Infopercept Proprietary Material

Managed Cloud Security
Technical Approach
Cloud Market Growth

**Storage**
(object storage, archive, backup etc.)

**Productivity applications**
(email, collaboration, instant messaging etc.)

**Business applications**
(CRM, marketing automation ERP, BI, project management etc.)

**IT operations applications**
(administration, backup, provisioning monitoring etc.)

Workload

- Storage: 43%
- Productivity applications: 41%
- Business applications: 42%
- IT operations applications: 39%
Cloud Security Challenges

- Lack of visibility in cloud Security
- Insecure interfaces
- Unauthorized Access
- Lack of knowledge of cloud compliance
- misconfigurations of cloud services
- Improper access controls
- Data Loss & Data Leakage
Cloud Security Services Delivered by Infopercept

2. Web Application Firewall Management against OWASP Top threats
3. Identity and Access Management provisioning for Users and Applications
4. Vulnerability discovery, analysis and remediation recommendations
5. Application Security assessment using Static and Dynamic Analysis
6. Infopercept Kubernetes Security Services
7. Cloud Security Automation

"Infopercept Proprietary Material - Please do not copy or distribute"
Infopercept Security Services from the Cloud

Help Secure your Cloud application deployment and release management

Help provide proactive identification and remediation of vulnerabilities

Help plan, strategize and manage your security vision

Game plan for Cloud security Management

Security Threat Management Service

Development Security Operations

Manage Security Assessment

Security Event and log Monitoring

SOS Threat Analysis Service

Help assess your cloud config changes, policies, security features and reporting

Help Monitor and analyze security events

Customized security threat intelligence based on Infopercept research on threat landscape

Security Threats • Identity • Data • Apps • Cloud Workload

"Infopercept Proprietary Material - Please do not copy or distribute"
Elements of Cloud Environment

- Computer
- Network
- Storage
- Monitoring
- Infrastructure Management
- Application Management
- Devops
- Serverless
- Container Services
- Artificial Intelligence
- Internet Of Things
- Machine Learning
- Media Services
- Platform As a Service – PaaS
- Software As a Service – SaaS
- Infrastructure As a Service – IaaS
- Compliance As a Service – CaaS

*Infopercept Proprietary Material - Please do not copy or distribute*.
Managed Cloud Security Model

- Cloud Architecture Security Assessment
- Web Application Firewall
- Hosted application Security
- Identity Based Security
- Encryption of storage
- Network Security
- IPS/IDS
- Best Practices Architecture
Managed Cloud Security Model

- DR Setup
- DevSecOps
- Audit Ready Compliance Cloud Architecture
- Deep Analysis
- Continuous Patch Management
- Continuous Asset Management
- Monitoring & Alerts
Managed Cloud Security Model

- Virtual Security Operations Centre
- Automation in a Security
- Automation Remediation
Approach to data security in the Cloud

Understand, define policy
- Discover where sensitive data resides
- Classify and define data types
- Define policies and metrics

Secure and protect
- Encrypt, redact and mask virtualized databases
- De-identify confidential data in non-production environments

Actively monitor and audit
- Monitor virtualized databases and enforce review of policy exceptions
- Automate and centralize the controls needed for auditing and compliance (e.g., SOX, PCI)
- Assess database vulnerabilities

Establish compliance and security intelligence
- Automate reporting customized for different regulations to demonstrate compliance in the Cloud
- Integrate data activity monitoring with security information and event management (SIEM)
Managed Cloud Security Priorities

• Define Strategy Framework
• Assess the cloud-based risk
• Follow Cloud Best practices with scenario
• Defending against Malwares
• Reaching regulatory compliance
• Securing Cloud Apps in use
• Preventing Cloud mis-configurations
• SecDevops
• Continuous Monitoring & evaluation of Security
Integrating Security across IT Silos

- Security Devices
- Servers & Hosts
- Network & Virtual Activity
- Database Activity
- Application Activity
- Configuration Info
- Vulnerability Info
- User Activity

Security Event Correlation

High Priority Security Incidents

Security Policies and Rules Tuning

Diverse Data Sources

- Detecting real time threats
- Consolidating data silos
- Detecting insider fraud

Accurate and Actionable Security Incident Response

- Predicting risks against your business
- Addressing regulatory mandates
SIEM Security Event Monitoring

**Identity federation**
- Provisioning identities for public and hybrid cloud environments or Native IAM
- Identity and Access Management

**Web application scanning**
- Security Application Scanning for cloud based applications
- AppScan Static / Dynamic Analysis

**Virtualization security**
- IDS/IPS for VMware ESX / ESXi hosts and Cloud Native IPS for workloads
- Malicious traffic monitoring

**Network security**
- Cloud Native IDS/IPS for VPC and Vnet
- Malicious traffic monitoring

**Image and patch management**
- Vulnerability scanner for continuous assessment
- Assess/Patch

**Database monitoring**
- Weak default passwords, Database misconfiguration, missing security patches
<table>
<thead>
<tr>
<th>Audience</th>
<th>Development Teams</th>
<th>Security Teams</th>
<th>Penetration Testers</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDLC</td>
<td>Coding</td>
<td>Build</td>
<td>QA</td>
</tr>
<tr>
<td>Scanning Techniques</td>
<td>Dynamic analysis</td>
<td></td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>Black box</td>
<td></td>
<td>Production</td>
</tr>
<tr>
<td>Applications</td>
<td>Static analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>White box</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance &amp;</td>
<td>Programming Languages</td>
<td>Web Applications and Services</td>
<td>Mobile Applications</td>
</tr>
<tr>
<td>Collaboration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated</td>
<td>Build Systems</td>
<td>Defect Tracking</td>
<td>Development</td>
</tr>
<tr>
<td></td>
<td>Improve scan</td>
<td>System track</td>
<td>Environments</td>
</tr>
<tr>
<td></td>
<td>efficiencies</td>
<td>remediation</td>
<td>Remediation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>assistance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Intelligence raise</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Threat level</td>
</tr>
</tbody>
</table>

- Test policies, test templates and access control
- Dashboards, detailed reports & trending
- Manage regulatory requirements such as PCI, GLBA and HIPAA (40+ out-of-the-box compliance reports)

*"Infopercept Proprietary Material - Please do not copy or distribute".*
Cloud PMO

- Analysis & Design
- Implementation
- Cloud Compliance
- Process Compliance
- Process Risk
- Technical Risk
- Cloud Security Services
- Cloud Monitoring
- Cloud Security Team
- Risk & Process Team
- Compliance Team
- Cloud Architect Team

"Infopercept Proprietary Material - Please do not copy or distribute"
Infopercpet provides cloud security assessments from AWS, Azure, and Google Cloud Platform. We use automated tools, manual verification, and expert analysis to determine gaps that exist in your cloud security configuration. We can also assess web applications running in the cloud that may have vulnerabilities that could lead to infiltration and pivoting within your cloud environment. If desired, we can evaluate your development and deployment processes, CICD pipeline, and overall architecture of your cloud and hybrid cloud infrastructure.
SCOPE

We perform the following activities during an assessment of your AWS, Azure, or GCP account:

• Run automated scanning tools to assess the account
• Manually validate assessment findings in AWS, Azure, or GCP
• Assessments may include some reverse engineering and limited code review
• Cloud architecture reviews are also available upon request
• Staff interviews and documentation review, if available
Engagement

- We perform testing at a mutually agreeable time with the client.
- The testing period is a defined period with a start and end date.
- We perform tests from an AWS region; customers must provide network access.
- Rate limiting needs to be turned off to perform application vulnerability scans and testing.
- Contacts must be available who can help restore access as needed.
- We report in as desired by the client.
- We require C-Level executive approval for automated scanning.
- Customers need to provide appropriate credentials and respond in a timely manner.
How We Pentest your AWS, Azure, or GCP Account

At Infopercept, we focus on helping you improve security - not just finding some obscure way to attack your systems. We do more than use a tool to scan your systems and generate an automated report. We do leverage tools and automation and have a set process for performing penetration tests on cloud accounts. By using the same approach each time, we can dive deeper faster and provide more value. We execute a combination of assessment and penetration activities to determine the overall security of your account and the applications running in it. We provide analysis of each finding to offer mitigation steps your team can use to fix the problem and additional resources for those who want to dive deeper.
SCOPE

We perform the following activities during a pentest of your AWS, Azure, or GCP account:

- Web application testing to see if vulnerable applications provide access.
- Assess cloud configuration in AWS, Azure, or GCP.
- Tests include some reverse engineering and limited code review.
- Cloud architecture reviews are also available upon request and will require system documentation.
- We perform fuzzing for maximum coverage since the time for testing is limited.
Engagement

- Tests are performed part-time at random times over 3 to 4-week period
- The testing period is a defined period with a start and end date
- We perform tests from an AWS region, and network access must be available
- We test in non-production environments and can verify in production
- Rate limiting needs to be turned off for fuzzing to work
- Contacts must be available who can help restore access as needed
- We report in as desired by the client
- We require the approval of a C-Level executive to perform the test
- Customers need to provide appropriate credentials and respond in a timely manner
Cloud Penetration Testing Process

The cloud penetration process is different due to dynamic nature ephemeral resources and limitations on certain types of testing. Testers must understand cloud technologies and cloud provider-specific requirements related to scope. We request cloud credentials with a specific role and domain names, URLs, and an AWS account number instead of IP addresses. We test from dynamic IP addresses in an AWS region. We help customers understand the process further in the setup phase of the penetration test. We aim for coverage over stealth.

High-level penetration testing steps:

- Define scope and rules of engagement with the customer
- Set up and Reconnaissance
- Scan web applications, network, and cloud account
- Exploitation
- Validation of findings by various tools
- Report Writing and Delivery

Penetration Testing Report

Our reports include high-level and detailed prioritized findings, steps to reproduce, recommended remediation, and additional resources related to each finding.
Cloud Penetration Testing Process

Kubernetes Services

- Aqua Security
- Capsule8
- Cavirin
- Google SCC
- Layered Insight (Qualys)
- Neuvector
- StackRox
- Sysdig Secure
- Tenable Container Security
- Twistlock (Palo Alto)

Recommended Security platform for Kubernetes

- Kubernetes image scanning and static analysis
- Kubernetes runtime security
- Kubernetes network security
- Image distribution and secrets management
- Kubernetes security audit
Cloud Continuous Security Solution by integrating below points

- Write custom rules & remediation action
- Integration with change management
- Integrating with security automation tools
- Integration with end to end vulnerability remediation tools
Infopercept’s vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners’ cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

**Imprint**
© Infopercept Consulting Pvt. Ltd. 2021

**Publisher**
H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

**Contact Info**
M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

By accessing/proceeding further with usage of this platform/tool/site/application, you agree with the Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions, kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.