CYBERFORCE|Q

Phishing & Security Operations

Collective Cybersecurity - Advancing your Cybersecurity Program

Phishing	16%	$4.90M
is the leading cause of cyber security incidents and ransomware	of breaches in which phishing was the initial attack vector	Average cost of a data breach

Collective Security Operations Center (CoSOC) supports your cybersecurity program with remediation practices.

Phishing Incident Identified and Breach Averted in Less than 1.5 Hours.

An employee observed and reported a phishing attempt that the CyberForce|Q team analyzed and responded to in order to avert a breach. From the moment the client reported the suspicious email, it took CFQ less than 2 minutes to receive the case in their incident management technology. With the automated playbook, checking the email, it was noted as "High" priority. When this was identified as a "High" priority, investigation by our incident handler began. The email was categorized as phishing, and escalated to a Senior Analyst for further investigation. The email was considered malicious and was received by 20 users. The analyst took action and removed the email and blocked traffic from the malicious URL and IP address. Within 1.5 hours the investigation was concluded, and a breach was averted.

Contact Us:

CyberForce|Q
Proven Cybersecurity Program Advancement
(248) 837-1400
solutions@cyberforceq.com

CYBERFORCE|Q

Phishing & Security Operations

With 24x7x365 monitoring, incident response was immediate through CyberForce|Q's vigilant actions

Phishing is the most prevalent attack vector of cyber security incidents and ransomware, threatening risk to the clients' customers, employees, and financial impact.

24x7x365 engagement by our team involves the vigilant and proactive deployment of cutting-edge strategies, tools, and expertise to safeguard digital infrastructures against evolving threats. This specialized practice requires rapid response capabilities, astute analysis, and decisive action to detect, mitigate, and neutralize cyber threats in real-time. It entails hands-on, dynamic engagements where cybersecurity professionals actively confront and counteract imminent risks, fortifying defenses and preserving the integrity, confidentiality, and availability of critical systems and data.

Operating at the forefront of defense, these tactical engagements demand agility, precision, and a comprehensive understanding of emerging threats, ensuring a resilient and secure digital environment.

1.35 Min

average response time to start an alert review in our SOC.

97%

Phishing Noise Filtered Out saving time, money, and resources for these organizations.

24x7

Incident handlers availible for immediate response and forensic investigations.

With collective security operations centers, meaningful measurement, and quantifiable tactics CyberForce|Q provides our clients cybersecurity program advancement.

Contact Us:

CyberForce|Q
Proven Cybersecurity Program Advancement
(248) 837-1400
solutions@cyberforceq.com