BUREAU VERITAS

SECURITY INNOVATION
A BUREAU VERITAS COMPANY

Cloud Services

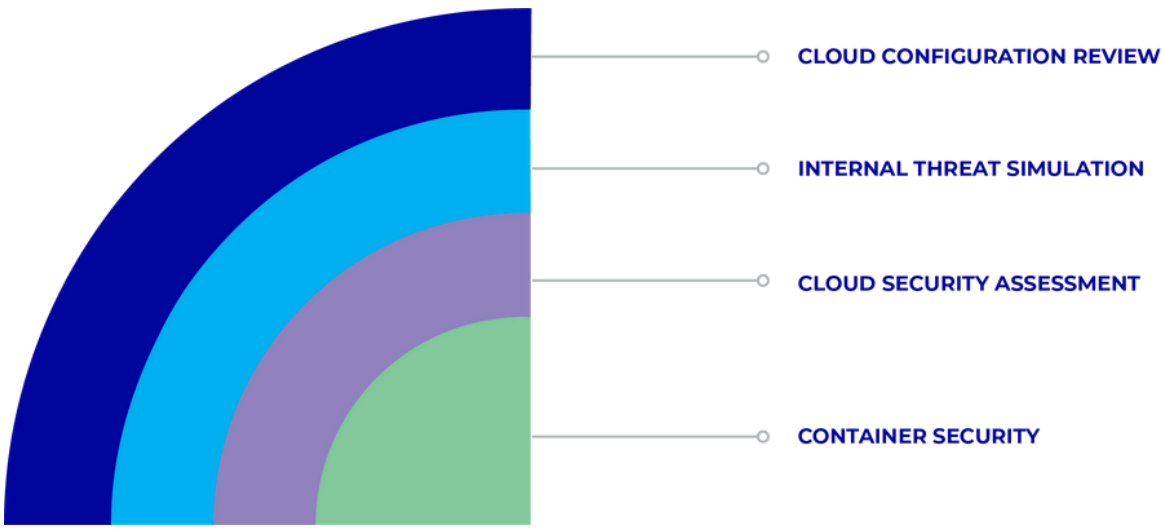
As a team of dedicated cybersecurity professionals, we specialize in delivering tailored, high-quality security solutions to organizations of all sizes. With over a decade of expertise in Cloud Security, Network Security, and more, we empower businesses to identify and mitigate potential vulnerabilities effectively.

Cybersecurity service offerings

Cloud Configuration Review

Our Cloud Configuration Review service offers an in-depth evaluation of cloud infrastructure's configuration to identify misconfigurations, strengthen security posture, and ensure compliance with industry standards. We provide tailored insights for each CSP (Cloud Service Provider), including Azure, AWS, GCP, Kubernetes, and Docker environments.

We adhere to industry benchmarks such as the CIS Foundations Benchmarks for AWS, Azure, GCP, Kubernetes, and Docker, ensuring best practices are followed for configuration and security. Our assessments integrate the NIST Cybersecurity Framework (CSF) for robust risk management, alongside cloud-specific controls. We also incorporate the OWASP Cloud Security Guidelines, Docker Security Best Practices, and the OWASP Kubernetes Top 10 to address platform-specific vulnerabilities. Additionally, our approach is guided by compliance frameworks such as PCI DSS, and the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) to ensure regulatory adherence and secure data handling. By leveraging these standards, we deliver actionable insights to strengthen your cloud infrastructure, mitigate risks, and align with global security expectations.



What we cover:

The following are some key aspects of Cloud Configuration Review that we evaluate. While this list highlights some of our core focus areas, our expertise extends beyond these, ensuring comprehensive security coverage tailored to specific cloud environment:

Amazon Web Services (AWS)

AWS Identity and Access Management Policies
- User Group Policies
- Principle of Least Privilege
- Inline and Assume Role Policies

AWS S3 Configuration Review
- Publicly Exposed S3 Buckets
- Server-Side Encryption
- TLS Used By Buckets

VPC Configuration Review
- Security Groups
- NACLs
- Flow Logs

API Gateway Configuration Review
- Client Certificates
- API Cache
- Access Logs

AWS Lambda
- Code Signing
- Exposed Functions
- Lambda Cross Account Access

AWS Key Management Service and Encryption
- Key Rotation
- Exposed Keys
- KMS Cross-Account Access

Amazon Elastic File System (EFS)
- EFS Encryption
- KMS Customer Master Keys for EFS Encryption

Amazon Elastic Kubernetes Service
- EKS Security Groups
- Kubernetes Cluster Logging
- Cluster Node Group IAM Role Policies
- EKS Cluster Node Groups

Amazon Simple Queue Service (SQS)
- SQS Cross Account Access
- SQS Dead Letter Queue
- Exposed SQS Queue
- Server-Side Encryption

AWS Secrets Manager
- Secrets Manager
- Secret Rotation
- Secret Encryption with KMS Customer Master Keys

Amazon Web Application Firewall
- Logging for Web Access Control Lists
- WAF against Web Exploits

Microsoft Azure

Azure Kubernetes Service (AKS)
- Cluster Disks and Encryption
- RBAC for Kubernetes
- Backups for AKS Clusters
- Private Kubernetes Clusters
- AKS Cluster Credentials

API Management
- TLS with API Gateways
- Unrestricted API Access

PostgreSQL
- Log Retention
- Database Exposure

Activity Logs
- Alerts for Security Events

Container Apps
- Public Network Access
- Azure Container Apps and Insecure Traffic
- Peer-to-Peer Encryption

Storage Accounts
- Infrastructure Encryption
- Secure Transfer in Azure Storage
- Soft Delete for Azure Blob Storage

Network
- Unrestricted Services
- Log Retention
- DDoS Protection on Virtual Networks
- Azure Network Watcher

Google Cloud Platform (GCP)

GCP Cloud Storage
- Data Retention Period for Cloud Storage
- Data Access Audit Logs
- Usage and Storage Logs
- Public Access Prevention
- Service Controls for Cloud Storage Buckets

GCP Certificate Manager
- SSL Certificates

GCP API
- Cloud Asset Inventory
- Critical Service APIs
- Google Cloud API Keys

GCP BigQuery
- Encryption with Customer-Managed Keys
- Publicly Accessible BigQuery Datasets

What we cover:

GCP VPC
- Legacy Networks
- Unrestricted Services
- Default VPN Networks
- Logging for VPC Networks

GCP Domain Name System (DNS)
- Dangling DNS Records
- DNSSEC Key-Signing Algorithm
- DNSSEC Zone-Signing Algorithm

GCP Compute Engine
- Publicly Shared Disk Images
- Load Balancers for Managed Instance Groups
- Interactive Serial Console Support
- Old Persistent Disk Snapshots

GCP Identity and Access Management (IAM)
- Google Cloud API Keys
- Primitive Roles
- User-Managed Service Accounts Keys
- GCP IAM Configuration

Kubernetes
- Role Based Access Control Configuration
- Mutual TLS Communication
- Kubernetes API Server and etcd Configuration
- Namespace Isolation Configuration
- Control Plane and Managed Services
- API Server and Misconfigurations
- Legacy Attribute-Based Access Control
- Privileged Containers
- Kubernetes Secrets
- Network Policies and Misconfigurations
- Use of Istio or Linkerd
- Internal Service Exposure
- Persistent Volume Claims
- Managed Container Registries (ECR, GCR, ACR)
- Kubernetes Service Configuration Review
- AWS EKS
- Azure Managed Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)

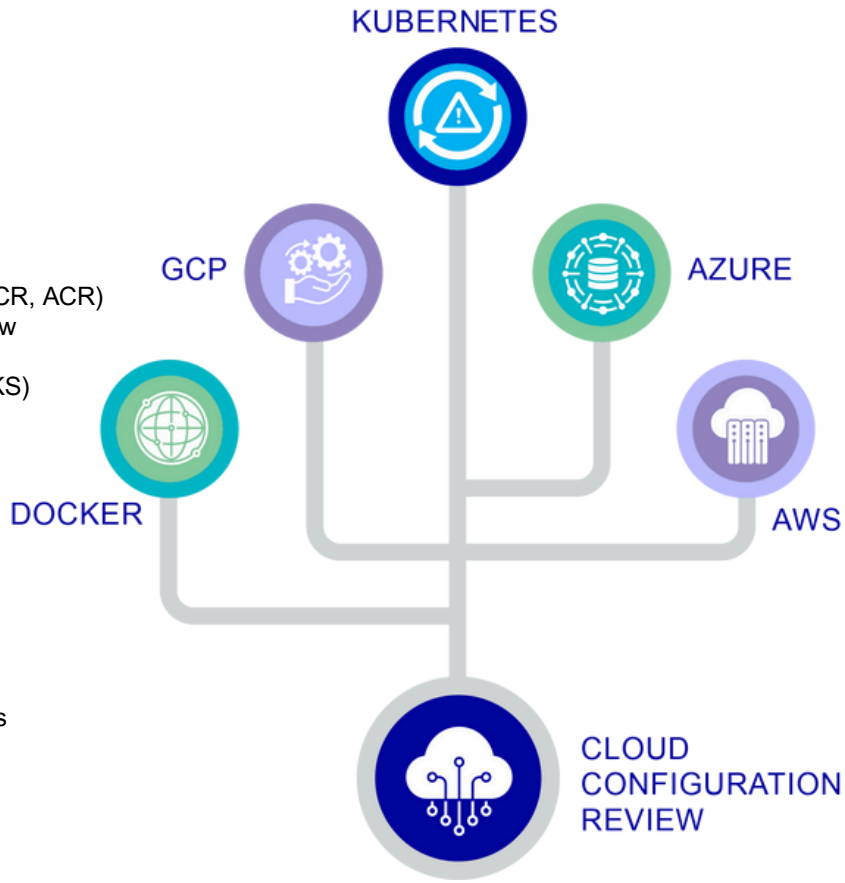
Docker
- Cgroups and Hosts
- User Accounts and Host Permissions
- Docker Daemon and TLS Encryption
- Restricted Access to Docker Socket
- Privileged Docker Daemon
- Namespace for Container Isolation
- Docker Daemon Logs
- Container Images and Trusted Registries
- Image Patch Management
- Docker Runtime Security
  - ReadOnly Flags
  - NoNewPrivileged Flags
  - CapDrop Flag
  - AppArmor or SELinux

Network Security
- User-Defined Docker Network
- Iptables and Network Traffic
- Docker Network Configuration

Volume and Storage Security
- hostPath Volumes
- Storage Backend and Sensitive Data

Monitoring and Logging
- Syslog or fluentd
- Docker Daemon Logs
- Real-time Monitoring
- Docker API Access Logs

In addition to these areas, our review can include any specific services, configurations, or use cases unique to your cloud architecture. Whether it's tailored assessments for serverless environments, advanced identity and access controls, or emerging cloud services, we adapt our approach to ensure complete security coverage.



CLOUD CONFIGURATION DIMENSIONS

INTERNAL THREAT SIMULATION

Internal Threat Simulation, also referred to as Insider Threat Simulation, is a systematic process aimed at identifying and evaluating potential security risks posed by internal actors, such as employees, contractors, or partners. These actors may intentionally or unintentionally compromise an organization's security, making this simulation a critical aspect of cybersecurity. The primary goal of Internal Threat Simulation is to:

Understand how internal threats can impact an organization's overall security posture.
Enhance defenses against insider threats by identifying gaps and weaknesses in existing controls.

What we cover:

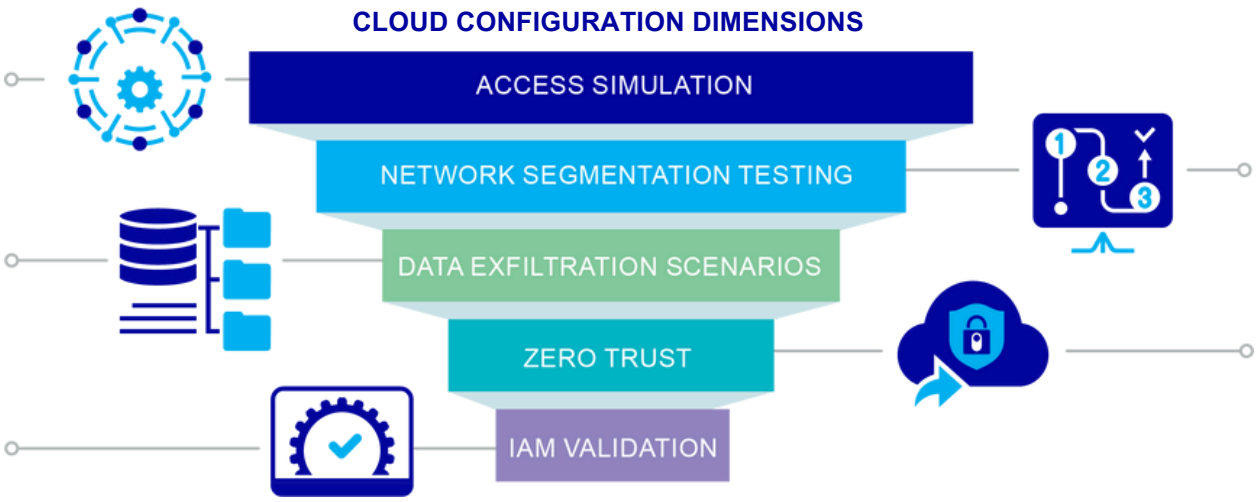
Access Simulation
- Basic Permissions Testing: Start with default employee, contractor, or partner-level access to evaluate potential misuse or exploitation.
- Privilege Escalation Attempts: Identify vulnerabilities that could allow unauthorized users to elevate their privileges and gain greater access to sensitive resources.

Testing Network Segmentation
- Lateral Movement Analysis: Assess whether internal users can move across different segments of the network or access restricted areas.
- Micro-Segmentation Validation: Test segmentation within the network to ensure critical assets are isolated and not easily accessible.

Data Exfiltration Scenarios
- Sensitive Data Access: Simulate attempts to access confidential files, databases, or intellectual property.
- Exfiltration Detection: Test the organization's ability to detect and respond to unauthorized data transfers.

Zero Trust Model Validation
- Policy Testing: Evaluate the implementation and enforcement of Zero Trust principles, ensuring all access requests are authenticated, authorized, and continuously validated.
- Continuous Monitoring: Test the effectiveness of monitoring systems in detecting and flagging anomalous insider activities.

Identity and Access Management (IAM)
- Role-Based Access Control (RBAC): Validate that access controls align with the principle of least privilege.
- Authentication Mechanisms: Assess the strength of password policies, MFA (Multi-Factor Authentication), and otherauthentication mechanisms.



CLOUD SECURITY ASSESSMENT

The objective of this service is to simulate real-world attacks on cloud infrastructure and configurations to uncover potential vulnerabilities and weaknesses. This includes testing cloud-native applications, APIs, and network security controls through a combination of automated and manual assessments. The Cloud Security Assessment service is designed to evaluate the security of cloud environments by identifying vulnerabilities, assessing configurations, and testing the effectiveness of security controls. This service caters to two primary aspects:

Penetration Testing
Vulnerability Assessment

What we cover:

Network Security

- Firewall Configuration: Review and test the effectiveness of firewall rules, including ingress and egress traffic controls.
- Network Access Controls: Validate the use of security groups, NACLs (Network Access Control Lists), and equivalent mechanisms to ensure proper traffic filtering.
- Perimeter Security: Assess the configurations of VPNs, load balancers, and public-facing services to identify exposure risks.
- DDoS Protection: Evaluate existing Distributed Denial of Service (DDoS) mitigation strategies using cloud-native tools like AWS Shield, Azure DDoS Protection, or GCP Cloud Armor.
- Traffic Encryption: Test the implementation of secure communication protocols (e.g., TLS/SSL) to ensure end-to-end data encryption.

Network Segmentation

- Segmentation Validation: Assess the logical isolation of cloud resources using Virtual Private Clouds (VPCs), subnets, and private endpoints.
- Micro-Segmentation: Evaluate whether sensitive workloads are isolated from less critical resources and verify the use of fine-grained security controls.
- Environment Separation: Ensure segmentation between production, staging, and development environments to prevent unauthorized access or data leakage.
- Traffic Restrictions: Validate network policies and route tables to ensure that only necessary traffic is allowed between network segments.

Network-Specific Attack Scenarios

- We simulate and evaluate defenses against the following attacks:
  - Man-in-the-Middle (MITM) Attacks
    - Test for vulnerabilities in secure communication channels that could allow interception or tampering of traffic.
    - Ensure proper implementation of certificate management and transport security protocols.
  - Lateral Movement
    - Assess the ability of an attacker to move within the cloud network once initial access is gained.
    - Test the effectiveness of segmentation and monitoring controls in limiting the attacker's movement.
  - Exposed Services and Ports
    - Identify publicly accessible services and test them for potential exploitation.
    - Ensure misconfigurations in cloud networking components, such as public IPs attached to sensitive workloads, are addressed.
  - DNS Spoofing and Poisoning
    - Evaluate DNS configurations to detect vulnerabilities that could allow attackers to redirect traffic to malicious destinations.
  - Subdomain Takeovers
    - Test for orphaned DNS records or misconfigured subdomains that could allow attackers to hijack unused resources.
  - Identity and Network Interaction
    - IAM Integration with Networking: Validate the integration of Identity and Access Management (IAM) roles with networking services to prevent over-permissioned access.
    - Privileged Access Testing: Simulate scenarios to test the misuse of network resources by privileged accounts

COMPREHENSIVE CLOUD SECURITY ASSESSMENT

CONTAINER SECURITY

This service assesses the security of containerized applications and their orchestration within cloud environments. This service ensures that all components of container security, including container images, runtime environments, and orchestration platforms like Kubernetes, are evaluated and secured against potential threats.

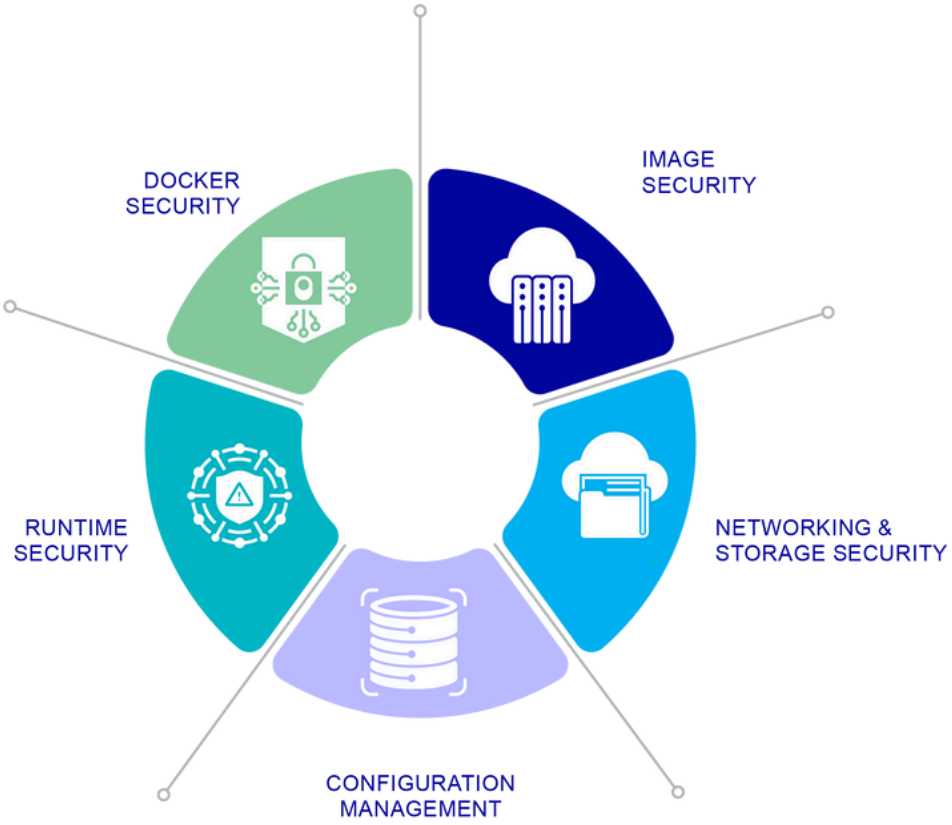
What we cover:

Docker Security

- **Image Security**
  - Base Image Analysis: Identify vulnerabilities in base images, ensuring they are updated and originate from trusted sources.
  - Embedded Secrets: Detect and remediate sensitive information such as API keys or credentials stored in images.
  - Image Scanning: Perform static analysis to identify known vulnerabilities using tools like Docker Security Scanning or Trivy.
- **Runtime Security**
  - Least Privilege Enforcement: Ensure containers run with minimal privileges and avoid privileged mode unless absolutely necessary.
  - Container Isolation: Validate the effectiveness of namespaces and groups in isolating workloads.
  - Runtime Monitoring: Monitor live containers for anomalous behavior such as privilege escalation or unexpected network calls.

- **Networking and Storage Security**
  - Network Segmentation: Evaluate Docker network configurations to ensure proper isolation between containers.
  - Volume Security: Assess mounted volumes to prevent unauthorized access to sensitive data on the host system.
- **Docker Configuration Management**
  - Dockerfile Review: Check for insecure practices, such as using latest tags, excessive layers, or improper caching.
  - Daemon Security: Harden Docker daemon configurations to prevent unauthorized access or exploitation.

COMPREHENSIVE CONTAINER SECURITY OVERVIEW



SECURITY INNOVATION
A BUREAU VERITAS COMPANY

About Security Innovation / Bureau Veritas

Security Innovation is a leader in software security, providing comprehensive assessment solutions to secure software from design to deployment, across all environments, including web, cloud, IoT, and mobile. Leveraging decades of expertise and as part of Bureau Veritas, a global leader in Testing, Inspection, and Certification, we seamlessly integrate world-class security into development processes, safeguarding the way companies build and deliver products.

Security Innovation is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80,000 employees and is active in 140 countries.

BUREAU VERITAS 1828

Interested?

Contact us today to start raising your cyber resilience.

sisales@securityinnovation.com
+1 877 839 7598
securityinnovation.com