CYBRAICS

Sophisticated attacks threaten election board agency

Situation

Limited IT team finds an attack, but can't verify the extent or fully remediate.

As a critical US election agency, our customer had multiple systems in place to help support their limited IT team. A breach was detected and remediated, or so they initially thought. Realizing they could not verify the full extent of the attack, they needed a solution that could provide network-wide visibility. The agency's IT team had to ensure all affected systems and networks were identified and remediated.

Solution

Sophisticated, geographically diverse, concealed attacks are immediately found.

Cybraics' nLighten was quickly deployed and immediately found additional, previously undetected, bad actors inside the agency's network using data from the agency's firewalls and Windows Event logs. Although the bad actors were using sophisticated, geographically diverse threat vectors with multiple IP addresses to conceal their activities, nLighten immediately detected three attacks that were of significant concern. Highly enriched automated cases, with data correlated from multiple log sources, were presented in the nLighten dashboard. The customer utilized the drill-down capabilities to stabilize the threats quickly.

Success

Election integrity secured, limited resources scaled.

The agency's IT team quickly identified and easily remediated previously undetected threats. nLighten proved especially valuable because the <5% false-positive rate allowed the limited IT team to focus their finite resources on actual cases instead of chasing threats. The unparalleled depth of the reports helped them pinpoint a swift resolution to the attacks.

> *We deployed nLighten after the 2016 election because we were concerned about our security systems. nLighten has identified issues, improved our situational awareness and provided us with visibility into threats we normally wouldn't uncover.*