CASE STUDY: BANKING

A Multi-State Bank Enlists Red Canary to Detect the Most Advanced Attacker Behaviors

BUSINESS ENVIRONMENT

AUM: $15B+

Endpoints: 3,300

Locations: 125+

RESOURCES

IT Budget: $25M

Employees in IT: 100

Employees in InfoSec: 10

SNAPSHOT

A mid-sized bank with over 100 locations had already invested in Carbon Black Protect (application whitelisting) and Carbon Black Response. Cb Protect was successful in defending against the vast majority of attacks, but the team knew they still had exposure. They didn't have the in-house expertise to manage CbR and get the full value out of the product. After struggling with the volume of data, they decided to partner with Red Canary.

DETECTING THE TIP OF THE SPEAR

The security team was immediately impressed with the scope and timeliness of Red Canary's detection. The bank's security team closely monitored application whitelisting bypasses and regularly tested Red Canary against the newest exploits. Every time the bank's red team weaponized a newly published attacker technique, Red Canary was right there to detect it and notify them.

"With Red Canary, we have a lot of confidence that an advanced attacker will not be able to slip through our defenses. The scope of their analysis is pretty amazing and we always are alerted to threats in a quick timeframe."
—Information Security Manager

SAMPLING OF RED CANARY DETECTIONS

Detection Results for [redacted]

We detect threats using hundreds of detectors that hunt for dozens of categories of threats...	**Events were detected** by this category of detector	**Threats were confirmed** by our analysts' review of those events
#3 **Specific threat actor campaigns and/or TTP** Patterns of behavior and movement associated with specific actors and/or used to achieve specific objectives.	166	4
#4 **Privilege escalation** Use of malware or native operating system utilities to escalate from userspace to superuser privileges. Used to gain access to resources not available upon arrival.	5,986	5
#16 **Exfiltration of data** Behaviors or intelligence that indicate movement of data from an endpoint to a suspicious network or media destination.	203	5

red canary

Red Canary is a true partner. They're in the fight with us. They are not just a vendor that's watching and sending alerts over the wall. If something happens, they are there to collect information and get us what we need to respond. It goes way beyond a normal vendor relationship."

— Information Security Manager

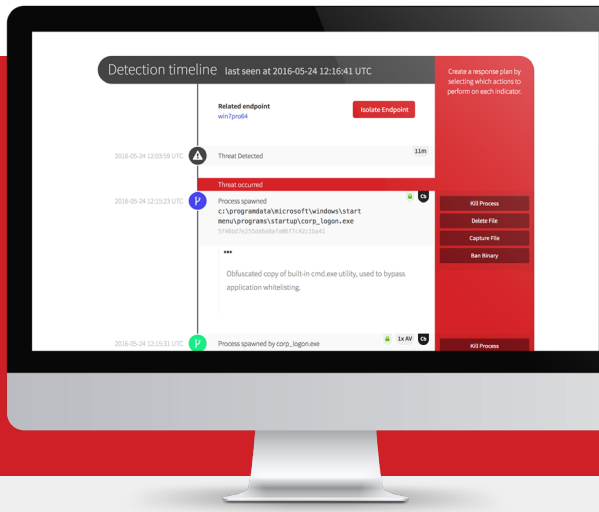
TYPICAL 30-DAY PERFORMANCE

49.8M	processes and executables analyzed
2,085	potentially threatening events investigated
1	confirmed threat detected
0	false positives delivered to the organization

THE RIGHT BALANCE OF TECHNOLOGY + EXPERTISE

Red Canary helped fill a critical gap by offering the ideal combination of advanced detection technology coupled with a team of experts in endpoint activity, forensic investigations, and threat hunting.

"One thing we really liked about Red Canary was their combination of technology and expertise. Their detection technology is extensive and they balance that with their security team. Everything is reviewed by a human, which eliminated the noise our team was dealing with. When I get a Red Canary alert, I know I need to respond because it's actually something and not a fake alert."
—Information Security Manager



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.

See how Red Canary can help you secure your endpoints.

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

red canary