CASE STUDY Non-Profit Foundation

Partners in Making a Difference: Red Canary Helps a Leading Foundation Safeguard Sensitive Information

CHALLENGE

The Foundation's sensitive work makes it a highly sought-after target. A data breach could not only lead to serious financial ramifications, but also endanger the safety and well-being of the Foundation's employees.

REQUIREMENTS

- Continuous endpoint monitoring, detection, and response to defend against highly targeted attacks and advanced threats
- Broad detection coverage that includes behavioral detection to identify abnormal endpoint and user activity
- The ability to quickly respond to a compromised endpoint regardless of its global location

SOLUTION

Red Canary's Managed Endpoint Detection and Response (MEDR) solution rapidly and accurately identifies attacks on the Foundation's endpoints. The solution combines multiple methods of detection to identify targeted attacks, crimeware, and suspicious activity.

SNAPSHOT

One of the United States' largest private Foundations is a highly sought-after target due to its work in critical causes that can sometimes run contrary to foreign government interests such as eliminating nuclear materials and promoting human rights. When the Foundation was attacked by an advanced threat, its security team worked to bolster the organization's security posture and protect against a similar attack. Red Canary's Managed Endpoint Detection and Response (MEDR) and Carbon Black Response now provide an extra layer of security that enables the Foundation to quickly identify and respond to threats.

DEFENSE IN ACTION

Since deployment, Red Canary has helped to stop a number of attacks that could have resulted in a breach of the Foundation. In one instance, its Indian office was hit by a highly targeted attack on a Friday afternoon. The attack was an email appearing to come from individuals the Foundation was in the process of granting money to. The attackers converted and weaponized a PDF using a unique macro. Red Canary analysts instantly detected the suspicious behavior. They jumped into action, notifying the Foundation's security team and working alongside them to support response efforts. Without Carbon Black and Red Canary, a single targeted attack may have persisted into the weekend, resulting in a breach.

TYPICAL 30-DAY PERFORMANCE

3	confirmed threats detected that bypassed existing protection across 406 endpoints
926	potentially threatening events reviewed and investigated by Red Canary's security analysts
48.8M	processes and unique executables or binaries collected by CB Response and analyzed for threats by Red Canary

red canary

"Red Canary delivers value beyond the specific threat detection and response capabilities we signed up for. It is a partnership that helps our organization improve. Their Technical Account Managers think about things in a broad context and provide us with the intelligence and perspective to prioritize and contextualize threats."

— Chief Information Officer

DIGGING DEEPER

Choosing the Right Technology and Managed Provider

When the Foundation suffered its first breach, the security team initially turned to a leading incident response (IR) firm to address the issue. However, after a thorough analysis of technical capabilities, quality, service, and price, they determined that Carbon Black and Red Canary would provide better security against an attack.

The Chief Information Officer said: "My evaluation gave me full confidence that Carbon Black and Red Canary deliver the best solution from a technical standpoint. Red Canary has proven time and time again they will detect the worst threats we face without ever burdening our organization with false positives. The detection and response service they built on top of Carbon Black is extremely effective, and Red Canary has become one of our closest partners."

Technical Account Services Deliver Value Beyond Threat Detection & Response

Red Canary's Technical Account Managers act as an extension of the Foundation's security team, working side-by-side to:

- Provide support during deployment to ensure seamless integration with the environment's existing security tools
- Understand security objectives and response operations in a broad context
- Support risk assessments and give actionable advice
- Provide guidance on the Foundation's IR plan and day-to-day response operations

Market-Leading Endpoint Detection & Response Technology

The Red Canary solution includes Carbon Black Response, the market's leading endpoint visibility and forensic product. Red Canary analyzes the endpoint data collected by Carbon Black using multiple detection technologies, giving the Foundation coverage against the behaviors commonly used during an attack.

Benefits of a Managed Security Approach

Red Canary helps the Foundation scale its IT and security team by giving them the expertise, tooling, and intelligence they need to contextualize and respond to threats on their endpoints. Over the past year, Red Canary has identified multiple targeted attacks as they progressed and supported the Foundation as they worked to eliminate the threat. Having a third-party to provide intelligence, answer questions, and enable rapid response gives the Foundation the confidence that future attacks will be quickly detected and addressed.