intellias

Cloud Security Assessment

We breathe life into **great ideas**
with the power of **digital technology**

Inc. Power Partner

IAOP THE BEST OF The Global Outsourcing 100

Forbes Best IT employer in Ukraine

EY Building a better working world

2024 | intellias.com

Imagine if you could

ADDRESS

the following needs:

- Identify and mitigate security threats
- Ensure compliance with industry regulations
- Provide expert guidance on cloud security
- Identify and resolve misconfigurations
- Assess and optimize infrastructure security automation

intellias

Top Cloud Challenges*

Lack of Cloud Security architecture and strategy

Abuse and nefarious use of cloud services

Misconfiguration and inadequate change control

Inside threat

Account hijacking

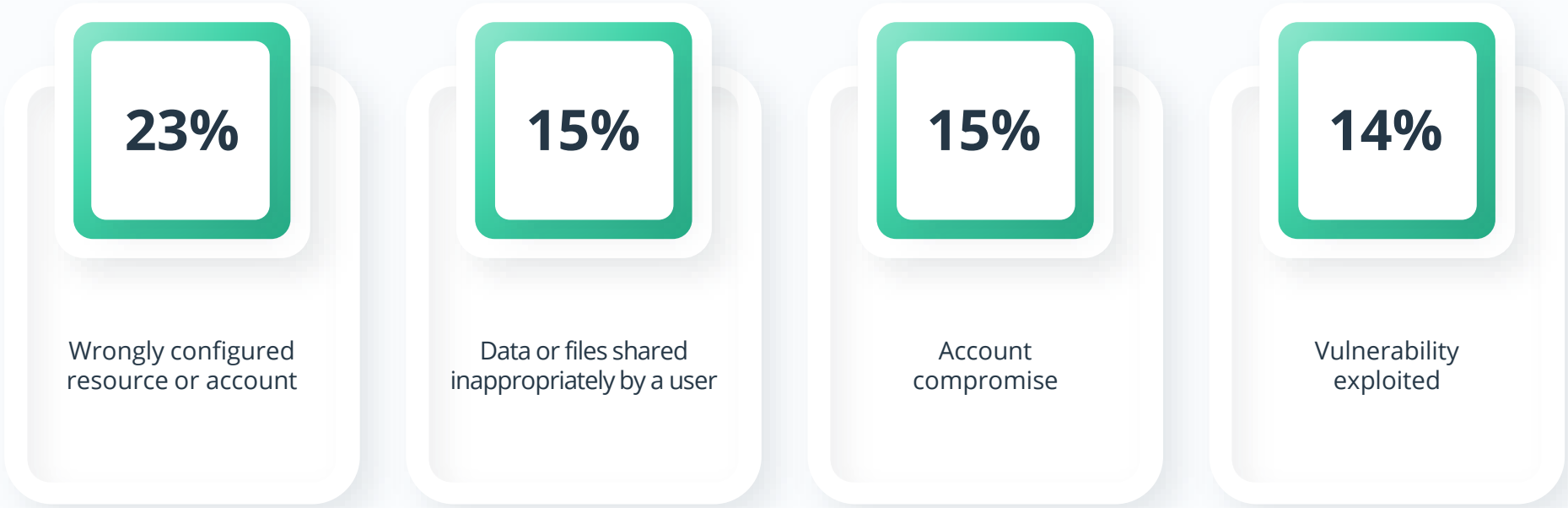
Insufficient identity, credential, access and key management

Insecure interfaces and APIs

Weak control planes

* According to Cloud Security Alliance

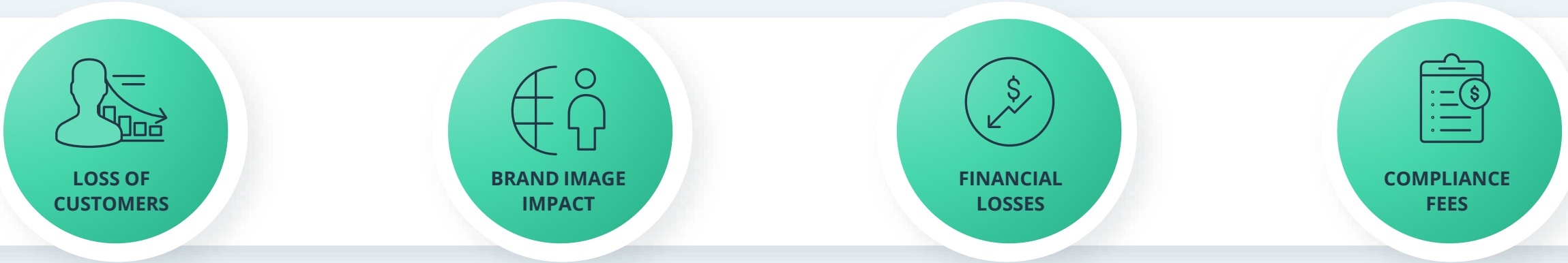
Top Causes of Cloud Security Incidents*



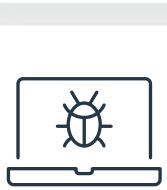
Data or files uploaded to an unsanctioned cloud resource 12% | Malware infection 9% | Data or files downloaded to an unsafe device 9% | Other 8%

* According to Check Point Cloud Security Report

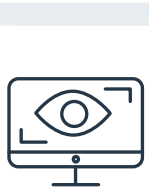
Cloud Security Breach: Business Impact



What Companies Typically Do

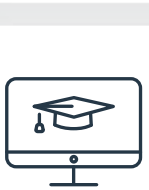


Penetration testing/
vulnerability scanning



Security
monitoring

Hiring
security experts



Training sessions
for personnel

Cloud security
tools

Intellias Service Approach

Requirement Definition

- Identifying security requirements and objectives based on your organization needs and project peculiarities
- Defining security level for the specific cloud infrastructure: fundamental, industry standard, or advanced

Controls Validation

- Verifying a security baseline checklist by leveraging automated tools, custom-built scripts, and manual review
- Conducting in-depth architecture analysis with further evaluation against reference architecture
- Executing an external attack surface discovery

Recommendations

- Estimating cyber risks and cloud security breach likelihood along with the scale of their potential impact on your business
- Issuing actionable recommendations structured by priorities and criticality levels

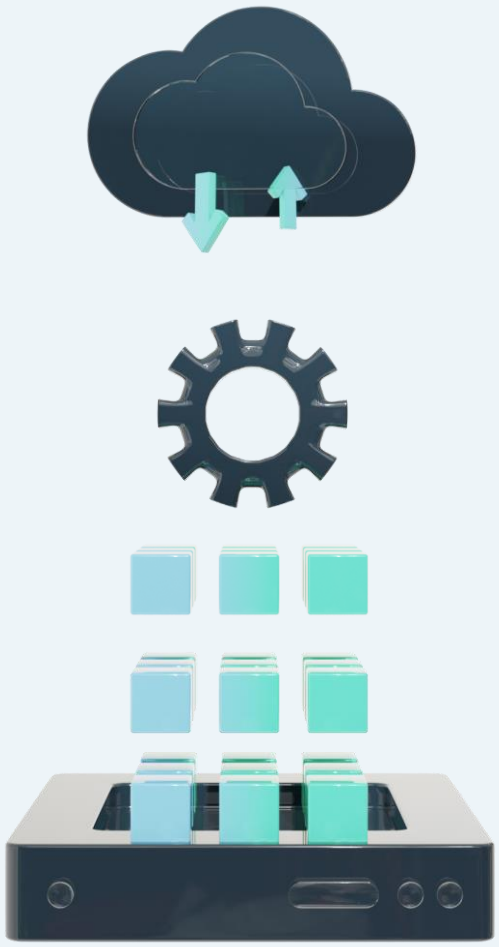
Assessment Components

Governance
An in-depth analysis of organization's security posture, policies, and procedures to identify potential vulnerabilities, risks, and compliance gaps

Architecture
Analysis of cloud infrastructure's architecture to identify potential weaknesses in the design and implementation of security controls

CIS Benchmark
Validation of the security baseline checklist using a combination of automated tools, custom-built scripts, and manual checks

Perimeter Scan
Scanning of organization's external-facing assets, such as servers, applications, and network devices, to identify potential vulnerabilities and security gaps



High-Level Assessment Roadmap

Kick-off meeting

- Presenting the service, its execution flow and outcomes
- Aligning the implementation flow and schedule

Week 1

Information gathering

- Filling out the questionnaire
- Collecting documentation and other related artifacts
- Identifying security requirements based on your organization and project needs
- Q&A session

Interview

- Clarifying uncertainties
- Obtaining access to additional materials

Week 2

Week 3-5

Assessment

- Reviewing documents and assets
- Conducting interviews with relevant personnel
- Analyzing system configurations and to identify potential risks
- Examining and validating processes and policies affecting cloud security

Reporting

- Collaborating with your team to resolve disputes related to security policies, controls, and findings
- Preparing an assessment report and arranging a meeting to discuss findings
- Providing recommendations on how to resolve the issues identified

Week 5

Week 6

Next steps

- Security control implementations
- Maintenance and support

Report Structure

Executive Summary	A resume of the assessment findings, including an overview of the organization's cloud environment, identified vulnerabilities, and recommendations for improvement. Written in non-technical language.
Assessment Methodology	Explains the methodology used to conduct the assessment, including the tools and techniques used to gather data and evaluate the organization's cloud security posture.
Cloud Architecture Analysis	In-depth analysis of the organization's cloud architecture, including an assessment of the cloud service provider (CSP) selected, the types of cloud services used, and any security controls in place.
Governance Assessment	Evaluation of the organization's cloud governance framework, including policies, procedures, and guidelines related to cloud security. Identifies if the organization has a clear understanding of its roles and responsibilities in terms of securing its cloud environment.
CIS Security Fundamentals Assessment	Evaluation of the organization's compliance with security best practices for cloud environments, including identity and access management, configuration management, data protection, network security, and application security.
OSINT/Perimeter Scan	An overview of the organization's public-facing assets and its perimeter security, including an analysis of any vulnerabilities or potential threats.
Recommendations	Specific recommendations for improving the organization's cloud security posture, including proposed actions towards mitigating identified vulnerabilities and risks. It is typically organized by priority and includes both technical and non-technical recommendations.
Evidence	Provides evidence of the assessment, including any documentation or logs collected during the assessment phase. It is included to support the findings and recommendations presented in the report.

EXPERTISE

Cloud Security Assessment Levels

	Standard	Plus
Risk management and compliance	-	+
Asset management	-	+
Human resources security	-	+
Change management	-	+
Identity and access management	+	+
Secure configuration of enterprise assets and software	+	+
Network configuration and protection	+	+
Application software security	+	+
Data protection	+	+
Incident response	+	+
Backups and disaster recovery	+	+
Logging and monitoring	+	+
Vulnerability management	+	+
Architecture review	-	+
Perimeter scan	+	+

intellias

EXPERTISE

Cloud Security Assessment Standard

You are

A company that utilizes a cloud infrastructure for storing sensitive data or performing critical business functions, which:

- needs to comply with industry-specific regulations and standards, such as HIPAA, PCI DSS, or GDPR
- does not have dedicated security personnel or lacks expertise in the cloud security space
- requires to identify potential security risks and implement best practices for mitigating them

You get

- Baseline security check
- Reviewed security policy in accordance with the CIS Benchmark
- Quick insight and expert-led guidance on cloud security controls improvement
- Report that identifies if your applications meet or fail to meet security criteria defined by the List of Cloud Misconfigurations

EXPERTISE

Cloud Security Assessment Plus

You are

A company that operates complex cloud environments, handles sensitive data, and prioritizes strong security measures. Your cloud infrastructure has a complex structure with multiple components and interdependencies. You are looking to:

- identify potential security gaps, scalability issues, and other areas for improvement that impact the overall performance of your cloud environment
- get an external perspective and validate your existing security controls

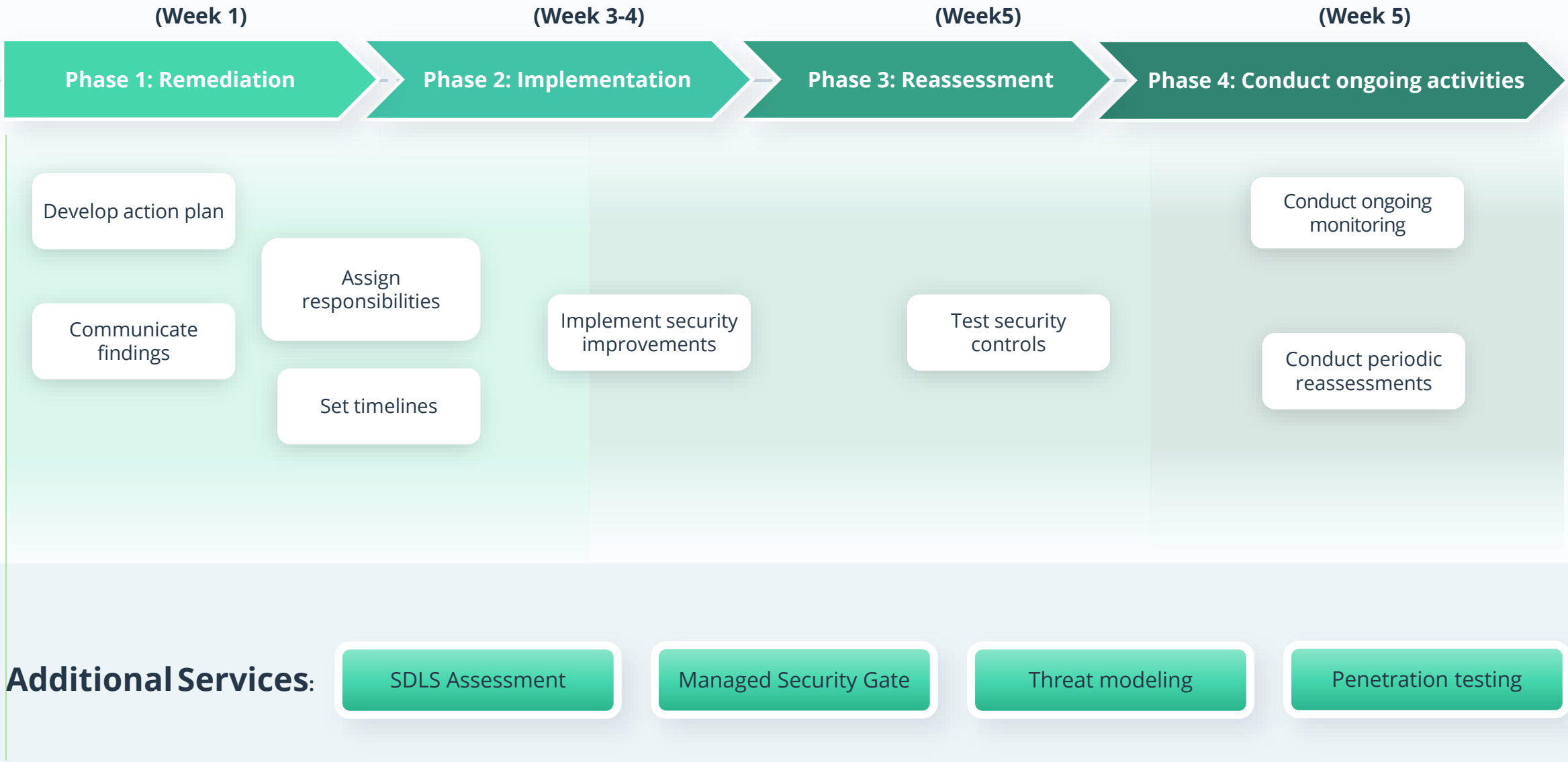
You get

- Manual in-depth analysis
- Expert-led assessment of cloud security/ program
- More effective cloud operations, architecture and strategy
- Mature cloud security architecture aligned with business objectives and risk profile

intellias

EXPERTISE

Express pathway - Roadmap



Additional Services:

- SDLS Assessment
- Managed Security Gate
- Threat modeling
- Penetration testing

intellias

Thank you!

Let us engineer the digital strength of your business!

Lviv

24 Panasa Myrnoho Street,
Lviv 79034

info@intellias.com

Krakow

Al. Pokoju 18C, 31-564,
Kraków Fabryczna Office Park

info-krakow@intellias.com

Chicago

500 West Madison Street,
60661

info-chicago@intellias.com

Learn more about **Intellias**