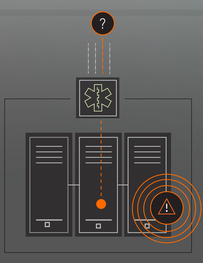
Caught in the Act

HOW ARMOR HELPED A CUSTOMER SLAM THE DOOR ON POTENTIAL DATA EXFILTRATION

1

Alert: Even the stealthiest assault on a customer's network won't go unnoticed by Armor's highly-trained security experts. Case in point: Armor's incident response and forensics (IRF) team detected unusual traffic coming from a healthcare customer.

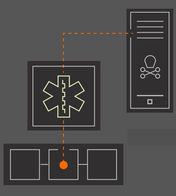


2

Response: Going into reconnaissance mode, the team performed a network packet capture on anomalous traffic. This technique involves capturing packets of data to further analyze for indicators of compromise on the customer's network.

3

Discovery: The team quickly spotted sensitive data being transmitted in clear text to another server on the web, one with no relation to the affected customer. Already warranting immediate action, the need to respond was even more pressing considering highly regulated healthcare data could have been exposed.



4

Remediation: With a full understanding of the situation, the Armor team alerted the customer of the misconfiguration causing the vulnerability. The customer could act quickly to mitigate any further exposure and risk their compliance posture being negatively impacted.

ATTACK & RESPONSE SUMMARY

ALWAYS WATCHING

ARMOR'S 24/7 SECURITY MONITORING ENSURED THE CUSTOMER COULD RESPOND BEFORE THEIR COMPLIANCE POSTURE WAS AFFECTED.

COLLABORATIVE DEFENSE

ARMOR'S EXPERTS SHARE THE BURDEN OF SECURITY WITH THE CUSTOMER, WORKING AS AN EXTENSION OF THEIR TEAM.

PERFECT TIMING

IF GONE UNNOTICED, THE ATTACK COULD HAVE BEEN FINANCIALLY DEVASTATING. ESPECIALLY CONSIDERING THE AVERAGE DATA BREACH COSTS $4 MILLION.

Your data doesn't belong to them.

WE WON'T LET THEM TAKE IT.

ARMOR™

THE FIRST TOTALLY SECURE CLOUD COMPANY™