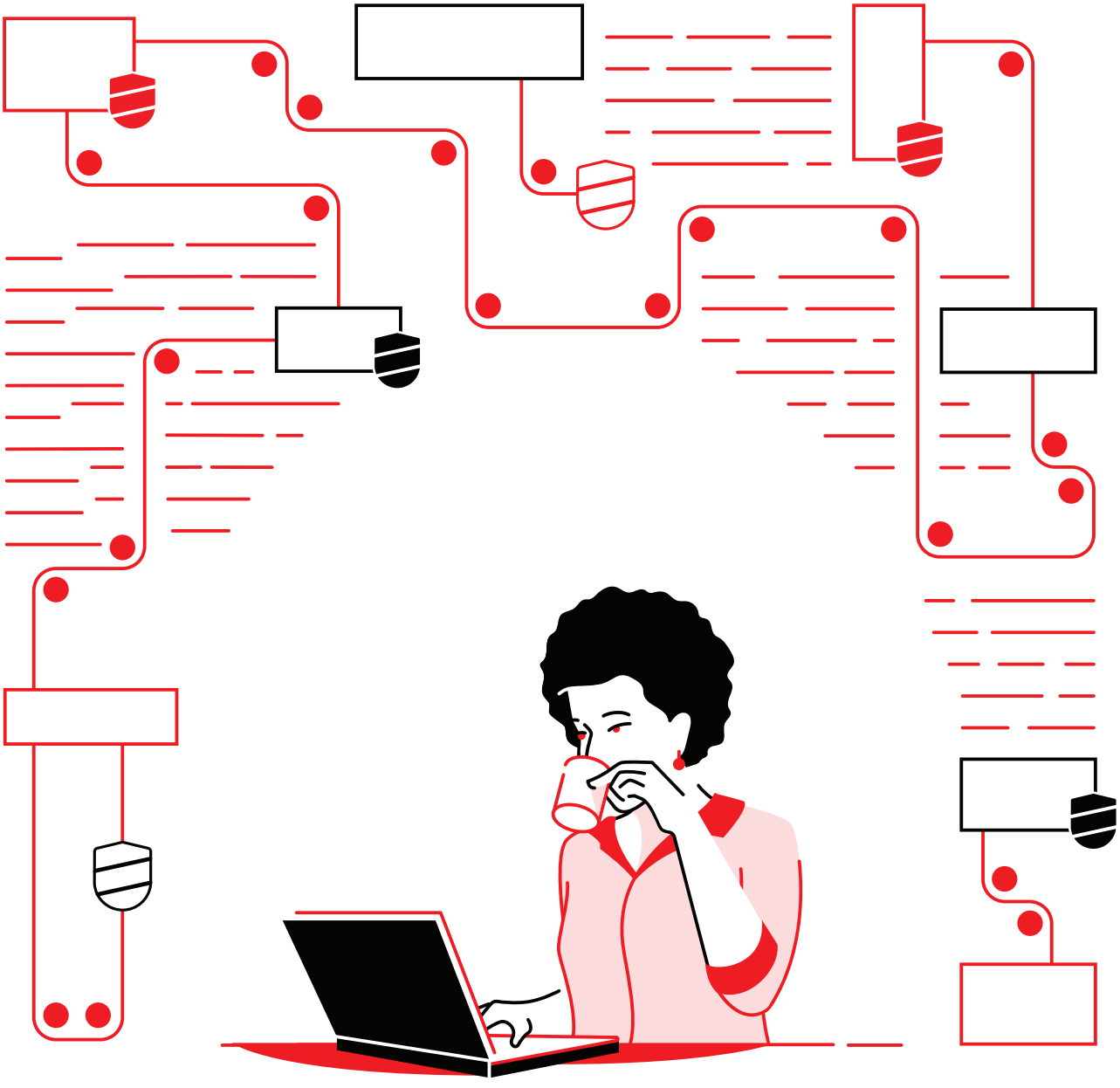
Simplify your security operations center

Gain speed, time, and security with a unified automation platform



Red Hat | IBM

See what's inside

IT security is a top concern

Security is a leading issue for most organizations. In fact, 33% of CEOs are extremely concerned about cyber threats.[1] This apprehension is not unfounded: 32% of organizations experienced major cyber attacks in the past two years.[2]

Protecting your organization is a critical—but frequently daunting—task. Security teams must assemble, maintain, manage, and adapt complex environments using multiple tools and services from a variety of often-competing vendors. The quantity of offerings increases each year, so teams must continually research, assess, and integrate new products as the security landscape changes.

Additionally, the number, severity, and cost of security breaches continue to grow. The likelihood of experiencing a breach within two years is 29.6%, up from 22.6% in 2014.[3] The average number of records involved in each data breach increased by 3.9% from 2018 to 2019.[3] And the average cost of a data breach rose to US$3.92 million in 2019.[3]

Most organizations handle security operations manually. Security-related tasks can be time-consuming, tedious, and error-prone when human intervention is required. As a result, security teams are overwhelmed. They face an increasing number of threat alerts from numerous tools. In reality, 60% of security teams receive more than 5,000 alerts daily, and 16% receive more than 100,000 alerts daily.[4]

And increasing infrastructure size and complexity make it more difficult to identify vulnerabilities and verify breaches. Most security tools do not integrate with each other, resulting in more manual work for security staff. Correspondingly, incident investigation and response times are increasing. In 2019, the average time to identify and contain a data breach was 279 days, up 4.9% from 2018.[3] And it's hard to find new talent to expand teams and keep up; 39% of organizations reported a shortage in cyber security skills in 2019.[2] Finally, budgets for cyber security activities are limited. Only 33% of organizations report having sufficient funding to achieve a high level of cyber resilience.[5]

Consequently, typical security teams only review and respond to 48% of the alerts they receive and only 50% of legitimate threats are remediated.[4] This leaves many organizations vulnerable to attack.

77% of organizations plan to increase automation to simplify and speed up response times in their security ecosystems.[4]

Impacts of ineffective security

The number, severity, and cost of security breaches continue to grow.

US$3.92 million
average cost of a data breach in 2019[3]

279 days
average time to identify and contain a data breach in 2019[3]

US$1.22 million
savings in costs if a breach can be identified and contained in

200 days
or less[3]

29.6%
likelihood of experiencing a breach within two years[3]

50%
proportion of legitimate threats that are remediated[4]

1 *PWC, "23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty," 2020.* **pwc.com/ceosurvey**.

2 *Harvey Nash and KPMG, "CIO Survey 2019: A Changing Perspective," 2019.* **home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html**.

3 *IBM Security, "2019 Cost of a Data Breach Report," 2019.* **ibm.com/security/data-breach**.

4 *Cisco, "Cisco Benchmark Study: Securing What's Now and What's Next," February 2020.* **cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html**.

5 *Ponemon Institute, sponsored by IBM Security, "The Cyber Resilient Organization," April 2019.* **ibm.com/account/reg/us-en/signup?formid=urx-37792**.

What is security automation?

Security automation involves automating the manual tasks associated with maintaining the security posture of your business. It consists of multiple practices, and we have divided these into four general categories:

Response and remediation
Event-driven activities that involve security analyst participation, guidance, or both

Security operations
Day-to-day process- and policy-driven activities performed on your security infrastructure by technology teams

Security compliance
Activities to ensure infrastructure is compliant with security policies and regulations

Hardening
Activities to apply custom security policies to infrastructure with the targeted intent and goals

Learn more about security compliance and hardening

Discover how automation can help security compliance and hardening by reading these resources:

- **Boost hybrid cloud security e-book**
- **Why automate security and compliance overview**
- **Red Hat Services: Automate security and reliability workflows datasheet**

This e-book focuses on automating response and remediation activities and security operations.

Benefits of automation for security operations, response, and remediation activities

Boost speed and efficiency

Automation streamlines tasks and removes the need for manual intervention, speeding security operations and allowing staff to refocus on high-value initiatives. It can also reduce IT infrastructure complexity: 40% of high-automation organizations report having the right number of security solutions and technologies.[6]

Increase security at scale

Applying automation across your security infrastructure increases consistency and allows you to take a more holistic approach to security. Each staff member can manage more tools, devices, and systems, so you can operate at scale. Automation also reduces the risk of human errors, improving accuracy.

Reduce the risk and cost of breaches

Organizations that automate extensively are better able to prevent security incidents and business disruptions.[6] Fully deploying security automation can reduce the average cost of a breach by 95%.[7] As a result, 52% of organizations deployed some amount of security automation and 36% more plan to do so in the next 24 months.[7]

6 *Ponemon Institute, sponsored by IBM Security, "The Cyber Resilient Organization," April 2019.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

7 *IBM Security, "2019 Cost of a Data Breach Report," 2019.* ibm.com/security/data-breach.

Automation integrates your security tools, systems, and processes

Unite people, processes, and tools with a consistent, flexible platform

An automation platform can serve as an integration layer between your security teams, tools, and processes. A flexible, interoperable platform lets you:

- Connect your security systems, tools, and teams.
- Collect information from systems and direct it to predefined systems and locations quickly and without manual intervention.
- Change and propagate configurations quickly from centralized interfaces.
- Create, maintain, and access custom automation content related to your security tools and processes.
- Trigger automated actions across multiple security tools when a threat is detected.

Using a consistent automation platform and language across your organization can also improve communication and collaboration. When every solution in a security portfolio is automated through the same language, both analysts and operators can perform a series of actions across products in a fraction of the time, maximizing the overall efficiency of the security team. And a common framework and language lets security and IT teams share designs, processes, and ideas more easily both internally and across your organization.

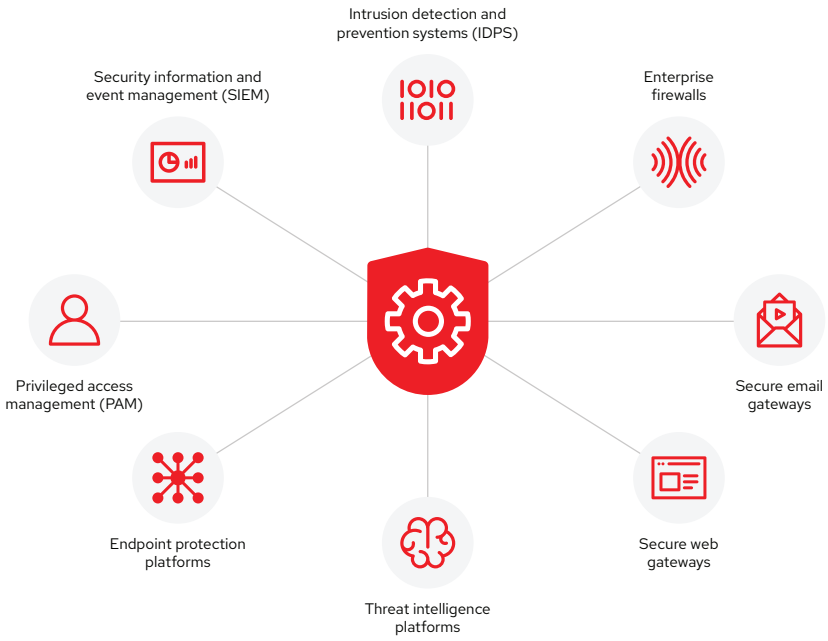


Figure 1. An automation platform can connect your security systems, tools, and teams.

Automation success = people + processes + platform

Maximizing the value of automation requires more than just a tool—you also need to consider your people, processes, and platform.

- **People** are at the core of any business initiative. Participation within and across teams lets staff share ideas and collaborate more effectively.
- **Processes** move projects within your organization from start to finish. Clear, documented processes are essential for effective automation.
- An automation **platform** provides the capabilities for building, running, and managing your automation assets. In contrast to simple automation tools, an automation platform gives your organization a unified foundation for creating, deploying, and sharing consistent automation content and knowledge at scale.

Read the e-book

Security automation is a journey

Implementing automation in any aspect of your organization does not happen instantly, and it is not an all-or-nothing proposition. Security automation is a journey. Each organization will start – and stop – at different points according to their needs. Those needs will also dictate the path that each organization takes. Even so, no matter where you are in your journey, even small security automation efforts can deliver benefits.

Assess your security automation maturity level

Most organizations fall into one of three main stages of security automation maturity. Determining your organization's current stage will help you adopt the right tools and processes at the right time to make your automation journey more successful.

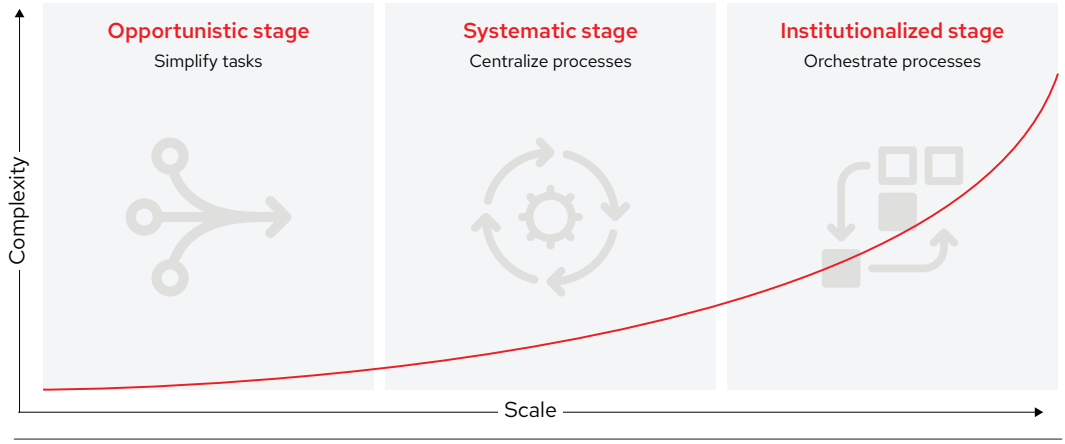


Figure 2. Stages of security automation maturity

Stage 1: Opportunistic

This stage focuses on saving time by automating security operations. Common goals include standardizing security actions across similar devices and technologies and streamlining manual tasks performed across products from different vendors.

Stage 2: Systematic

This stage focuses on improving processes and efficiency by adopting a cohesive set of security operations tools and services. Common goals include building security processes into higher-level workflows and centralizing security response processes.

Stage 3: Institutionalized

This stage focuses on boosting collaboration and integrating security across your organization. Common goals include creating automated, programmatic workflows that span all aspects of security and integrating your security and IT technologies.

Use cases and integrations

Define your path to security automation

Common, high-level use cases for security automation

Each of these use cases can serve as a starting point for your security automation journey. The key is to start small and simple, and build over time.

Investigation enrichment

Investigating security alerts and incidents involves collecting information from a variety of security systems to assess whether a legitimate event has occurred. Information is typically gathered through a series of user interfaces, emails, and phone calls. This inefficient process can delay action against threats, leaving your business vulnerable and increasing the potential costs associated with a breach. Automation allows you to programmatically assemble information across your security systems, supporting on-demand enrichment of triage activities performed through security information and event management (SIEM) systems. As a result, you can assess—and respond to—alerts and incidents faster.

Threat hunting

Threat hunting involves identifying and investigating potential threats to security in a proactive fashion. As with incident investigation, staff manually gather and send information between many systems. Using automation, you can customize and streamline alerts, correlation searches, and signature manipulation to examine potential threats faster. You can also automatically create and update SIEM correlation queries and intrusion detection system (IDS) rules to improve detection. Consequently, you can update your organization's security defenses more frequently and efficiently to better protect your business.

Incident response

Incident response involves taking action to stop a breach from continuing. Once a breach is discovered, security staff must respond quickly and at scale to contain it. However, response actions often include multiple manual tasks, slowing remediation time and leaving your organization vulnerable for longer. Automation helps you react faster by codifying actions into repeatable, preapproved playbooks. You can speed tasks like blocking attacking IP addresses or domains, allowing non-threatening traffic, freezing compromised credentials, and isolating suspicious workloads for further investigation to minimize the damage associated with the incident.

Integration is essential

Unified automation approaches require integration between your automation platform and your security technologies. Essential integrations include:

- **Firewalls** control traffic flow between networks, protecting internet-exposed applications. Automation can speed policy and log configuration changes.
- **Intrusion detection and prevention systems (IDPS)** monitor network traffic for suspicious activity, issue threat alerts, and block attacks. Automation can simplify rule and log management.
- **Security information and event management systems** collect and analyze security events to help detect and respond to threats. Automation can provide programmatic access to data sources.
- **Privileged access management (PAM) tools** monitor and manage privileged accounts and access. Automation streamlines credential management.
- **Endpoint protection systems** monitor and manage devices to improve their security. Automation can simplify common endpoint management tasks.

Simplify your security operations center with Red Hat Ansible Automation Platform

There are many automation solutions available, but not all include the capabilities needed for effective security automation. Look for automation platforms that offer:

- **A universal, accessible automation language.** A language that is easy to understand and write allows you to document and share information between security team members with different domain expertise.
- **An open and unbiased approach.** To be effective, your automation platform must interoperate with your entire security infrastructure and vendor ecosystem.
- **A modular and extensible design.** A modular platform allows you to deploy automation in steps. Extensibility helps you accommodate additional and future security tools from other vendors as needed.

Move your security organization forward with Red Hat

A foundation for building and operating automation services at scale, Red Hat® Ansible® Automation Platform delivers all the tools and features you need to implement security automation. It combines a simple, easy-to-read automation language with a trusted, composable execution environment and security-focused sharing and collaboration capabilities. An open foundation allows you to connect and automate almost everything in your security and IT infrastructure, creating a common platform for participation and sharing across your entire organization. Red Hat Ansible Automation Platform has also delivered proven outcomes in other areas, including IT and network operations and DevOps.

A supported set of security-focused Ansible collections – including modules, roles, and playbooks – is Included with the platform. These assets coordinate the activity of multiple classes of security solutions for a more unified response to cyber threats and security operations:

- Chain workflows and playbooks for modular reusability.
- Consolidate and centralize logs.
- Support local directory services and access controls.
- Integrate external apps using RESTful application programming interfaces (APIs).

Red Hat Ansible Automation Platform also includes tools and capabilities to help you optimize your automation. Automation Analytics provides insight into how your organization uses automation. Automation Hub lets team members access certified automation content through a centralized repository. And Content Collections streamline the management, distribution, and consumption of automation assets.

Get help from the experts

Red Hat can help you successfully deploy automation faster.

- **Red Hat Services Program: Automation Adoption** provides a framework for managing an organization-wide automation adoption journey.
- **Red Hat Training and Certification** offers hands-on training and practical certification to help you use automation more effectively.
- **Red Hat Support** works with you to ensure success on your IT journey. Award-winning web support[8] gives you access to best practices, documentation, updates, and security alerts and patches. You can also connect with a support engineer or technical account manager to resolve issues and obtain specialized guidance.
- **Certified partner content collections** allow you to readily automate hardware and software from a broad selection of vendors. This trusted, pre-built automation content is available through Automation Hub and is supported by both the partner and Red Hat.

8 Red Hat Customer Portal awards & recognition, **access.redhat.com/recognition**.

Automation in action

Red Hat Ansible Automation Platform delivers proven business value

Red Hat Ansible Automation Platform provides a more efficient, streamlined way to automate your security operations center. Analyst studies of organizations that use Red Hat Ansible Automation Platform demonstrate measurable business value. In fact, IDC interviewed multiple decision makers about their experiences with Red Hat Ansible Automation Platform and found that each organization realized significant productivity, agility, and operational benefits through automation.

more efficient and productive IT security teams[9]

more efficient security incident mitigation[9]

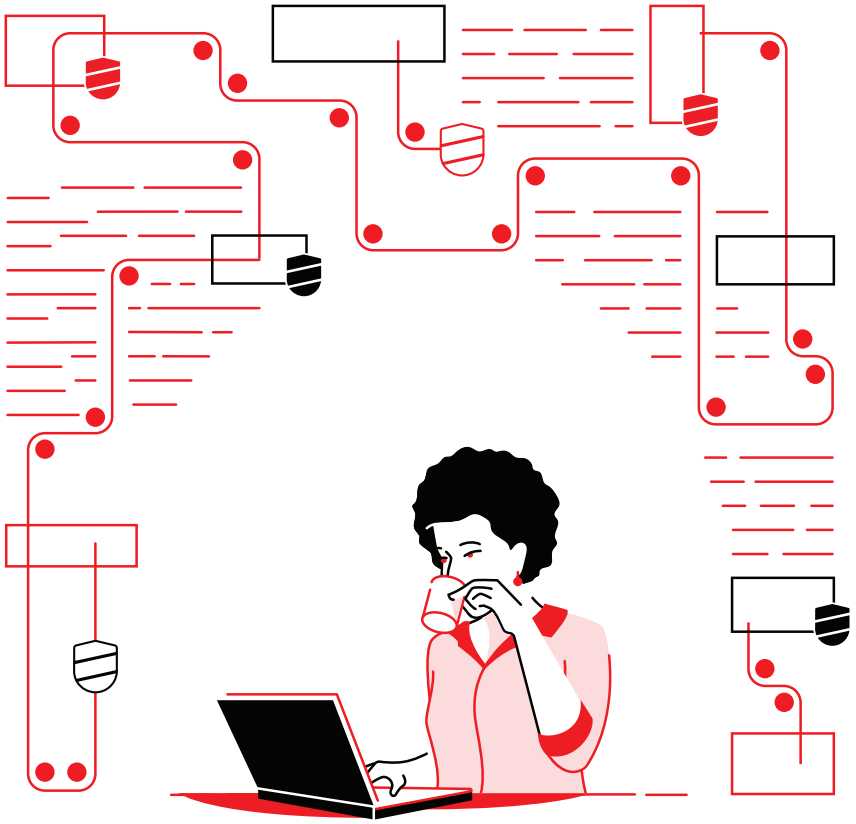
more efficient security patching[9]

"Red Hat Ansible [Automation Platform] is phenomenal for bringing our IT teams together. The server, security, network, and database teams can all work on their separate tiers and then use Red Hat Ansible Automation to create their own playbooks."[9]

9 *IDC White Paper, sponsored by Red Hat. "Red Hat Ansible Automation Improves IT Agility and Time to Market," June 2019.*

Ready to simplify your security operations center ?

Automation can help you identify and respond to growing security threats faster and at scale. Red Hat helps you protect your business by connecting your security teams, tools, and processes with a consistent, collaborative automation platform.



Learn how to automate security with Red Hat Ansible Automation Platform

F24343_0720_KVM

Red Hat | IBM