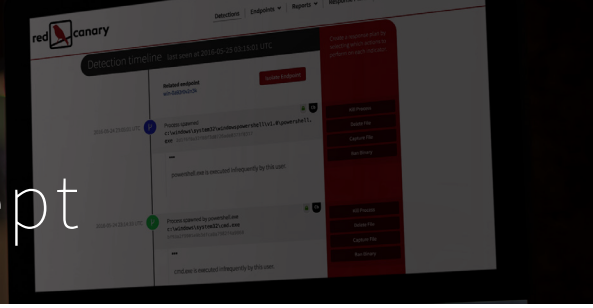
What's Included in a Red Canary Proof of Concept



A Red Canary POC gives you the opportunity to experience the full benefit of a partnership with Red Canary. Each phase of the POC is detailed below.

A POC WILL HELP YOU CLEARLY UNDERSTAND:

1. How Red Canary will fit into your security program
2. The breadth of Red Canary's detection
3. How we can help you better secure your environment

Objective	Key Activities
POC Kickoff	• Red Canary portal setup (inviting users, setting privileges, enabling MFA, etc.) • Establish POC timeline, objectives, and testing plan
Deployment	• Deploy sensors to environment using SCCM, GPO, Casper, Jamf, etc. • Configure firewall to allow communication from endpoints to Red Canary
Tool Integration and Response Workflow Configuration	• Define Red Canary detection alerting plan (email list, ticket tracking system, SMS, SIEM, etc.) • Integrate Red Canary detections/intelligence into security tools
Environment Baseline	• Review anomalous behavior and application use with Red Canary incident handlers
Red Canary Feature Tour	• Review Red Canary detection format • Test Red Canary response tooling (isolation and remediation) • Understand Red Canary reports • *Bonus:* Investigate endpoint activity
Detection Coverage Testing	• Use open source Atomic Red Team tests and MITRE ATT&CK to test Red Canary detection coverage against attacker TTPs
POC Close Out	• Review objectives and results • Review detection results, alert actionability, and response workflow • Review Red Canary summary reports and discuss work done by Red Canary security team

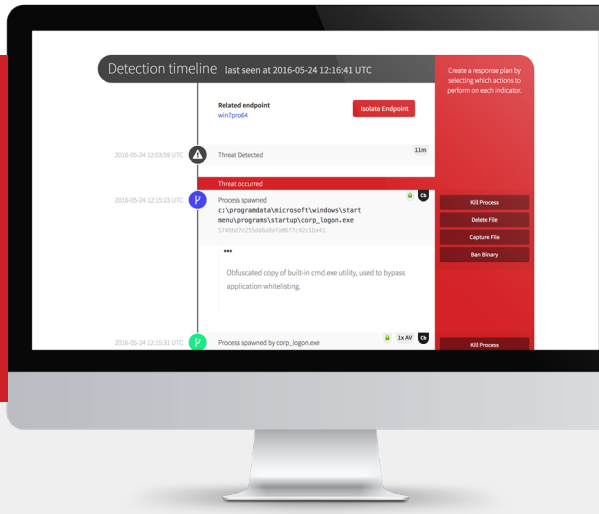
red canary

POC Best Practices

- Establish your criteria for success.
- Deploy Red Canary across all or most of your environment.
- Plan on running tests—the harder, the better. Although executing malicious binaries from Virus Total can be effective when testing AV, you should plan for more advanced testing during your Red Canary POC.
- Involve all teams that will interact with Red Canary.

"The technology under the hood of Red Canary is extraordinary and can adapt as quickly as adversaries adapt. By having a hosted solution we were up and running incredibly fast, and have been able to alleviate any capacity concerns and constraints we had."

—Information Security Manager, Multi-State Bank



red canary

Ready to start a POC?

Contact your Account Executive today.