ATOMICdata

SECURITY & COMPLIANCE

CYBERSECURITY ESSENTIALS

The cyberthreat landscape has never been more volatile, making security hardening indispensable. You need experts on the front lines to defend and protect your business, and we're here to help.

After testing and fine-tuning our approach, we've put together a security and compliance strategy built upon four core pillars: Policy & Procedure Consulting and Development, Security Awareness Training & Phishing Simulation, Vulnerability Scanning and Management, and Security Operations Center as a Service (SOCaaS).

Policy & Procedure Consulting and Development

We'll review your current security and compliance documentation to architect recommendations. The process begins with an initial analysis phase to identify organizational goals and compliance requirements followed by a development phase where we'll collaborate to write, publish, and enforce your new policies and procedures.

Security Awareness Training & Phishing Simulation

Policies will dictate a need for ongoing security awareness training. We'll step up your IT hygiene by implementing monthly phishing campaigns to counter the quickly evolving cyberthreat landscape.

Vulnerability Scanning and Management

With automated vulnerability scanning and management, we'll identify, manage, and remediate technology risks, exploits, and threats. By leveraging industry-leading tools, we'll bring visibility to your vulnerabilities, assess risk levels for each exposure, and develop a plan for both initial and ongoing remediation.

- Routine, interval-based scans
- Endpoint vulnerability detection
- Risk assessment & prioritization
- Remediation workflows
- Patches & security enhancements
- Scheduled vulnerability reports

Security Operations Center as a Service (SOCaaS)

Atomic Data's Security Operations Center team is built on three core functions: threat detection, incident response, and mitigation. We'll leverage Security Information and Event Management (SIEM) software to aggregate data & continuously monitor a wide range of data sources across all environments.

- Firewalls
- Servers (AD, ISE, etc.)
- HTTP/TLS
- DNS
- Email gateways
- Wireless access points
- Infrastructure as a Service
- Workstations
- Software as a Service