Improving cyber compliance with infrastructure automation

Monitor events across multiple agencies. Automate the response using each agency's playbook.

Red Hat solutions

Red Hat Integration connects data from multiple agencies' network devices, servers, and edge devices.

Open Data Hub on Red Hat OpenShift lets you train machine learning models to recognize malicious patterns.

Red Hat Decision Manager maps security events to responses according to each agency's rules.

Red Hat Ansible Automation Platform automatically invokes the agency's action when a threat is detected, according to the agency playbook.

Malware does not respect departmental boundaries

Federal government law enforcement agencies need to protect sensitive data such as criminal records and investigations, biometrics, tax filings, security camera footage, and personnel records. Exposure of sensitive information can disrupt operations, put staff in harm's way, and erode trust in government. Common attacks include data exfiltration and denial of service.

Barriers to cyber compliance in law enforcement include:

- **Limited staff.** Agency security teams don't have the resources to monitor growing traffic volume, including streams from edge devices like IP cameras that can carry malware. Delays in detecting and remediating threats extend the window of vulnerability.
- **Lack of central monitoring across agencies.** Attacks targeting multiple agencies are often more sophisticated and carry higher risk of major business disruption and information leakage. Agencies unaware that a security event is part of a multi-agency attack might underestimate its severity.
- **Remediation cannot disrupt operations.** Law enforcement agencies often cannot shut down a compromised device without disrupting continuity of operations. They need more nuanced remediation based on threat severity.

Solution: Holistic view of network events—and automated response

Protecting public data requires two capabilities that federal law enforcement agencies lack today. One is a holistic view of all network and server activity across multiple organizations. The other is automated remediation based on the nature of the threat and the agency's playbook. Examples include enforcing the same list of banned network addresses across multiple agencies, sending alerts if these addresses are seen, quarantining a suspicious workload until it can be investigated, and terminating a virtual server exhibiting anomalous behavior and then spinning up a new one from a trusted source.

Benefits of automated cyber compliance in law enforcement include:

- Faster incident detection.
- Faster remediation, shortening the vulnerability window.
- Reduced resource requirements for threat mitigation.
- Increased job satisfaction because cybersecurity professionals can shift their focus from mundane monitoring activities to higher-value work—a recruitment and retention advantage.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

Why Red Hat?

Increased security. Our solutions meet stringent federal government security requirements.

Partner ecosystem. Work with our partners to link solutions for data interrogation and automated remediation.

Proven in federal government. The Cybersecurity Infrastructure and Security Agency (CISA), among others, uses Red Hat OpenShift.

Flexibility through open APIs. As you add new devices, use open APIs to monitor them alongside existing devices.

Lower costs. Our subscriptions can cost less than proprietary software licenses and support contracts.

Red Hat's approach to automated cyber compliance

We provide a complete solution for strengthening cyber compliance through infrastructure automation.

Train a machine learning model to distinguish between normal and anomalous activity. Use Open Data Hub, an AI platform, on Red Hat® OpenShift®. Test the model by simulating threats. Continually tune the model by feeding in data about newly discovered threats and the effectiveness of the response.

Map different types of threats to remediation. Use Red Hat Decision Manager to specify responses such as blocking an attacker's IP address, whitelisting non-threatening traffic, quarantining a suspicious workload, or spinning down an infected virtual server and spinning up a new one.

Automate monitoring and response—across multiple agencies. Use Red Hat Ansible® Automation Platform to collect logs from multiple agencies' firewalls, IDS, edge devices, and ecosystem products like Sensu for log aggregation or ServiceNow for operational case management. Ansible Automation Platform automatically invokes the specified action from the playbook. If the action does not resolve the issue, Ansible Automation Platform sends an alert and opens a case in ServiceNow.

Give agencies control over their own playbooks. Individual agencies are the experts on how much risk they can tolerate before shutting down a particular service. With Ansible Automation Platform, agency cybersecurity teams can use a web interface to modify thresholds, hostnames, and playbooks to meet mission requirements.

Learn more. To learn more about how Red Hat can help government IT innovate, visit redhat.com/government.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#F26748_0121

Thank you for downloading this Red Hat brief! Carahsoft is the Master GSA and SLSA Dealer and Distributor for Red Hat Enterprise Open Source solutions available via GSA, SLSA, ITES-SW2, The Quilt and other contract vehicles.

To learn how to take the next step toward acquiring Red Hat's solutions, please check out the following resources and information:

For additional resources:
carah.io/RedHatResources

For upcoming events:
carah.io/RedHatEvents

For additional Red Hat solutions:
carah.io/RedHatPortfolio

For additional Open Source solutions:
carah.io/OpenSourceSolutions

To set up a meeting:
redhat@carahsoft.com
877-RHAT-GOV

To purchase, check out the contract vehicles available for procurement:
carah.io/RedHatContracts