Security

GEORGEJON

GEORGEJON.COM

Security Audits

Knowledge is power.

The George Jon Security Team will conduct an end-to-end security assessment of your environment and operating model, from planning to execution.

We will conduct on-site and virtual interviews, coupled with remote environment review sessions, to diagnose the current state of your security posture. This is followed by a gap analysis, relative to industry best practices, and recommendations for galvanizing your environment across the following parameters:

- Data workflow and data management, including the end-to-end data handling process, from acquisition through remediation
- Identity and access management solutions for optimization opportunities and gap/weaknesses identification in process and controls
- Vulnerability management, from scanning to remediation, aligned with business SLAs
- Encryption methodologies in conjunction with data workflow and management
- Security architecture relative to zone separation, perimeter controls, egress filtering, and proxy internet access
- Cybersecurity operations, response plans, and process effectiveness/preparedness
- Application security configurations and recommend baseline images for security enhancement

SECURITY AUDIT BENEFITS

Identifies weaknesses in your security posture that expose your business to unnecessary risk

Explains industry Best Practices and how other organizations in the eDiscovery realm are protecting their environments

Provides insight across security tools and controls, backed by GJ testing, that ensures efficacy while avoiding platform performance and stability degradation

Forges a clear and defined roadmap for achieving a “Desired State” environment security posture

Delivers an end-to-end overview of your current data handling and management workflow, identifying key areas for improvement

SECURITY AUDIT FRAMEWORK

Our solution framework for conducting and delivering successful client Security Audits consists of three holistic phases to ensure we not only capture and present an accurate representation of your current state, but also understand and construct a roadmap for achieving the ideal future state.

PHASE 1

GJ holds client workshops and gathers environment security documentation, conducting a 360-degree security review of the environment to determine the current baseline state.

Information Gathering
- Security vision and management expectations
- Current InfoSec policies and procedures
- Existing environment documentation
- Data workflow documentation
- Client-required information security controls

Assess and Baseline the Current State
- Security tools and configuration
- Cyber Ops and response plan
- Data handling and encryption
- Security-based environment pain points

PHASE 2

GJ compares the current state baseline against industry-specific security best practices to deliver a gap analysis across key security controls, prioritized by risk severity and expectations.

Gap Analysis
- Data encryption
- Identity and access management
- Vulnerability management and patching
- Security operations (SIEM)
- Security architecture
- Data handling

Prioritize Security Findings
- Alignment to management expectations
- Alignment to industry best practices
- Alignment to contractual requirements
- Budget considerations
- Implementation intensiveness (complexity, impact, tradeoffs)

PHASE 3

George Jon's Security Team will deliver a final Security Assessment Report & Executive Summary detailing key areas for risk mitigation and outlining the "Desired State".

Security Health Report and Remediation Roadmap
- A comprehensive view of the current state, identifying critical security weaknesses and the associated remediations
- Prioritization of security concerns and the associated risks aligned with management acceptance
- Detailed implementation plan broken down by workstream, with budgetary and timeline estimates