red canary

CASE STUDY

Outsourcing Security in the Defense Industrial Base

Industry

Defense Industrial Base

Security Challenge

Customer is a lean, onsite government contractor and needed advanced information security that minimally increased overhead costs.

Solution

Red Canary's Endpoint Detection and Response Solution

Key Benefits

- *Extensive threat detection.* Red Canary records all endpoint activity and automatically hunts for threats – from malware to advanced multi-stage targeted attacks.
- *Human expertise.* Red Canary's team acts as an extension of the customer: endpoint threat detection, false positive removal, and endpoint product management.
- *Breakthrough economics.* Approximately the same cost as health insurance premiums paid for one employee.

Summary

An onsite government contractor with limited infrastructure and staff needed additional security that minimally impacted overhead costs. The organization deployed Red Canary's managed endpoint threat detection and response service to ensure comprehensive detection that did not require additional staffing.

The Problem

The Defense Industrial Base (DIB) contractor managed a modest unclassified infrastructure environment with one System Administrator. The organization protected itself with Anti-Virus and a Firewall, but knew they needed an additional layer of defense to detect threats missed by the traditional tools.

The Solution

Red Canary's endpoint threat detection and response solution drastically increased the organization's security. Red Canary

- Continuously records and monitors all endpoint activity
- Automatically hunts for threats throughout their lifecycle – known and unknown malware, suspicious behavior, lateral movement, escalation of credentials and exfiltration of data
- Staffs its own internal Security Operations Center that confirms threats, removes false positives, and gathers intelligence on threats
- Empowers quick and effective response with automated tooling
- Costs a fraction of what it would cost the organization to build comparable internal security capabilities.

During the past 12 months, Red Canary detected 20 threats that bypassed perimeter security, including crimeware and multiple phishing attacks.

The Red Canary endpoint Security Operations Center removed 1,624 false positive alerts during this time, ensuring the limited resources at the organizations were used effectively.

Interested in learning how Red Canary can help defend your endpoints?
Contact us at info@redcanary.co to schedule a demo.