XLAB Steampunk

Automate your security with Ansible

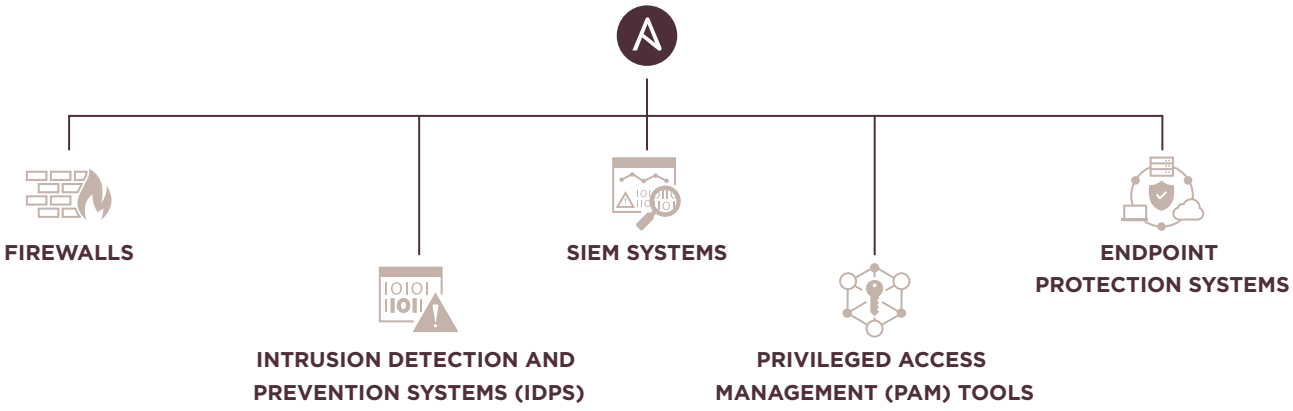
Take the pressure off your overburdened security teams by transforming your security processes into automatically executed workflows. Strengthen your security posture and respond faster to security threats. Gain better productivity, agility and operational benefits through automation with Ansible Automation Platform.

Siloed security teams. Unintegrated tools.

Security departments are often faced with numerous domain-specific security tools and services from multiple vendors that cannot be integrated with each other. They all play an important role in risk management and control but present a challenge for security teams to juggle them all simultaneously. In addition, many security-related activities are still performed manually, which is time-consuming, tedious and error-prone. As a result, it takes more time from detection to response, and security breaches are not handled appropriately, leaving the organization at high risk.

Improve your security through automation

Ansible is the common language between security tools:



Achieve effective protection against security incidents and business disruptions. Minimize costs associated with security breaches, reduce the risk of human error, and improve reliability, accuracy, and consistency.

Who is it for?

Security teams in large organizations	Managed Security Service Providers
dealing with increasingly fast and complex attacks.	dealing with thousands of security solutions across their whole customer base.

Security automation in action

Investigation enrichment

Automation enables programmatic collection of logs from security systems such as firewalls and intrusion detection systems (IDS) to optimize and support activities performed through SIEM systems.

Threat hunting

Automating alerts, correlation searches and signature manipulations, as well as creating and updating SIEM correlation queries and rules for IDS accelerates the investigation of potential threats.

Incident response

Automation speeds up tasks such as setting up blacklists, blocking attacking IP addresses or domains, allowing non-threatening traffic, freezing compromised credentials, and isolating suspicious workloads for further investigation.

There are many additional options to automate your security and make your life easier: SIEM and firewall automation, configuration of security rules within operating systems (e.g., user access rights), remote access (VPN), user and rights management and logs across systems, and more.

Red Hat Ansible Automation Platform

The Ansible Automation Platform enables organizations to successfully implement security automation across their infrastructure. A supported set of modules, roles, and playbooks unifies disparate security technologies, systems, and processes, as well as siloed security teams, enabling a more efficient and streamlined way to identify, search for, and respond to security events.

Ansible seamlessly integrates with

IBM, Cisco, Check Point, F5, Splunk, Snort, Fortinet, Palo Alto, CyberArk, Syncope.

Rely on the experts

Implementing security automation can be challenging. To find the right automation strategy that fits your business needs, and to truly reap the benefits of security automation, it is advisable to work with experts. Our XLAB Steampunk team, IT automation specialists and experts in Ansible, can help you on your way to simplified security operations.

Let's talk

About XLAB Steampunk

XLAB Steampunk is IT automation specialist and leading expert in building Red Hat Certified Ansible Collections (such as ServiceNow and Sensu Go). We have extensive Ansible expertise and as an Ansible Certified Partner collaborate closely with the Ansible product team.

+386 1 2447 756
steampunk@xlab.si

www.steampunk.si