CASE STUDY: MANUFACTURING

Augmenting In-House Expertise with Red Canary's Incident Handlers

BUSINESS ENVIRONMENT

Endpoints:
7,000+

Locations:
40+

IT Security Team:
5 + offshore partners

"I'm looking for a partnership. I want someone who takes an interest in what I do and invests time in knowing my environment. I feel that with Red Canary. The team proactively reaches out to ask me what I want and need so we can look for solutions together. They are driven to provide a high-quality service, and it shows."

— IT Security Leader

The security team at a global manufacturing firm was struggling to secure the company's infrastructure and IP against advanced internal and external threats. The firm produced highly innovative products and constantly faced the threat of attackers attempting to steal their IP.

The IT security leader (we'll call him Henry) oversaw a team of four security practitioners that had recently joined the security field. The team was responsible for managing security operations and controls, setting and enforcing policies, monitoring activity, and responding to threats.

Even though Henry had a solid team of four, he struggled to find the additional security experts he needed to defend his organization. The company was headquartered in a region with a shortage of cybersecurity professionals—and even if Henry could locate the right expertise, his budget would not accommodate the high salary such roles would require.

PARTNERING TO MAKE SECURITY BETTER

Henry's biggest priority was to improve his team's ability to simplify and expedite incident response. The existing IR solution (Mandiant and FireEye HX) continually missed threats and rarely provided sufficient information for a decision to be made. After receiving a recommendation to look at Red Canary, Henry ran a Proof of Concept (POC) for Red Canary and two competitors.

Several qualities led Henry to decide that Red Canary was the best partner. In addition to the thorough hunting and investigation performed by Red Canary, Henry was impressed by Red Canary's incident handling team. Red Canary was the only solution to include access to dedicated security experts as part of its core service.

red canary

"Usually when you buy a product, you're either doing it all by yourself or hiring a professional service to help with implementation, configuration, and training. Not only did Red Canary provide hands-on training for my staff, but anytime I send an email for any reason, a bunch of people jump on it right away. I've never seen that kind of attention and expertise."

— IT Security Leader

AUGMENTING IN-HOUSE EXPERTISE

As a Red Canary customer, Henry was able to tap into the incident handling team to gain the expertise he needed to level up his security program. From strategic support and program development to tactical advice and actionable threat intelligence, they worked together to improve his organization's security. A few dedicated projects included:

- **Endpoint Hunting and Investigation Training:** Henry wanted to ensure that his team knew its selected Endpoint Detection and Response (EDR) product inside and out. A Red Canary incident handler spent several days on-site digging into the intricacies of the tool and training the team from the perspective of a seasoned threat hunter.
- **Expedited High-Risk Deployment:** After WannaCry hit, Henry needed to quickly deploy Red Canary across an additional 3,000 systems in his network. Several of these systems were highly sensitive production lines that could cause millions of dollars in losses if any downtime occurred. Henry and the Red Canary team worked together to ensure that all 3,000 agents were deployed flawlessly over three days with no downtime.
- **Specialized Hunting:** Late one Thursday, Henry sent Red Canary an urgent request for help. A recently terminated high-level executive appeared to have exfiltrated data and Henry was searching for signs of suspicious behavior. An incident handler was able to quickly scan the data repository and locate the information Henry needed.

With Red Canary serving as an extension of his security team, Henry has gained confidence and peace of mind. He said: "Last year I had to work right up until the end of the year. This year I took two weeks off at Christmas. For the first time in my ten-year InfoSec career, I feel really good about my security posture. I have experts looking at every single one of my computers, plus the process and tooling to deal with an issue as soon as I see it. That's something I've never had before."

About Red Canary Incident Handlers

Comprised of seasoned security professionals, Red Canary's incident handling team is chartered to help customers improve their security. Common ways they augment security teams include:

- **Strategic support** to help you build and mature your security program
- **Incident handling** to help you scope incidents and develop a remediation plan
- **Actionable intelligence** around threats and activities specific to your environment and vertical

People with this kind of skill set are rare and expensive. It's the reason why many Red Canary customers can't find or afford these people for their teams. It's also the precise reason why Red Canary includes them as part of its core service.

See how Red Canary can help defend your organization.

www.redcanary.com/demo

red canary