certified by the PCI Security Standards Council to provide investigative services in the U.S.
- CrowdStrike is one of 12 organizations accredited by the National Security Agency for National Security Cyber Assistance Program (NSCAP) Cyber Incident Response Assistance (CIRA).
- Additional compliance, certification and attestation information is available for review at [www.crowdstrike.com/services/compliance/](http://www.crowdstrike.com/services/compliance/)

### ABOUT CROWDSTRIKE

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. Our Professional Services team has worked on some of the largest, most publicized and challenging cyber intrusion incidents within the last few years. The world's largest organizations trust CrowdStrike to stop breaches, including three of the 10 largest global companies by revenue. CrowdStrike Falcon Host is deployed in 176 countries around the globe.

### LEARN HOW CROWDSTRIKE STOPS BREACHES:

Learn how CrowdStrike Services can help your organization reduce costs associated with cyber incidents.

Phone: (303) 887-0506 | Email: [Charlie.Groves@CrowdStrike.com](mailto:Charlie.Groves@CrowdStrike.com)

[www.crowdstrike.com/services](http://www.crowdstrike.com/services)