Soluzioni per la continuità aziendale

Dove l'esperienza diventa innovazione ↘

AS Group

AS Group nasce dalla convergenza delle esperienze, delle competenze e della conoscenza di tutti coloro che hanno contribuito alla progressiva crescita del progetto All Services.

Il compito di AS Group è di fungere da fulcro direzionale per tutte le realtà che coinvolge, analizzando i mercati e gli scenari futuri, tracciando le rotte da seguire.

Il suo ruolo è quello di gestire le identità di ogni azienda e prodotto che ne fanno parte, di coordinare il network di partner e affiliati, di armonizzare le strategie per affrontare le sfide del futuro.

Vision

Essere un polo di eccellenza nella cultura tecnologica e imprenditoriale, di innovazione di processo e prodotto e di sicurezza per l'ICT aziendale e privata, instaurando nuovi standard metodologici e promuovendo buone pratiche di efficacia ed efficienza.

Mission

Garantire tempestività, affidabilità e concretezza ad ogni nostro Cliente e su ogni nostra attività.

Parola d'ordine: continuità

Informatica, digitalizzazione, automazione, networking, cloud: oggi le imprese e perfino le vite dei privati fondano i propri equilibri sulle tecnologie della computazione e della comunicazione.
Un guasto ad un hardware o un malfunzionamento di un software possono compromettere ore di lavoro, opportunità, hobby, relax, quotidianità.

La tecnologia si può riparare o sostituire ma il tempo, la continuità lavorativa e le informazioni perse a causa di un guasto costituiscono un danno irrecuperabile.

e-Zen è un pacchetto integrato di soluzioni per la continuità informatica, con funzioni di analisi predittiva della stabilità dei sistemi e della qualità delle performance, di backup automatico in cloud, di assistenza diretta da remoto e di assistenza hardware, tutto volto a un solo scopo: arrivare a prevenire il problema, e se proprio non fosse possibile evitarlo, risolverlo con la più totale tempestività e sicurezza.

Care

Servizio predittivo di monitoraggio e assistenza remota per client, dispositivi mobile, server e network con possibile estensione di garanzia hardware in base al livello di servizio scelto.

Small

- SPOC (ticketing)
- Assistenza Remota (4h)

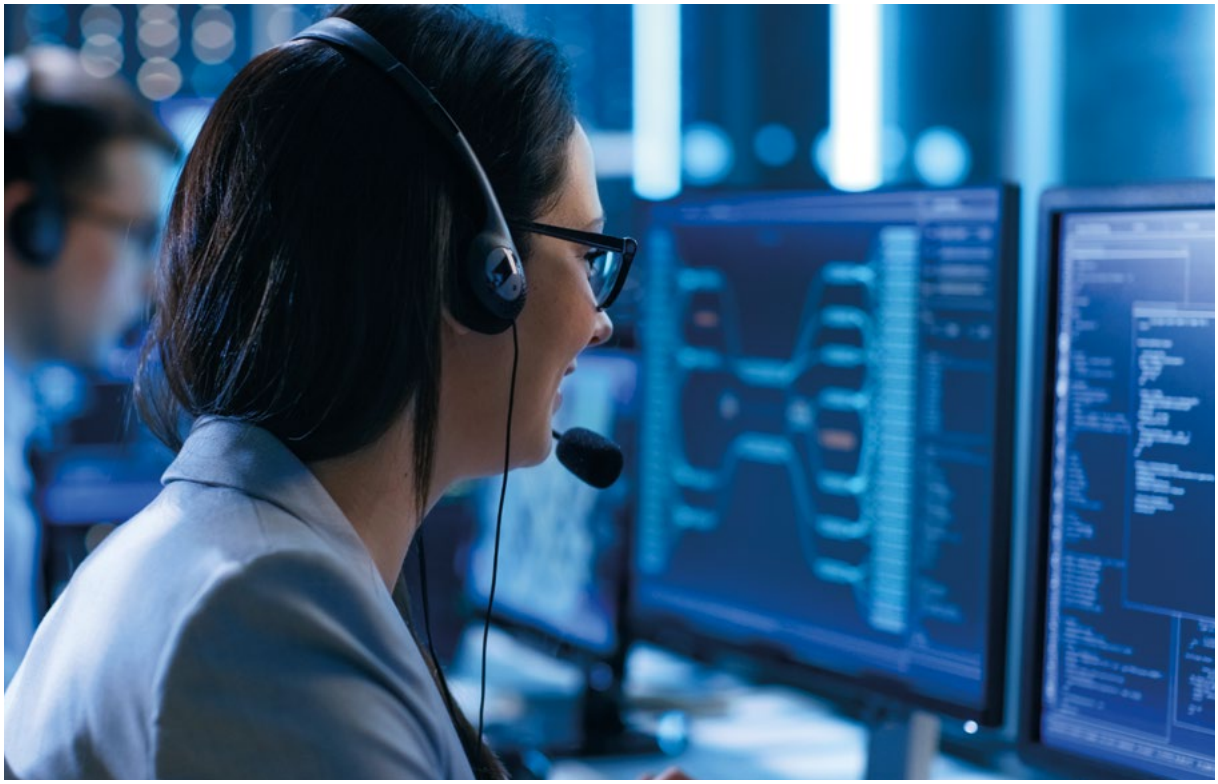
Medium

- SPOC (ticketing)
- Assistenza Remota (4h)
- Patch Management
- Estensione di garanzia HW*
- Monitoraggio passivo

Large

- SPOC (ticketing)
- Assistenza Remota (2h)
- Patch Management
- Estensione di garanzia HW*
- Monitoraggio Proattivo
- Antivirus
- Asset Management

* valido solo per il servizio e-Zen Care PDL. Per Server e Network l'assistenza HW è sempre quotata a parte



PDL

Small*

- Assistenza Remota (AMC) SLA 4h
- Ticketing

Medium*

- Assistenza Remota SLA 4h
- Ticketing con piattaforma dedicata
- Patch Management
- Asset Management
- Monitoring Passivo
- Assistenza Hardware Onsite SLA NBD

Large*

- Assistenza Remota SLA 2h
- Ticketing con piattaforma dedicata
- Patch Management
- Asset Management
- Monitoring Proattivo
- Antivirus
- Assistenza Hardware Onsite SLA NBD

Network

Small*

- Assistenza Remota (AMC) SLA 4h
- Ticketing

Medium*

- Assistenza Remota (AMC) SLA 4h
- Ticketing con piattaforma dedicata
- Documentazione
- Monitoring Passivo

Large*

- Assistenza Remota (AMC) SLA 2h
- Ticketing con piattaforma dedicata
- Documentazione
- Asset Management
- Monitoring Proattivo
- Patch Management (se presente Maintenance)
- Backup

Add-on

- Manutenzione HW Onsite

Server

Small*

- Assistenza Remota (AMC) SLA 4h
- Ticketing

Medium*

- Assistenza Remota (AMC) SLA 4h
- Ticketing con piattaforma dedicata
- Monitoring Passivo

Large*

- Assistenza Remota (AMC) SLA 2h
- Ticketing con piattaforma dedicata
- Patch Management
- Asset Management
- Monitoring Proattivo
- Documentazione

Add-on

- Manutenzione HW on site
- MDR (Managed Detection & Response)

*Servizio attivabile per una durata minima di 6 mesi

Servizi Disponibili ↘

Remote Assistance

Intervento tecnico in teleassistenza (include operazioni correttive come ripristino S.O. ed applicazioni standard).

Ticketing

Possibilità di aprire ticket di assistenza, monitorarne lo stato ed i tempi di risoluzione, semplificando e velocizzando il flusso operativo.

Monitoring

Possibilità di monitorare stato, prestazioni e sicurezza di router, switch, firewall e dispositivi che supportano il protocollo SNMP.

Patch Management

Distribuzione automatica di patch per S.O. ed applicazioni standard, per un aggiornamento costante e la piena funzionalità dell'infrastruttura.

Asset Management

Gestione dell'inventario hw/sw, per azioni di aggiornamento rapide e mirate.

Backup Configuration

Raccolta automatica delle configurazioni degli apparati di rete con alert in caso di modifiche.

HW On Site

Intervento tecnico on site, include manodopera e parti di ricambio necessarie al totale rispristino hw della macchina.

SW On Site

Ove necessario, intervento tecnico on site per operazioni correttive.

e-Zen Care

e-Zen Care è una soluzione RMM (Remote Monitoring and Management) completa, in grado di proteggere e gestire a distanza la tua struttura informatica supportando HW e SW.

Vantaggi

- Riduzione del carico di lavoro IT
- Visibilità completa dell'intera infrastruttura IT attraverso il nostro portale dedicato
- GDPR Compliance
- Canone annuale su misura del Cliente: trasparente, fisso e senza sorprese

e–ZEN Care MDM

Servizio di gestione, monitoraggio e protezione dei dispositivi mobili utilizzati dai dipendenti. Include la gestione della configurazione dei dispositivi, l'applicazione di politiche di sicurezza, il controllo delle app installate, la protezione dei dati aziendali e la capacità di bloccare o cancellare da remoto i dispositivi in caso di smarrimento o furto.

MDM è essenziale per garantire la sicurezza e la conformità in ambienti di lavoro con dispositivi mobili.

e–ZEN Care Tenant

Base: Setup dei servizi di gestione Entra ID.

Medium: Base + Servizio di gestione Exchange (messaggistica), Servizio di gestione Entra ID avanzati.

Advanced: Medium + Servizio di gestione Teams, Servizio di gestione Sharepoint, Servizio di gestione OneDrive.

Security: (Add-on ai livelli precedenti) Valutazione iniziale della Sicurezza, configurazione delle Policies di Sicurezza, gestione delle Policies di Accesso, Monitoraggio Continuo della Sicurezza, aggiornamento delle Policies di Sicurezza, implementazione di Soluzioni di Sicurezza Avanzate, ottimizzazione delle Configurazioni di Sicurezza, gestione delle Identità e degli Accessi.

e–ZEN Security MDR

Servizio di sicurezza informatica gestito che fornisce monitoraggio continuo, rilevamento avanzato delle minacce e risposta agli incidenti. Le soluzioni MDR combinano tecnologie avanzate con analisi umane per identificare e mitigare le minacce alla sicurezza in tempo reale. I servizi possono includere monitoraggio delle reti, analisi comportamentale, investigazione delle minacce, risposta agli incidenti e miglioramento continuo delle difese di sicurezza. L'obiettivo è proteggere le organizzazioni da attacchi sofisticati riducendo il tempo di risposta e minimizzando l'impatto degli incidenti di sicurezza.

Cloud

Servizio per la virtualizzazione dei server. Per avere sempre l'azienda a portata di qualsiasi dispositivo.

I servizi nascono per garantire il massimo livello di continuità operativa, performance e sicurezza dei dati e delle infrastrutture che li ospitano; anche per ambienti Enterprise e Business Critical come SAP, Oracle, AS/400.

Enterprise IAAS

Un servizio Private Cloud che consente di modellare un vero e proprio Data Center a livello Enterprise amministrandolo da una semplice console web.

Cloud Power As/400

L'infrastruttura tecnologica del servizio Cloud Power AS400 è completamente scalabile e permette alte performance, conformi al variare delle esigenze del Cliente.

SAP Hana Cloud IAAS

Un'infrastruttura Cloud su hardware certificato SAP HANA, per costruire il tuo ambiente protetto e sicuro su cui creare macchine virtuali con sistema operativo Red Hat Enterprise per SAP.

Oracle Cloud IAAS

Oracle Cloud Infrastructure è la soluzione IaaS che fornisce potenza di calcolo altamente performante per eseguire carichi di lavoro Oracle su Infrastruttura certificata, dove installare i tuoi ambienti in modalità BYOL (Bring Your Own License).

e-Zen Cloud è anche ↘

Gestione Semplificata

Il Cliente ha la possibilità di creare, configurare e accedere alle macchine virtuali in qualsiasi momento e da qualsiasi dispositivo.

Monitoraggio

Il Cliente può verificare lo stato delle macchine attraverso il nostro portale dedicato e la configurazione di alarm via mail.

Massima Sicurezza

Include firewall virtuali ad alta affidabilità e VPN site-to-site per le comunicazioni con la sede del Cliente.

Backup Giornaliero

Con finestra continua 24h e funzionalità di compressione e decuplica incluse.

MDR

Servizio di sicurezza informatica gestito con monitoraggio continuo, rilevamento avanzato delle minacce e risposta agli incidenti.

Backup

Soluzione di backup automatico per tutte le piattaforme per una protezione totale dei dati.

Sicurezza continuativa e automatizzata.

Local Backup

Questa soluzione prevede la copia e la conservazione dei dati su dispositivi fisicamente presenti dal Cliente.

Cloud Backup

Questa soluzione prevede la copia e la conservazione dei dati su un server remoto preservandoli da cancellazioni fortuite o in caso di guasti HW.

Hybrid Backup

Questa soluzione prevede la copia e la conservazione dei dati sia in Cloud che in locale, per una totale sicurezza e durabilità dei backup.

Applicazioni ↘

e-Zen Backup nasce come soluzione di backup automatico per tutte le principali piattaforme: Windows, Linux, macOS, VMware e HyperV.

Il servizio è, inoltre, in grado di garantire backup di SQL Server ed Exchange Server, con ripristino a livello di singola casella mail.

Tutto questo grazie ai principali Cloud Provider, per la totale protezione e durabilità dei dati aziendali.

Pacchetti Disponibili

- **PDL**
  PC/notebook, workstation con S.O.
  Windows, Linux e macOS

- **Server**
  Windows Server, VMware, ESXI/V Center, Office365/Google Cloud apps

- **Storage/Opzioni**
  SQL Server
  Exchange Server Cloud Storage (a partire da 500GB)

Livelli
di Servizio

La nostra soluzione e-Zen Backup è in grado di garantire

- Durabilità dei dati pari al 99.999999999%
- Disponibilità del servizio >99%

Per il servizio di gestione e reportistica:

- Controllo giornaliero circa l'esito dei backup pianificati
- Notifica in caso di problemi relativi all'esecuzione di una attività entro il giorno successivo il termine dell'esecuzione stessa

Perimetro
del Servizio

Il servizio e-Zen Backup include:

- Supporto all'installazione e prima configurazione del software
- Controllo remoto giornaliero circa l'esito delle attività di backup pianificate
- Realizzazione di report mensili a dimostrare lo stato di protezione del cliente
- Fornitura di spazio di archiviazione in cloud come da contratto
- Monitoraggio dello spazio occupato in cloud

Opzionalmente il cliente può richiedere:

- Supporto per ripristinare files o VM
- Supporto per attività di ripristino Bare Metal attraverso l'uso di una apposita unità USB di boot
- Test di ripristino
- Configurazione del server di deduplica

Maintenance

Contratti di assistenza hardware con tempi di risoluzione personalizzabili in base alle effettive esigenze del Cliente, per un sistema integrato informatico sempre efficiente e performante.

Livelli di servizio

Tempo di intervento ↘	Descrizione ↘	Finestra di copertura ↘
NBD	Intervento tecnico entro il giorno successivo all'apertura della richiesta	8x5
SBD	Intervento tecnico il giorno dell'apertura della richiesta	13x5
6h	Intervento tecnico entro sei ore dall'apertura della richiesta *	24x7
4h	Intervento tecnico entro quattro ore dall'apertura della richiesta	

* CTR (Call To Repair)

Opzione attivabile per contratti di assistenza con tempo di intervento 6h. Definisce la massima reattività di risoluzione disponibile garantendo il ripristino del corretto funzionamento della macchina o la sostituzione della stessa, entro le tempistiche concordate con il Cliente.

Security

Soluzioni di prevenzione e difesa da attacchi esterni per pc, server, mobile e network, per una totale protezione dell'integrità e la privacy dei dati e dei sistemi informativi aziendali.

Information Gathering

Interviste al cliente e attivazione di routine di monitoraggio, per comprendere le necessità e le reali priorità e mantenere il quadro sempre aggiornato, andando così a sintetizzare l'intervento più coerente ed efficace.

Penetration Test

Crash test dell'infrastruttura e dei sistemi informativi aziendali, attraverso la simulazione di un cyber attacco.

Remediation Plan

Raccolti e razionalizzati tutti i dati, si pianifica il lavoro di miglioramento della sicurezza informatica, stabilendo delle precise azioni correttive e best practices da implementare.

Vulnerability Assessment

Scansione profonda condotta sulla rete aziendale e sulla sua presenza sul Web: vengono analizzati computer, smartphone, tablet, server, NAS, access point, dispositivi intelligenti, stampanti Wi-Fi, connessioni domotiche, postazioni di smart working e sito aziendale, per verificare qualsiasi tipo di potenziale vulnerabilità.

User Security Awareness

È formazione sulla sicurezza aziendale: aiuta tutto il personale a riconoscere, evitare e segnalare potenziali minacce che dati, si pianifica il lavoro di miglioramento della sicurezza informatica, stabilendo delle precise linee prioritarie d'azione e non lasciando nulla al caso.

Security Information and Event Management (SIEM)

Sistema di gestione preventiva e predittiva della sicurezza informatica aziendale: è una soluzione che permette di riconoscere minacce e vulnerabilità prima che abbiano la possibilità di interrompere le operazioni di business, ma è anche utile per i suoi sistemi di reportistica (per la valutazione delle conformità, il monitoraggio di utenti e app, oltre che per eventuali indagini forensi).

Information Gathering ↘

Si tratta della **ricerca di informazioni** che risulteranno vitali durante lo svolgimento del test di sicurezza informatica. Sapere cosa dovrà essere analizzato è il primo passo per garantire al cliente la buona riuscita del test.
Si punta soprattutto a dettagli rientranti in due macrocategorie: business e infrastruttura.

Business aziendale ›
Si raccolgono informazioni circa la tipologia, le caratteristiche salienti, gli asset strategici, la composizione di prodotti e servizi, gli stakeholder e i ruoli organizzativi – lavoratori dipendenti, collaboratori, fornitori.

Infrastruttura aziendale ›
Lo scopo è quello di captare gli entry point per l'exploit. Dunque, si cercheranno informazioni sul network dell'organizzazione, sui piani di indirizzamento IP, sui sistemi utilizzati, servizi, domini, sottodomini e indirizzi di posta elettronica.

Vulnerability Assesment ↘

Continuo

A seguito delle attività di penetration test, viene effettuata un'analisi su tutte le vulnerabilità presenti, vengono proposte le soluzioni necessarie e approfondita la scansione sugli apparati chiave identificati allo scopo di mantenerli costantemente in sicurezza. In questa tipologia l'attività viene eseguita con cadenza giornaliera, viene inviato un report dettagliato e gli operatori segnalano separatamente le criticità rilevate. Non sono necessarie attività di penetration test ulteriori in quanto la situazione è monitorata costantemente.

Periodico

A seguito delle attività di penetration test, viene effettuata un'analisi su tutte le vulnerabilità presenti, vengono proposte le soluzioni necessarie e approfondita la scansione sugli apparati chiave identificati allo scopo di mantenerli costantemente in sicurezza. In questa tipologia l'attività viene eseguita con cadenza stabilita dal cliente, se il periodo è superiore a 3 mesi vanno rieseguiti alcuni penetration tests per verificare il resto dell'infrastruttura.

Penetration Test ↘

Black Box

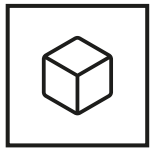
Questa tipologia di penetration test simula realmente un attacco esterno quindi senza che il cliente fornisca alcuna informazione specifica sull'infrastruttura e sui servizi, ma vengono concordati gli orari in cui questa attività viene svolta.

Grey Box

In questa tipologia si hanno solo informazioni parziali sull'infrastruttura e sulle applicazioni, può ad esempio essere richiesto di ottenere i privilegi di domain admin partendo da un'utenza standard. Uno dei principali vantaggi è che vengono forniti risultati mirati sulla sicurezza della rete in breve tempo.

White Box

In questa tipologia si hanno tutte le informazioni e i privilegi dell'infrastruttura da esaminare. L'obiettivo è quello di ottenere quante più informazioni possibili e dettagliate sulle falle di sicurezza presenti.



Red Box

Il Red Teaming è un attacco senza esclusione di colpi usato per simulare un avversario reale capace di sfruttare e testare tutte le falle presenti nel sistema informativo di una compagnia. Verranno attaccati tutti i settori, Tecnologico, Umano e Fisico, la durata è molto lunga ed è finalizzato a sensibilizzare e verificare l'efficacia delle politiche aziendali e difensive.

Remediation Plan ↘

Read only

Una volta condotte le indagini preliminari, le interviste e i test di vulnerabilità, forniamo al Cliente un report dettagliato sullo stato dell'arte della sua sicurezza informatica. Sarà poi il Cliente a dover provvedere ad agire autonomamente in base ai risultati fornitigli.

Co-managed

Oltre alla fornitura del report dettagliato sullo status di vulnerabilità dei suoi sistemi, al Cliente vengono forniti tutti i suggerimenti utili per implementare azioni correttive efficaci, che dovranno però poi essere condotte autonomamente senza un nostro ulteriore supporto.

Full managed

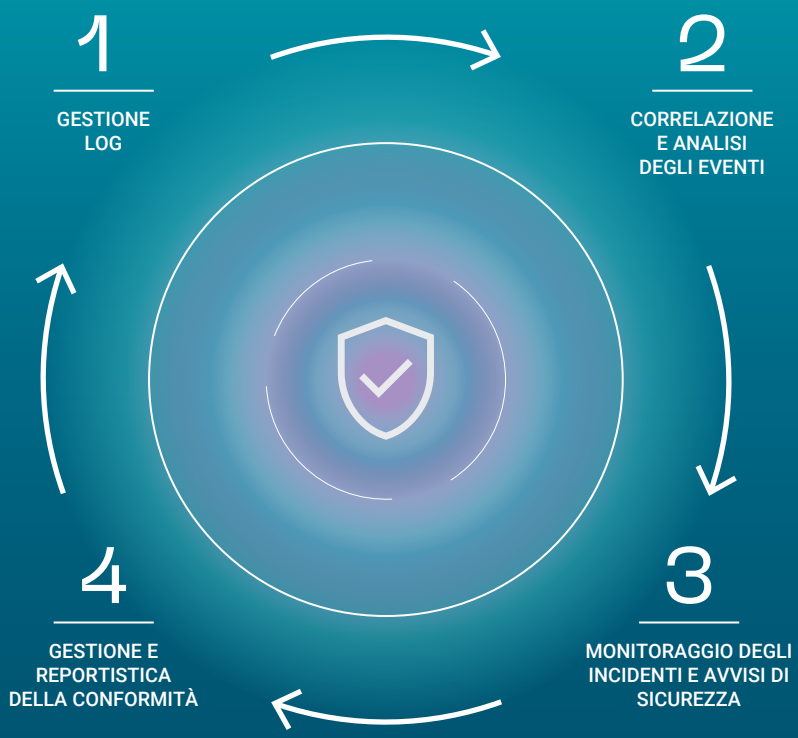
Oltre alla fornitura del report dettagliato sullo status di vulnerabilità dei suoi sistemi, al Cliente viene fornito un vademecum delle risoluzioni, che verrà integralmente gestito da noi, fornendo così un servizio completo, chiavi in mano, dall'emersione del fabbisogno alla sua soddisfazione.

User security awareness ↘

È formazione sulla sicurezza aziendale: aiuta tutto il personale a **riconoscere**, evitare e segnalare **potenziali minacce** che possono compromettere dati e sistemi critici, inclusi phishing, malware, ransomware e spyware.

I livelli di apprendimento vengono testati mensilmente effettuando **campagne di phishing mirate** e concordate con il cliente, sia nel layout che nei contenuti allo scopo di comprendere se le attività formative hanno raggiunto gli obiettivi prefissati.

SIEM
Security Information and Event Management ↘



Vantaggi

- Riconoscimento avanzato delle minacce in tempo reale
- Audit di conformità normativa
- Automazione basata sull'intelligenza artificiale
- Migliore efficienza organizzativa
- Rilevamento di minacce avanzate e sconosciute
- Conduzione di indagini forensi
- Valutazione e reportistica sulla conformità
- Monitoraggio degli utenti e delle applicazioni

www.as-srl.com