NIS2 Compliance Help

Everyone deserves the best protection

NIS2 Compliance
Security Consulting

Our NIS2 Cybersecurity Consulting team identifies and helps eliminate security configuration vulnerabilities in your IT infrastructure.

WE HELP CUSTOMERS INTEGRATE CYBERSECURITY INTO THEIR DAILY OPERATIONS VIA OUR SECURITY PROGRAM PLAN

SMB BREACH FACTS

Most security breaches and data leaks happen in small businesses. They usually go unnoticed for years due to SMBs having little to no in-house resources to detect or respond to cybersecurity threats.
Security Monitoring, Breach Detection, Security Hardening, Security Awareness were usually only available to larger organizations due to their complexity and price.

WE ARE HERE TO CHANGE THAT

As organization migrate to the cloud at a rapid pace, they often lose track of everything they store in the Cloud. This presents a significant threat to their security posture and could lead to financial and regulatory penalties, especially in the event of a breach. Cybersecurity breach insurance rarely covers negligence on behalf of a customer's IT team. This is where our consulting solutions provide clarity in identifying the vulnerabilities and misconfigurations in place and providing a remediation plan to implement the right security controls.

HOW ATLANT | SECURITY CAN HELP

We have developed and extremely efficient methodology to protect small businesses from complex cybersecurity attacks.
Our customers get the same quality a bank would – because our team consists of CISOs previously worked at banks, nuclear power plants and telecoms.

Our team consists of ex-Microsoft security experts with a broad and deep understanding of the underlying principles of protecting data in the cloud.

CUSTOMER BENEFITS

- Protect your small business better than all your closest competitors and use this as your own competitive advantage
- Identify the potential business impact of all discovered vulnerabilities and prioritize their remediation based on business value
- Obtain detailed, technical remediation recommendations which are easy to follow by any IT team
- Ongoing monitoring and reporting of any new misconfiguration in the future (optional)

SECURITY EXPERTISE

Our consultants come from nuclear, government, financial and technology giant backgrounds, with a wide array of security certifications in both offensive and defensive skills.

They have served on both sides – at the cloud providers themselves and on the customer side, which gives them a unique set of skills in identifying security gaps in the logical and technical security configurations of small businesses.

Service Range

We help customers with cloud forensics and incident response, security assessments and consulting services.

2-day NIS2 Assessment

Most organizations can be audited for NIS2 compliance within 2 business days. If yours is larger or smaller, we will tailor our service to accommodate the size of your company and infrastructure. The NIS2 Assessment will identify the high-priority tasks that need to be executed immediately and we will help you prioritize them.

NIS2 compliance planning

During the Planning phase, we will build a NIS2 compliance plan for your organization which will help guide resource allocation for the months ahead.

Implementation and Compliance

Our team will work closely with yours to help all aspects of your business transform and comply with the NIS2 cybersecurity requirements.

3 Steps to your NIS2 compliance:

- 2-day NIS2 assessment
- 1-week NIS2 compliance planning
- Implementation and Compliance

THESE ARE JUST SOME OF THE AREAS COVERED BY OUR ASSESSMENTS. THE FULL LIST DEPENDS ON THE CLOUD PROVIDER AND ON THE DEPLOYMENT – COMMUNICATIONS, SERVERS, APPS, OTHERS

Prevent. Detect. Respond.

IDENTITY & ACCESS MANAGEMENT

The most critical area for all cloud customers and the most widely abused by attackers and insiders. Failures here most often lead to security breaches and data leaks. Administrators often abuse their powers and leave their own accounts unprotected.

LOGGING AND MONITORING

All external access to your cloud environment should be logged and those logs should be immutable. In addition, you should enable monitoring capable of detecting anomalies such as logins from new locations, large data transfers and attempts to breach security controls.

MICROSOFT 365 AND GOOGLE APPS

Microsoft 365 and Google's Apps offer great usability and security features, but many of them are turned off by default or are available only after deep reconfiguration. Each has more than 280 security settings, each of them needs a business impact assessment before implementation.

DATA STORAGE SECURITY

Many governments require a certain level of data encryption at rest and in transit, but customers should also check their file / folder encryption and key storage / access security, access controls and file activity monitoring, backup and restore practices, among many others.

VIRTUAL MACHINE SECURITY

Virtual Desktop Infrastructure and Virtual Servers need to be checked for proper access controls, logging, encryption, shared storage security, resource utilization management and segmentation control.

DATABASE SECURITY

We observe a rapid increase in the public availability of misconfigured ElasticSearch and other databases, exposed by mistake by developers, QA and IT. In addition, each database has hundreds of security settings and each of them could be misused by an attacker.

Cybersecurity is in our blood. We live and breathe defense and love helping customers with it

About Atlant | Security

Atlant | Security ® is a global cybersecurity company serving clients in the

Contact us for a free consultation.