CASE STUDY: MANUFACTURING

How a Lean Security Team Defends a Global Manufacturing Company Against Advanced Attacks

BUSINESS ENVIRONMENT

- Annual Recurring Revenue: $1.6B
- Endpoints: 7K+
- Locations: 40+ worldwide
- IT Security Team: 5 employees + offshore partners

CHALLENGE

An IT security leader knew that Carbon Black Response (CbR) was one of the best ways to defend his organization against evolving threats. However, his green security team did not have the in-house expertise to operationalize the product.

SOLUTION

Red Canary Managed Endpoint Detection & Response (MEDR) layered on top of Cb Response to deliver a complete EDR capability on Day 1.

DEFENDING A GLOBAL INFRASTRUCTURE

The manufacturing company has a lean IT security team that is tasked with overseeing the sprawling global infrastructure. The team is responsible for leading security operations, defending against advanced attacks and insider threats, and managing policies and security controls.

The IT security leader (we'll call him Henry) decided that Carbon Black Response (CbR) was a critical piece of infrastructure to complete the company's defense-in-depth strategy. However, he knew they did not have the staff or expertise to analyze the vast amount of data the product would produce—nor did they have the tools and processes in place to quickly remediate threats once they were detected.

FINDING A PARTNER WITH EDR EXPERTISE

Henry realized that investing in technology without the right people and processes in place would provide sub-par defense and ineffective ROI. He began looking for a partner with deep CbR expertise to augment his team and deliver the full Endpoint Detection and Response (EDR) capability they needed.

The organization had a legacy EDR offering and premium signature-based AV product in place. Henry and his team had worked tirelessly to tune the solution, but it no longer fit their requirements. The team had recently been downsized, the threat landscape continued to evolve, and threats continued to slip past defenses—sometimes going undetected for days.

EVALUATING SOLUTIONS

Knowing that the security infrastructure team would rely heavily on the right partner for Managed Endpoint Detection and Response (MEDR), Henry ran a POC amongst the incumbent (FireEye HX and Mandiant), Red Canary, and another leading MEDR provider.

> “For the first time in my ten-year InfoSec career, I feel really good about my security posture as far as incident response is concerned. With Red Canary I have experts looking at every single one of my computers and I have the process to deal with an issue as soon as I see it. That’s something I’ve never had before.”
>
> — Henry, IT Security Leader

Requirements

- Lightweight solution deployable to all systems, including legacy systems
- Expansive, detailed telemetry recording
- Expert endpoint analysis to augment in-house resources
- Simple incident response for off-site contractors and junior-level analysts

After a lengthy evaluation, the results were clear. Red Canary detected 100% of the test events while the incumbent failed to detect half. Red Canary’s easy-to-read threat detections combined with the ability to respond to incidents from the portal gave Henry confidence that Red Canary was the best fit.

SIMPLIFYING INCIDENT RESPONSE

The company wanted to outsource as much incident response as possible. An offshores partner handles remediation, so preventing direct access to the company’s infrastructure (and to Carbon Black) was a key requirement. Simplicity was the key to orchestrating this workflow.

Red Canary’s visually clear alert reporting and response capabilities enabled the foreign partner to isolate problematic endpoints, stop processes, capture files, and ban infected files on behalf of the entire organization. International partners could easily navigate through complex queries and multiple views in the tool to research incidents or create reports without learning another language. The portal saved the team hours of investigation time each day, which they could reallocate to support other areas of the security program.

Henry said: “If you have a good internal team with a focus and expertise in endpoint analysis, they will be able to get a lot of value out of Carbon Black. But if you’re struggling with the right resources and know your team will not have time to master Carbon Black, hiring Red Canary gives you the expertise and team you need. That leaves you room to think about the things that are important to you.”

472M	processes and executables analyzed
3,689	potentially threatening events investigated
52	confirmed threats detected
0	false positives delivered to the organization

IN THEIR OWN WORDS

Deployment

“We had deployed coverage on about half of our endpoints and planned to roll out the remaining systems over the next few years. But when WannaCry hit, we realized we needed to cover all vulnerabilities immediately. We pushed coverage to 3K highly sensitive endpoints in three days without a single issue. It went smoother than any of us expected.”

Leveraging Expertise

“Analysis is the hardest part. The key to success is getting somebody who is skilled enough to gather the information, accurately analyze what happened, and then take a course of action. This is not our area of focus or expertise. If you can’t get and maintain the talent, the only option is to outsource. All of our processes are now built around Red Canary and we’ve greatly simplified incident response. I consider Red Canary and Carbon Black to be our last line of defense.”

Remediation

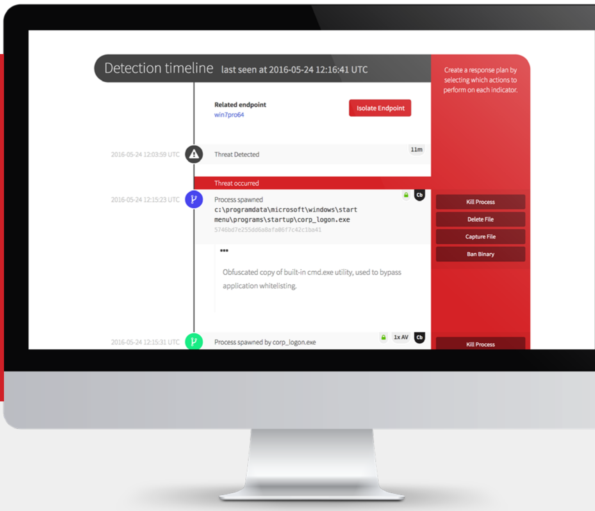
“What really blew me away was the remediation side. For the first time, I knew exactly what happened and could click a button to quickly and easily respond with the action I needed. Sometimes I get an alert in the middle of the night, and if it’s medium or high, I log into the portal from the mobile phone next to my bed, isolate that box, and then go back to sleep.”

Technical Account Managers

“I’m looking for a partnership. I want someone who takes interest in what I do and what my company needs so we can look for solutions together. That requires investing time in knowing my environment. I feel that with Red Canary. The team proactively reaches out to ask me what I need and what I want. They are driven to provide a high quality service, and it shows.”

About Red Canary

Red Canary helps customers secure their endpoints and stop attacks before they result in breaches. The Managed Endpoint Detection and Response solution quickly and accurately identifies threats on customers’ endpoints ranging from compromised credentials to lateral movement to crimeware. Every threat is investigated by a Red Canary Analyst to remove false positives and provide the context required for remediation.



Detection timeline last seen at 2016-05-24 12:16:41 UTC

Create a response plan by selecting which actions to perform on each indicator.

Related endpoint
win7pro64

2016-05-24 12:03:59 UTC Threat Detected 11m

Threat occurred

2016-05-24 12:15:23 UTC Process spawned

```
c:\programdata\microsoft\windows\start menu\programs\startup\corp_logon.exe
5746bd7e255dd6a8afa06f7c42c1ba41
```

Obfuscated copy of built-in cmd.exe utility, used to bypass application whitelisting.

2016-05-24 12:15:31 UTC Process spawned by corp_logon.exe 1x AV

red canary

See how Red Canary can help you secure your endpoints.

855.977.0686 | info@redcanary.com | www.redcanary.com