CENTRE OF EXCELLENCE CYBERSECURITY

Elastic SIEM with Red Hat OpenShift on AWS

Self-managed Elastic SIEM hosted on Red Hat OpenShift on AWS

Solution Overview

Elastic provides a scalable, secure and resilient Security Information and Event Management (SIEM) platform using Elastic stack on Red Hat OpenShift hosted on AWS, enabling centralised threat detection, investigation, and response across hybrid environments. The solution provides great flexibility and automation opportunities.

Technology Partners

elastic Red Hat aws

Key Benefits

- **Unified Threat Detection and Response:** Elastic SIEM consolidates logs, metrics, and security telemetry into a centralised platform. Detect and investigate threats in real time using prebuilt and custom detection rules, MITRE ATT&CK-aligned analytics, and behavioural anomaly detection (via ML). Simplified investigations with timelines, correlation, and case management.

- **Cloud-Native Scalability with OpenShift:** Red Hat OpenShift enables dynamic, container-based deployment of Elastic components. Easily scale Elasticsearch data nodes, ingest pipelines, and Kibana. OpenShift's automated rollout, rollback, and self-healing features ensure high availability.

- **Flexible and Elastic Infrastructure on AWS:** Use on-demand and auto-scaling infrastructure (EC2, EBS, S3) to match workload demands. Offload long-term retention and backups to cost-efficient AWS services (e.g., S3). Integrate seamlessly with AWS-native security sources like GuardDuty, CloudTrail, and VPC Flow Logs.

Tech Data Centre of Excellence

Elastic SIEM on Red Hat OpenShift, available for Demos, PoCs and Workshops.

USE CASES

- Container Security Monitoring
- Cloud Threat Monitoring
- Detection of malware execution, suspicious login, lateral movement, insider threats etc.
- Automated deployment to AWS

CENTRE OF EXCELLENCE

CYBERSECURITY • AUTOMATION

Infoblox with Red Hat Ansible Automation Platform on AWS

Seamless Network Automation and Reliability in the Cloud

Solution Overview

Infoblox with Red Hat Ansible Automation Platform on AWS provides automated, reliable, and scalable network services within the AWS cloud, combining industry-leading DNS, DHCP, and IPAM with efficient automation of network configurations. This integrated solution enhances operational efficiency, optimises resource usage, and supports the dynamic needs of modern cloud environments.

Key Benefits

Leverage certified content collections in Ansible Automation Platform to drive automation into Infoblox NIOS environments.

- **Automation of Network Services:** Reduces human error and speeds up deployment processes through automated network configurations.
- **Flexibility and reliability:** Support dynamic needs of modern cloud environments, adapting to changing requirements while providing industry-leading DNS, DHCP, and IPAM services for robust network reliability.
- **Enhanced security and operational efficiency:** Ensures secure network management with advanced security features whilst enhancing operational efficiency by optimising resource usage.

Technology Partners

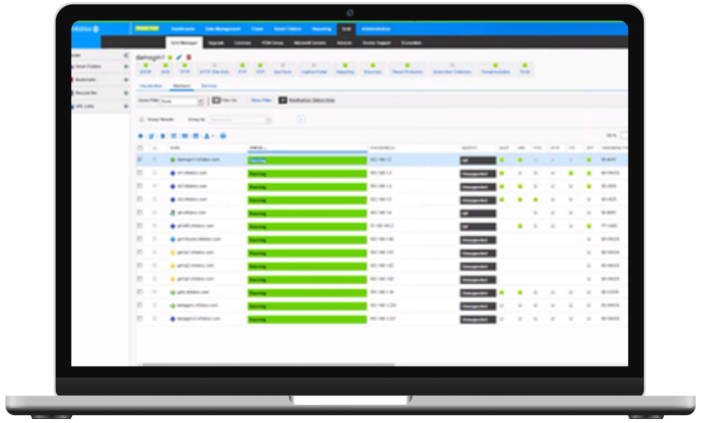
infoblox. Red Hat aws

Tech Data Centre of Excellence

Red Hat Ansible Automation Platform with Infoblox NIOS on AWS, available for Demos, PoCs and Workshops.

USE CASES

- Network Configuration Management
- Incident Response Automation
- Automated deployment to AWS



CENTRE OF EXCELLENCE

CYBERSECURITY • AUTOMATION

Check Point with Red Hat Ansible Automation Platform on AWS

Accelerate Cyber Threat Prevention

Solution Overview

Integrate Red Hat Ansible Automation Platform with Check Point Security Management through application programming interfaces (APIs), providing a framework for codifying processes into automated workflows, freeing SOC and IT security teams to concentrate on more critical tasks.

Technology Partners

CHECK POINT

Red Hat

aws

Key Benefits

- **Reduce Incident Analysis Time:** Automated tools can collect data about security threats from multiple sources without human assistance, reducing overall investigation analysis time.
- **Automate Incident Response:** Seamlessly trigger mitigation policies on Next-Gen Threat Prevention firewalls.
- **Automate Routine Tasks:** Reduce the time it takes to maintain large, distributed security deployments.
- **Improve Speed and Agility:** Rapidly provision both physical and virtualised next-generation firewalls.
- **Configure with Confidence:** Apply the security you need in a simple, consistent manner.

Tech Data Centre of Excellence

Red Hat Ansible Automation Platform with Event-Driven Ansible and Check Point Security Management, available for Demos, PoCs and Workshops.

USE CASES

- Security Automation – investigation and threat response
- Triage of suspicious activities
- Threat hunting
- Incident response
- Configuration management

CENTRE OF EXCELLENCE

CYBERSECURITY • AUTOMATION

IBM Guardium Data Protection with Ansible Automation Platform on AWS

Secure critical enterprise data from both current and emerging risks, wherever it lives

Solution Overview

Automate and orchestrate a single-instance IBM Guardium Collector on AWS with Red Hat Ansible Platform. Leverage Ansible Playbooks to simplify deployment, security configuration, and lifecycle management— ensuring real-time data discovery, classification, and protection. This streamlined, repeatable approach enhances security and compliance for critical cloud databases.

Key Benefits

- **Real-time security & compliance:** Continuously monitor database activity, detect threats, and generate robust compliance reports.
- **Comprehensive data insight:** Discover and classify sensitive data across environments for a clear view of data at risk.
- **Effortless deployment & updates:** Easily deploy Guardium Collector on AWS, with Ansible automating provisioning and maintenance.
- **Centralised management:** Maintain consistent security policies and alerts for critical cloud workloads.

Technology Partners

IBM Distributor

Red Hat

aws

Tech Data Centre of Excellence

Red Hat Ansible Automation Platform with IBM Guardium on AWS, available for Demos, PoCs and Workshops.

USE CASES

- Automated compliance monitoring
- Securing hybrid cloud
- Proactive threat detection
- Automated deployment on AWS
- Integration with AWS resources

CENTRE OF EXCELLENCE

CYBERSECURITY

HCL AppScan with Red Hat Ansible on Red Hat OpenShift on AWS

Accelerate and Automate Application Security Testing on an Enterprise-class Container Platform

Solution Overview

HCL AppScan provides robust application security testing (DAST, SAST, SCA, IAST) integrated into CI/CD pipelines. AppScan secures applications deployed on OpenShift, whilst Ansible is leveraged to automate deployment and remediation workflows.

Key Benefits

- HCL AppScan embeds security and compliance directly into automated development pipelines, providing compliance-as-code. Application code and container images are scanned for vulnerabilities, and AppScan acts as a "security gate" that prevents non-compliant applications from being deployed.
- Red Hat OpenShift brings together tested and trusted services to help reduce the friction of developing, modernising, deploying, running, and managing applications.
- Red Hat Ansible Automation Platform enables infrastructure and application automation across hybrid environments.
- Together, AppScan, OpenShift and Ansible enable secure, scalable and automated DevSecOps.

Technology Partners

HCLSoftware Red Hat aws

Tech Data Centre of Excellence

HCL AppScan with Red Hat Ansible on Red Hat OpenShift on AWS, available for Demos, PoCs and Workshops.

USE CASES

- Secure CI/CD Pipeline Automation
- Policy-as-Code for Secure DevOps
- App Compliance Reporting Post-
- Breach Response Automation

CENTRE OF EXCELLENCE CYBERSECURITY

GitLab on Red Hat OpenShift on AWS

Accelerate DevOps with Scalable, Cloud-Native Efficiency on an Enterprise-class Container Platform

Solution Overview

GitLab on Red Hat OpenShift on AWS integrates GitLab's CI/CD capabilities with OpenShift's container orchestration to create a scalable and efficient DevOps environment. This solution streamlines software delivery, enhances development efficiency, and supports cloud-native application development.

Technology Partners

GitLab Red Hat aws

Key Benefits

- Red Hat OpenShift brings together tested and trusted services to help reduce the friction of developing, modernising, deploying, running, and managing applications.
- GitLab provides the most comprehensive AI-powered DevSecOps platform to help you produce better, more secure software faster across the software development lifecycle.
- Together, OpenShift and GitLab can help you code better and scale faster to maximise compute,
developer, and operational efficiency and provide a consistent experience.

Tech Data Centre of Excellence

Red Hat OpenShift with GitLab Runner on AWS, available for Demos, PoCs and Workshops.

USE CASES

- Containerised Application Development
- Secure and streamlined CI/CD AI-
- powered DevSecOps
- Automated deployment to AWS