SECURITY

Atlantica Digital SpA

Information Security

Cyber Security

Training e formazione

Security Product

Atlantica Digital S.p.A.
Via Barberini, 29 - 00187 Roma; Tel. 06 4620171 Fax 06 4746655
www.atlantica.it email: atlanticadigital@atlantica.it;
Cap. Soc. € 1.058.800,00; CF/P.IVA 14650841001

Offerta Security di Atlantica Digital

L'offerta Security di Atlantica Digital copre la totale esigenza di protezione dei propri Clienti, è articolata in componenti complementari, utilizzabili anche singolarmente per adeguarsi ad ogni specifica esigenza; in particolare la proposta è organizzata a copertura delle seguenti aree di interesse:

1. **Information Security**
2. **Cyber Security**
3. **Security Training**
4. **Security Product**

A) *Information Security*

La proposta nell'ambito della "**Information Security**" si configura come Servizi di Consulenza ad elevato valore aggiunto, in grado di coprire tutte le esigenze di difesa del business e di compliance:

GDPR Compliance, ***NIS Compliance***,***ISO 27XXX Compliance***, ***Misure Minime AgID, Risk Analysis, Cyber Security Act***.

B) *Cyber Security*

La proposta dell'area "**Cyber Security**" è basata sui servizi coordinati ed erogabili dal next generation SOC (Security Operation Center) di Atlantica Cyber Security.

Servizi SOC primari:

- ***MDR – Managed Detection and Response basato su protezione End Point IT***
- ***CVA - Continuos Vulnerability Assessment delle infrastrutture IT***
- ***SOC OT***
- ***SOC OT & IOT***

Altri Servizi avanzati: ***Monitoraggio attivo, Analisi e correlazione, Incident Response, Early Warning, Security Awareness, Vulnerability Assessment/Penetration Test, Threat Intelligence, Malware Analysis, Forensic.***

C) *Security Training*

Corsi di formazione per le figure professionali in ambito Security

D) *Security Product*

SAM (Security Administration Management): un prodotto di Atlantica Digital dedicato alla gestione ed al controllo totale delle utenze privilegiate, per l'accesso in sicurezza, il monitoraggio delle attività e le possibili registrazioni legali di sessione.

A) Information Security

A1) Governance Risk & Compliance

Le consulenze di Governance coprono le esigenze di compliance a leggi, regolamenti e/o standard internazionali riconosciuti ed è prevista la possibilità di certificazione per ciascuna attività.

A2) Periodical Audit

Con frequenza stabilita da un programma studiato in base alle criticità e alla dinamica del business viene eseguito un ciclo di audit tale da mantenere alta l'attenzione sui processi della security.

A3) Advisory

E' il servizio consulenziale che recepisce i risultati della Governance Risk & Compliance e dell'Internal audit per fornire soluzioni di metodo e di processo alle vulnerabilità tecnico-organizzative riscontrate, anche grazie ai risultati dei servizi forniti dall'area Cyber Security. L'attività consiste nel fornire soluzioni organizzative e/o procedurali e della relativa formazione ai destinatari.

A4) Education & Awareness

E' il punto di forza per garantire l'efficacia dell'Advisory. Periodicamente sono avviate sessioni di awareness finalizzate a verificare il grado di attenzione e consapevolezza degli interessati.

B) Cyber Security

B1) MDR - Managed Detection and Response protezione End Point IT

Con il servizio di Managed Detection and Response è possibile gestire in modo centralizzato l'analisi, la gestione e la risposta agli incidenti su endpoint, server e dispositivi mobili. Il servizio gestito prevede l'analisi, la correlazione degli eventi, la risposta agli incidenti e l'automazione della risposta di contenimento e/o eradicazione delle minacce.

B2) CVA - Continuos Vulnerability Assessment delle infrastrutture IT

Il SOC fornisce servizi di Vulnerability Assessment e Penetration Test, sia in sinergia con le attività di monitoraggio delle minacce, sia in modalità stand-alone.

B3) Servizi SOC OT/IoT

Nell'ottica del continuo scouting tecnologico, Atlantica Cyber Security, ha individuato le migliori tecnologie più performanti e tecnicamente avanzate nell'ambito dei sistemi di OT-IoT Security.

Le componenti utilizzate integrano funzionalità di monitoraggio per i dispositivi OT e IoT, compresa l'analisi comportamentale sulle reti OT, oltre a sistemi di intelligence in grado di rilevare minacce informatiche, vulnerabilità, rischi e anomalie. Inoltre, attraverso la protezione della flash memory dei dispositivi critici.

B4) SOC OT

Il livello di servizio del SOC OT è basato su due diversi parametri funzionali:

- Active Monitoring.
- Analysis and Correlation
- Active Response.

Il Security Operation Center contrasta e risponde agli incidenti di sicurezza rispettando le fasi del framework NIST:

- Preparazione
- Rilevamento e Analisi
- Contenimento, Eradicazione e Recupero
- Post Incident Activity

B8) Early Warning

Il servizio di Early Warning ha come obiettivo principale l'individuazione tempestiva delle principali minacce informatiche, relative alle casistiche del cliente, che potrebbero avere un impatto rilevante sull'infrastruttura informatica e sul business.

B9) Security Awareness

Le attività di Security Awareness comprendono le azioni di formazione e di sensibilizzazione che vengono fornite al personale specialistico, e non, nel settore Informatico.

B10) Brand Protection e Fraud Management

Attraverso l'utilizzo del servizio di Brand Protection e Fraud Management è possibile individuare ed eventualmente contrastare l'utilizzo non legittimo del brand del cliente.

B11) Threat Intelligence

Il servizio di Threat Intelligence è volto a raccogliere, condividere e identificare le informazioni relative alle minacce, alle strategie e agli attori che si celano dietro le minacce stesse.

B12) Analisi Malware

Il servizio permette di analizzare malware o file sospetti in ambienti controllati e con le tecniche più avanzate di analisi dinamica e statica.

B13) Forensic

Il servizio Forensic ha lo scopo di individuare, estrarre, conservare e proteggere documenti a fini probatori senza comprometterne l'integrità (catena di custodia).

L'analisi Forense consente l'acquisizione di informazioni da dispositivi digitali compromessi a seguito di un incidente informatico.

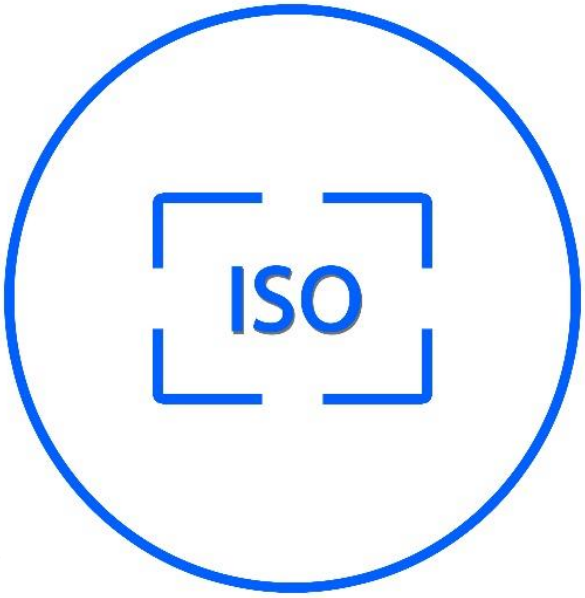
B14) Servizi SIEM

Il servizio di Managed SIEM comprende la totale gestione del SIEM: dall'installazione alla sua configurazione fino al mantenimento e installazione di patch e aggiornamenti, sia esso erogato in modalità MSSP con nostra piattaforma, che attraverso strumenti SIEM in uso al Cliente.

C) Security Training

Corsi di formazione per le figure professionali Governance and Technician:

- **GDPR (DPO Certificabile)**
- **GDPR (Formazione al personale)**
- **GDPR (Formazione E-Learning)**
- **NIST (Formazione al personale)**
- **ISO 9001 (Lead Auditor certificabile)**
- **ISO/IEC 20000-1 (Lead Auditor certificabile)**
- **ISO/IEC 27001 (Lead Auditor certificabile)**
- **ISO/IEC 27017 (Lead Auditor certificabile)**
- **ISO/IEC 27018 (Lead Auditor certificabile)**
- **ISO/IEC 27035 (Lead Auditor certificabile)**



Certificazione aziendali rilasciate da OdC Accreditato:

- **ISO 9001 Qualità**
- **ISO/IEC 20000-1 Servizi ICT**
- **ISO 22301 Business Continuity**
- **ISO/IEC 27001 Sicurezza delle Informazioni**
- **ISO/IEC 27017 Sicurezza dati di business nel Cloud**
- **ISO/IEC 27018 Sicurezza dei dati personali nel Cloud**
- **ISO/IEC 27701 Sistema di Gestione Protezione Dati Personali**
- **ISO/IEC 27035 Gestione degli incidenti di sicurezza delle informazioni**
- **ISO/IEC 25010 Qualità del Software**

D) Security Product

Prodotto Atlantica di Sicurezza Accessi, “SAM”

SAM (Security Administration Management) è una soluzione per la sicurezza degli accessi completamente sviluppata e supportata da Atlantica:

- È una piattaforma di gestione degli accessi privilegiati flessibile e veloce
- È una piattaforma per il tracciamento delle attività degli utenti privilegiati e per l'accesso alle risorse aziendali critiche
- È una soluzione agentless e clientless che si integra facilmente nell'infrastruttura IT dei clienti

Un'ampia varietà di soluzioni in un'unica piattaforma

- Monitoraggio e tracciamento delle attività sui sistemi critici
- Monitoraggio e tracciamento dell'accesso del fornitore esterno ai sistemi IT
- Indagine sulla violazione dei dati (GDPR)
- Riduzione del rischio di possibile esfiltrazione di dati dall'azienda
- Rilevazione dei tentativi di accesso non autorizzati