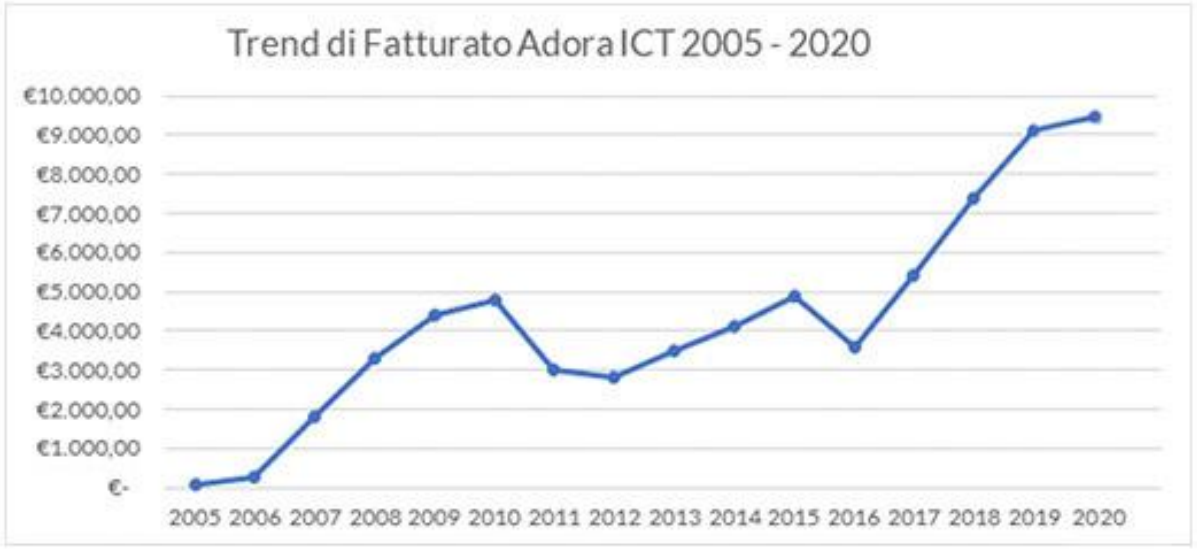
Adora ICT
CyberSecurity Linking Humans

SIAMO UNA CYBERSECURITY FACTORY

E NON SOLO

Adora ICT
CyberSecurity Linking Humans



Chi siamo?

- Costituita il 15 Luglio 2005
- Sedi: ROMA (Principale) Milano, Bari
- Oltre 80 dipendenti
- CEO: Massimo Santangelo

Abbiamo oltre 15 anni di esperienza in ambito ICT. Dal 2005, abbiamo da sempre tenuto in grande considerazione la sicurezza informatica, certi che sarebbe diventata una componente imprescindibile di ogni progetto. Dopo tanta esperienza fatta sul campo con la nostra partecipazione e le nostre competenze siamo pronti a proteggere i nostri clienti sviluppando nuovi servizi ed affiancandoli nel loro core business.

Clusit
Associazione Italiana per la Sicurezza Informatica

Security Services

Vulnerability Assessment

Attraverso tool automatici e personale altamente specializzato, offriamo un servizio di Assessment della sicurezza atto a fornire alle aziende gli elementi utili per poter adeguare la propria infrastruttura, mediante attività di patching, tuning o modifica dei propri asset IT.
Tale attività può essere ripetuta, con cadenze concordate, per avere sempre il controllo della propria sicurezza aziendale.

Penetration Test

Il processo si attua attraverso software specializzati e le competenze dei nostri esperti di sicurezza, i quali possono agire dall'esterno del perimetro aziendale conoscendo o meno il suo asset interno.
L'utilizzo di questi strumenti rende possibile la verifica puntuale del grado di sicurezza della tua infrastruttura.

OSINT

Open Source INTelligence, è un processo di analisi di Intelligence delle Fonti Aperte. È una disciplina adottata da Agenzie di Intelligence per valutazioni tattiche o semplici considerazioni statistiche di tipo operativo e strategico. Si tratta di un metodo di investigazione, ovvero una attività di raccolta, elaborazione ed analisi di informazioni liberamente e legalmente accessibili.

Security Services

IT Risk Management

La gestione del rischio consente di indirizzare le politiche e le contromisure di sicurezza secondo criteri di completezza e concretezza (analisi delle minacce), aderenza al business (valutazione degli impatti), fattibilità tecnico-economica (determinazione e accettazione del rischio residuo), trasparenza e tracciabilità (Statement of Applicability).

I nostri servizi per l'IT Risk Management sono conformi alla ISO27001 e contemplano:

- Modelli di processo per la gestione del rischio IT
- Best Practice sulle relazioni tra rischi e contromisure
- Definizione e pianificazione della risposta al rischio
- Assistenza nei progetti di mitigazione del rischio
- Formazione.

Digital Forensics

La vostra organizzazione ha subito un attacco informatico? Un dipendente infedele ha sottratto informazioni riservate? Gestiamo casi semplici o complessi da uno ad un numero indefinito di device digitali con metodologie ripetibili e adottando standard di riferimento internazionali, come la ISO 27037 per la cristallizzazione e gestione delle prove digitali.
Siamo in grado di gestire diversi casi, adottando i migliori software di analisi disponibili.
Il nostro personale pluricertificato vanta oltre 10 anni di esperienza in ambito privato, Procura e in ausilio alle Forze dell'Ordine, come CTU, CTP e Ausiliari di Polizia Giudiziaria

GDPR Compliance

Con l'arrivo del General Data Protection Regulation- UE 2016/679 (GDPR) le esigenze informatiche delle aziende sono mutate in maniera sensibile per ottemperare ai requisiti del regolamento. Adora ICT è in grado di conformità e di aderenza al GDPR valutando come sanare eventuali difformità, per migliorare la salute della tua azienda e metterla al sicuro dalle sanzioni previste.

Infrastructure Services

Cloud

- Valutazione dell'infrastruttura e delle applicazioni
- Progettazione e implementazione della maggior parte delle piattaforme cloud private/pubbliche/ibride
- Pianificazione di un approccio delle migrazioni per ridurre al minimo il rischio e i costi

DataCenter

- Progettare e creare suite di Data Center personalizzate
- Gestione dell'hardware installare
- Migrazione fisica o di hardware tra Data Center
- Consolidamento del data center
- Pianificazione dettagliata e mitigazione dei rischi

Disaster Recovery

- Valutare requisiti di DR e BCP
- Consigliare Best Practice
- Soluzioni architetturali per supportare gli obiettivi RPO e RTO
- Implementazione di failover e replication
- Creazione, test e manutenzione dei piani di DR

Darktrace

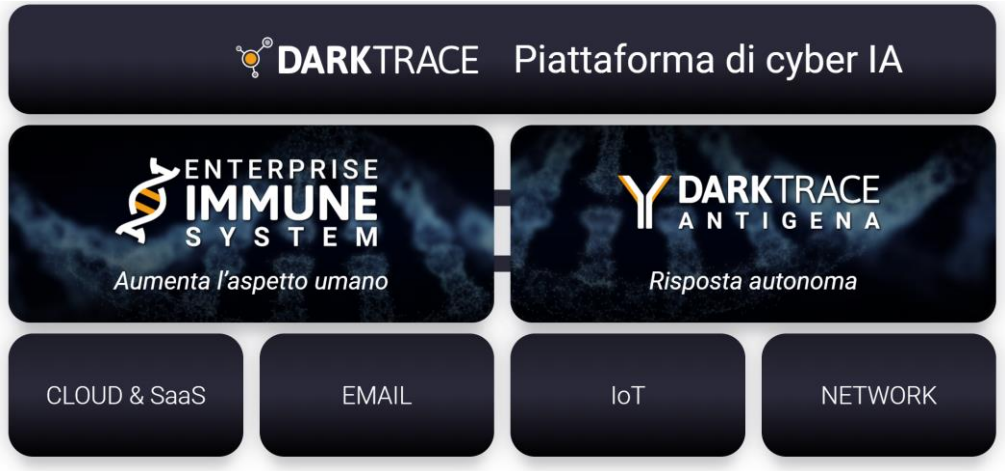
L'applicazione di intelligenza artificiale alle sfide di cyber defense ha segnato un cambiamento fondamentale nella nostra capacità di proteggere i sistemi di dati e le infrastrutture digitali fondamentali.

Se soluzioni basate su regole e firme offrono una qualche protezione contro minacce pre-identificate, la realtà è che oggi gli attacchi eludono continuamente queste soluzioni e ottengono l'accesso alla rete.

La soluzione Darktrace, alimentata da un machine learning "unsupervised, risponde a queste minacce prima che si trasformino in crisi.

La cyber IA è tecnologia di auto-apprendimento che, come il sistema immunitario dell'uomo, apprende "in corsa d'opera" dai dati e dalle attività che osserva in situ. Ciò significa fare miliardi di calcoli basati sulla probabilità alla luce di evidenze in continua evoluzione

Darktrace è compatibile con i principali fornitori di cloud e applicazioni SaaS, fra cui AWS, Microsoft Azure, Salesforce e Office 365. La tecnologia si integra facilmente con dashboard SIEM e ambienti SOC, consentendo ai team della sicurezza di adottare Darktrace senza modificare i processi aziendali esistenti.



Settori di mercato

- Trasporti
- Media e Entertainment
- Tecnologia e Telecomunicazioni
- Servizi Finanziari
- Retail e E-Commerce
- Sanità e Settore Farmaceutico
- Produzione e Manufacturing
- Energia e Utilities
- Governo e Difesa

Circles of Trust (CoT) by CryptoMill

Circles of Trust ™ è una soluzione studiata per eliminare i rischi associati alla violazione dei dati da un attacco a rete, cloud, dispositivo ed e-mail, nonché perdite di dati attraverso dispositivi smarriti o rubati.

CoT consente infatti la protezione in un «Ciclo Continuo» dei dati sensibili.

CoT è una soluzione di sicurezza semplice da usare, che facilita la creazione di un "gruppo di fiducia" composto di utenti, sia interni che, tramite una sandbox, esterni, per la la collaborazione e condivisione sicura di dati sensibili, CoT è in grado di proteggerli ovunque siano. La protezione dei dati è garantita anche quando vengono condivisi tramite e-mail, USB, dispositivi mobili, nel cloud, ecc. Solo i membri fidati possono accedere ai dati crittografati e solo finché fanno parte di quel “gruppo di fiducia”. Uno dei pochi software GDPR compliance!

Convenient Security

No extra passwords, no interruption to workflow, no reworking of business processes.

Learn More

Mobility

Data can be shared securely on any device. Laptops, tablets, smartphones, Windows, Mac, iOS, Android.

Learn More

Offline Access

Data can be shared securely on any device. Laptops, tablets, smartphones, Windows, Mac, iOS, Android.

Learn More

Secure Cross-Border Sharing

Secure Cross-Border Sharing

Learn More

Strong Security

CryptoMill uses AES 256-bit encryption to ensure that all your data remains protected with the highest level of security

Learn More

Varied levels of access

Level 1: Confidently share data with others in a limited, view-only sandbox. Level 2: Empower your core group to edit and collaborate securely.

Learn More

Settori

- Trasporti
- Media e Entertainment
- Tecnologia e Telecomunicazioni
- Servizi Finanziari
- Retail e E-Commerce
- Sanità e Settore Farmaceutico
- Produzione e Manufacturing
- Energia e Utilities
- Governo e Difesa

Sophos Security Suite

SOPHOS
Security made simple.

Nel rapido evolversi delle minacce Sophos offre una soluzione che integra le varie componenti consentendo **tempi di risposta estremamente rapidi nell'applicazione di una remediation efficiente ed efficace.** Il tutto è basato su un'integrazione unica sul mercato di tutte le sue componenti che comunicano fra di loro attraverso un canale condiviso (Sophos Security Heartbeat).

In questo modo l'informazione di una minaccia rilevata dai sistemi perimetrali viene condivisa immediatamente con i vari end-point per un'azione di quarantena che consenta poi agli specialisti IT di intervenire per riportare il sistema colpito alla sua normalità riducendo al minimo l'eventuale diffondersi di minacce.

Componenti Ecosistema Sophos

- XG Firewall
- Intercept X
- Cloud Optix
- Sophos Email
- UTM
- Secure Web gateway
- Sophos Wireless
- Sophos Mobile
- Safeguard Encryption

Adora ICT
CyberSecurity Linking Humans

Incident Response

I controlli di sicurezza informatica, per quanto possano essere adeguati, non sono mai sufficienti a sventare eventuali attacchi informatici e di conseguenza è possibile che incidenti di sicurezza si verifichino anche in aziende che effettuano molto spesso I suddetti controlli.

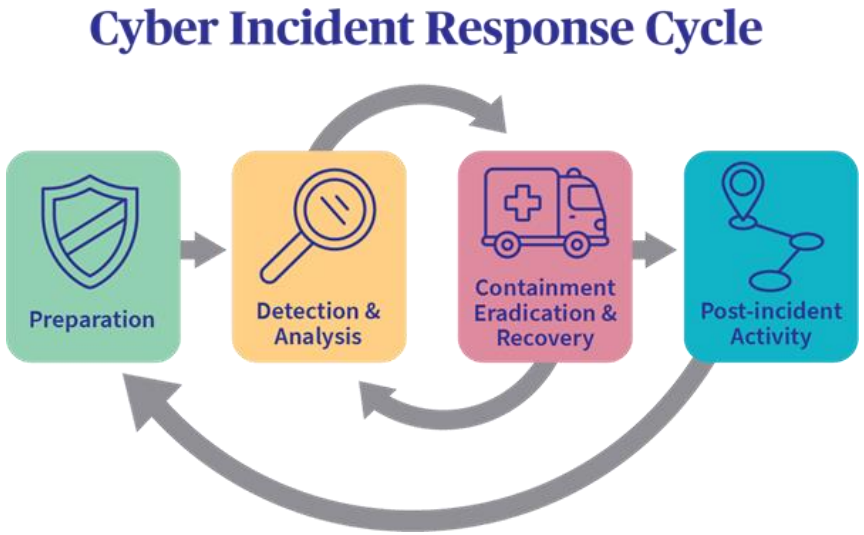
Gli 'Information Security Incidents' riguardano generalmente lo sfruttamento di vulnerabilità non controllate o non riconosciute.

Lo scopo

Adora ICT gestisce gli Incidenti in 5 fasi:

- **Preparazione** – Essere a conoscenza di un possibile incidente e formare un team con competenze utili alla gestione.
- **Identificazione** – Quando avviene un Incidente, identificarlo e documentarlo.
- **Valutazione** – Valutare un incidente (Es. Cyber Triage) e decidere quali contromisure applicare (es. Patching)
- **Risposta** – Contenere l'incidente ed investigare sulle cause e l'impatto, identificando i responsabili quando possibile (Digital Forensics).
- **Apprendimento** – Apprendere cause ed effetti riguardanti l'incidente per evitare che si verifichi di nuovo.

Incident Response



Il piano

La predisposizione di un piano di incident response (o "piano di risposta") costituisce una modalità con cui il titolare, in un'ottica di accountability, non solo si propone di pianificare misure e controlli periodici per evitare incidenti sulla sicurezza del trattamento dei dati, ma conferisce alla propria struttura un "metodo" per gestire la fase "patologica" del trattamento.

Maggiore è il tempo necessario a capire la tipologia di danno, l'entità, il numero di dati coinvolti, nonché necessario a capire quali siano le misure tecniche e organizzative più idonee da attuare per la gestione del rischio specifico, maggiore sarà l'impatto della violazione non solo sugli interessati ma anche, conseguentemente, sulla reputazione dell'azienda.

È pertanto fondamentale che il titolare dell'azienda individui dapprima un rappresentante (il cosiddetto "Incident Lead"), che dovrà gestire operativamente le attività in caso di violazione, coordinandosi però con un team e con gli altri dipartimenti coinvolti, tra cui rientrano il management, le risorse umane, l'area IT, l'area legale, le relazioni pubbliche e il customer care, ciascuno per le proprie competenze ed il proprio ruolo.

Ovviamente presupposto indispensabile ad una corretta formazione del personale in ordine alla gestione del piano di risposta, è una intensa, ripetuta, specifica formazione dei dipendenti sulle procedure da seguire e sulle misure di sicurezza da adottare nelle attività agli stessi demandate che importino il trattamento dei dati personali.

Di seguito un modello di esempio di gestione di un Incident:

Incident Response

Nelle prime 24 ore si dovrà registrare lo stato di fatto e mettere in sicurezza i dispositivi coinvolti nella violazione, avvisare I membri del team di incident response, mettere offline le machine interessate (senza spegnerle), interrogare coloro che sono coinvolti nella violazione o chiunque altro possa conoscerne le cause e avvisare le forze dell'ordine se necessario.

La redazione di un piano di incident response non deve essere considerata come un adempimento statico, da effettuarsi una volta per tutte e che rimane immutato nel tempo.

Perché scegliere noi

Scegliere ADORA-ICT come cyber security partner significa contare su **un team** in grado di **coniugare competenze specialistiche** in materia **di sicurezza informatica,** un forte **orientamento all'innovazione,** l'organizzazione tipica di **un'azienda affermata e dinamica,** ed infine, la capacità che deriva da un'ultra-decennale **esperienza** di accompagnare i propri partners attraverso tutte le sfide dell'IT odierno.

Adora ICT
CyberSecurity Linking Humans

I nostri partner

DARKTRACE
DELL
CryptoMill Cybersecurity Solutions
Microsoft
SOPHOS Security made simple.
KASPERSKY lab REGISTERED PARTNER
HUAWEI
Bitdefender
CYBERA
McAfee
vmware
veeam pro partner
tenable
LIBRA ESVA email security virtual appliance CERTIFIED PARTNER
CYBEROO

Le nostre certificazioni

ISO 9001:2015 COMPANY
ISO 27001 Certified
LEAD AUDITOR ISO 27001
Clusit Associazione Italiana per la Sicurezza Informatica
OSSTMM OPSA Professional Security Analyst
COBIT 5 AN ISACA® FRAMEWORK
CompTIA Security+
CompTIA Security+
CEH Certified Ethical Hacker
LPT Licensed Penetration Tester
OFFENSIVE Security OSCP
Microsoft CERTIFIED AZURE FUNDAMENTALS
PROJECT MANAGEMENT PROFESSIONAL PMP® CERTIFICATION
ITIL® Foundation V3
PRINCE2 PRACTITIONER CPD
Java Sun microsystems CERTIFIED Developer
PEGA CERTIFIED System Architect
Microsoft CERTIFIED ASSOCIATE
CISCO CCNA
SOPHOS Certified Engineer
vmware CERTIFIED PROFESSIONAL Data Center Virtualization 2021
ORACLE Certified Associate
ORACLE Certified Professional
Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

Adora ICT
CyberSecurity Linking Humans

Via Mosca 10, 00142 Roma
Mac4 – Via Benigno Crespi 19 – 20159 Milano
Viale Magna Grecia 51 – 70126 Bari

Info Line:
Tel 0643400115
Fax 064340018

info@adora-ict.com

-