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 (Assessment and advisory – Periodical audit), ***NIS Compliance*** (Risk assessment – Advisory - Education & awareness - Periodical Audit), ***ISO 27XXX Compliance*** (Risk assessment – Advisory - Education & awareness - Periodical Audit), ***Misure Minime AgID (***Adeguamento obbligatorio per le PA), ***Risk Analysis (***strumento fondamentale per la Business Impact Analysis), ***Cyber Security Act (***Regolamento europeo per la certificazione della sicurezza di prodotti e servizi in ambito ICT).

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

Il servizio consiste in un esame iniziale del contesto normativo di esercizio, dei processi di business e di supporto dell'organizzazione che interessano il perimetro di sicurezza. Per ciascun processo si selezionano i key-user e i risk owner e attraverso una serie di interviste si identificano gli asset gestiti, le principali vulnerabilità e le minacce correlate al contesto di esercizio. Valutato il rischio si scelgono le contromisure idonee all'abbattimento del medesimo e si propone il remediation-plan.

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. Il criterio di audit si basa sulla conformità alle procedure sulla security che l'organizzazione ha deciso di adottare ed applicare le best practice di settore. Il servizio rilascia un report con il grado di conformità e gli eventuali rilevi che saranno gestiti con il supporto dell'attività di Advisory.

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. Analizza elementi di attenzione e di criticità nei processi dell'organizzazione, raccoglie gli elementi procedurali più significativi enfatizzando le condizioni d'errore. Viene eseguita in modalità continua, sia con sessioni in aula che in modalità e-learning. Per ciascuna sessione è previsto un test di verifica di apprendimento. 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 sui seguenti moduli e funzioni:

- Anti-Malware
- Next-Generation Antivirus
- Anti Ransomware
- Active and Automation Response
- Active Hunting

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.

Tali attività possono essere svolte manualmente o tramite l'utilizzo di tools automatizzati. L'utilizzo di tali tool permette di schedulare nel tempo test periodici.

Le attività di Penetration Test, che si differenziano per modalità e tecniche da quelle di Vulnerability Assessment, sono volte a tentare di sfruttare nella pratica le vulnerabilità note, o sconosciute, in una rete.

Tali attività sono strettamente controllate e vengono effettuate con la dovuta attenzione per evitare di causare danni incontrollati nel perimetro target.

I target su cui è possibile effettuare attività di VA/PT sono:

- Applicazioni Web
- Reti e Sistemi (Infrastruttura informatica interna)
- Dispositivi Mobili
- Dispositivi OT/IoT
- Reti Wireless

La modalità di scelta dei test può essere definita tra "white box", "grey box" e "black box".

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, vengono introdotte le seguenti funzionalità:

- Prevenzione da danni locali
- Protezione da bug di SW e vulnerabilità sconosciute
- Protezione, validazione e gestione degli update "over-the-air"
- Validazione di real-time status, alert & forensic
- Rapido disaster recovery in caso di cyber breach o errore umano

B4) SOC OT

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

- Active Monitoring: è il servizio che prevede il monitoraggio, con differenti SLA operativi, degli alert e delle criticità, con conseguente segnalazione al cliente del problema rilevato;
- Active Response: è il servizio che abbina all'Active Monitoring anche la response e l'eventuale remediation sui dispositivi critici protetti con la tecnologia Nanolock.

B5) Monitoraggio attivo

Gli analisti di sicurezza che compongono il Security Operation Center Team svolgono nella routine quotidiana (h24 x 7) il monitoraggio attivo degli allarmi correlati all'infrastruttura completa del cliente (rete, Server, pc, dispositivi IoT, ecc.) relativi ad eventuali o potenziali minacce. Il monitoraggio attivo è anche il processo mediante il quale gli analisti del SOC monitorano e valutano i Malop, allarmi generati nell'ambiente dell'organizzazione dalla piattaforma software e forniscono raccomandazioni in merito concise e utilizzabili.

B6) Analisi e correlazione

Il Security Operation Center si occupa di analizzare e correlare allarmi ed eventi. L'analisi è necessaria per ridurre al minimo i falsi positivi. Il processo di analisi prevede la correlazione degli eventi che generano un allarme e la relazione che altri eventi hanno con esso.

B7) Incident Response

Le azioni di 'Risposta' agli incidenti hanno lo scopo di analizzare, contrastare, rimediare ed eventualmente eradicare minacce alla sicurezza di reti e sistemi cercando di evitare o minimizzare l'impatto che le stesse possono avere sul business aziendale.

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.

Il personale è altamente qualificato e in continuo aggiornamento nello studio e rilevazione delle nuove minacce tramite l'utilizzo di fonti esterne pubbliche (OSINT) e interne (ricerca e sviluppo interno).

Lo scopo del servizio di Early Warning è quello di dotarsi velocemente di adeguate contromisure a contrasto delle minacce.

Le attività di Early Warning prevedono l'invio di comunicazioni periodiche ufficiali (bollettini di sicurezza) per allertare prontamente i referenti preposti dal Cliente su informazioni relative alle vulnerabilità, software malevoli, campagne di phishing mirate (spear phishing).

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.

Lo scopo principale è quello di aumentare la consapevolezza e la conoscenza sulle principali e più comuni minacce informatiche (Phishing, Vulnerabilità, Policy, utilizzo di password deboli, navigazione web su siti poco legittimi, ecc.) cercando di diminuire la possibilità di errore umano che solitamente e nella maggior parte dei casi rappresenta la vulnerabilità più critica.

Le attività di Security Awareness possono essere svolte tramite webinar e/o seminari in presenza.

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.

Il monitoraggio della reputazione del Brand è effettuato h24 attraverso l'utilizzo di tool automatici, e in seguito, tramite l'analisi svolta dal SOC.

È possibile fornire i seguenti servizi relativi al Brand Protection e al Fraud Management:

- Individuazione dell'utilizzo improprio del brand online: l'utilizzo improprio e non autorizzato da parte di qualsiasi servizio online del brand del cliente (esempio: vendite non autorizzate, utilizzo del brand con fini fraudolenti, ecc.).
- Individuazione dell'utilizzo improprio del brand a fini di phishing: tentativi di attacco phishing che sfruttano l'immagine di un'azienda per rendere l'attacco più efficace.

- Individuazione dell'utilizzo di domini simili o con estensioni differenti (.com, .it): il Domain Fraud consiste nell'utilizzo di nomi di dominio molto simili (es. estensione differente rispetto al dominio originale) col l'obiettivo di ingannare l'utente/vittima proponendo una struttura del sito web similare o identica all'originale.

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.

Il team di intelligence si occupa di ricercare, tramite informazioni pubbliche e non, eventuali attività di attori o gruppi (Advanced Persistent Threat) che hanno come target principale organizzazioni specifiche.

Tipologie di Servizi erogabili:

- Info Leak e Data Breach detection
- Indagini OSINT
- Dark Web Monitoring

Info Leak e Data Breach Detection

Il servizio di Info Leak e Data Breach Detection comprende diverse tipologie di elementi. È prevalentemente volto a scoprire la presenza di "Data Leak" ("fuga di Dati" intenzionalmente resa pubblica) contenenti informazioni più o meno sensibili quali:

- Credenziali di account aziendali compromessi e/o esposti
- Credenziali bancarie e/o di altri metodi di pagamento
- Informazioni e documenti aziendali riservati

Indagini OSINT

Tramite le attività di Open Source Intelligence (OSINT) è possibile ottenere informazioni su aziende, individui, situazioni provenienti da fonti pubbliche.

Le attività di indagine OSINT consentono inoltre di effettuare una analisi e correlazione tra minacce e attori.

Dark Web Monitoring

Il monitoraggio del Dark Web consente di rilevare qualsiasi tipo di informazione pubblicata nelle piattaforme nascoste (forum nella "darknet", black market, siti web, ecc.).

L'attività può essere svolta sia in modalità attiva che passiva, ovvero in sinergia tra le due. La prima prevede la ricerca e l'analisi attiva da parte degli analisti specializzati, la seconda l'utilizzo di tools specifici per la ricerca delle informazioni nel Dark Web (Software di "parsing" e "spidering").

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.

L'analisi dinamica è volta a comprendere il comportamento dei malware, quali: connessioni esterne (analisi traffico di rete), creazioni di chiavi di registro, iniezioni di processi, utilizzo di librerie di sistema legate solitamente ad attività poco legittime, creazione di processi anomali o figli di processi legittimi, ecc. Il tutto viene analizzato in un ambiente controllato e isolato (Sandbox).

L'analisi statica ha lo scopo di analizzare il codice del software malevolo attraverso il debugging e il reverse engineering alla ricerca di anomalie comportamentali nella struttura del codice stesso.

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.

La consulenza tecnica è finalizzata alle seguenti attività:

- Analisi sistemi compromessi con conseguente ricostruzione attività illecite
- Analisi accessi abusivi
- Acquisizione informazioni e dati a fini probatori e non
- Recupero file cancellati

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.

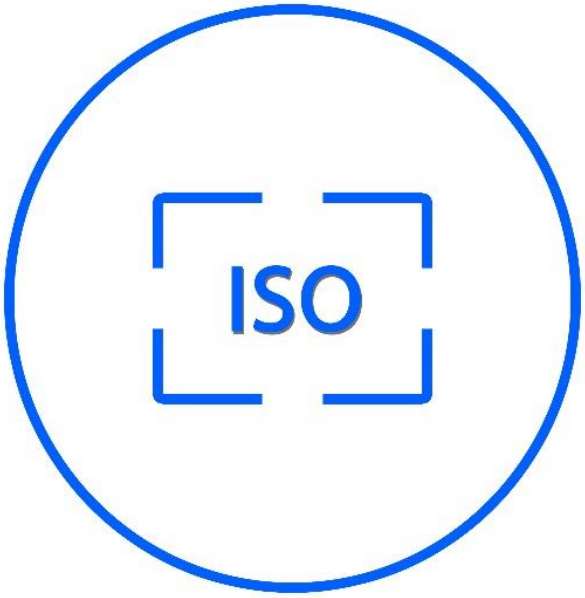
I servizi, erogabili in entrambe le modalità, sono:

- Installazione e configurazione
- Patching e aggiornamenti di sistema (device host) e applicativo web
- Controllo raggiungibilità e stabilità di sistema
- Configurazione, tuning e correlazione regole
- Mapping eventi (log)
- Stesura Parsing personalizzato per tipologia di log
- Integrazione Sorgenti di Log

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**

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