



trustsensor

// il servizio

trustsensor è un sistema automatico di controllo che rileva eventuali anomalie di traffico che possono ricondurre ad un tentativo di intrusione.

È un sistema IDS (Intrusion Detection System) che vigila 24x7x365 sul network del cliente rilevando ogni tipologia di traffico sospetto e notificando gli eventi anomali ai destinatari definiti.

// caratteristiche

Viene installato un sensore sul firewall o sul proxy del cliente che trasferisce i dati relativi al traffico di basso livello al sistema centrale digitaltrust che rielabora le informazioni e le rende disponibili in tempo reale su un sito ad accesso riservato personalizzato per il cliente

- **IDS:** un attento occhio sempre aperto e vigile sulla vostra rete, capace di analizzare ogni singolo pacchetto che entra nella vostra rete.
- **Monitoraggio dei servizi:** il sistema permette di monitorare in tempo reale il traffico di rete e lo stato dei servizi verificando anche lo spazio su disco dei sistemi e l'integrità di eventuali file critici individuati.
- **Alert System:** grazie all'invio automatico di messaggi di alert via email o SMS il responsabile viene avvisato in tempo reale di eventuali malfunzionamenti o tentativi di intrusione.
- **Interfaccia personalizzata:** una extranet dedicata con una console di monitoraggio per avere una rapida visuale dello stato dei sistemi 24 ore al giorno.
- **Gestione remota:** Il sistema viene gestito completamente in outsourcing, saranno i professionisti di digitaltrust a valutare le indicazioni di eventuali attacchi e avvisare al più presto il responsabile aziendale (oltre al servizio di alert)

// web interface



L'interfaccia web viene personalizzata in base alla corporate identità del cliente e resa disponibile tramite extranet ad accesso controllato.

// obiettivi

- Fornire un servizio in outsourcing di monitoraggio dei sistemi e dei servizi dei network.
- Garantire un monitoraggio 24x7x365
- Fornire una console di monitoraggio al cliente per una visione diretta dei sistemi

// target

Tutte quelle aziende che:

- intendono elevare la propria immagine verso clienti e fornitori
- Utilizzano collegamenti internet e/o extranet
- Utilizzano tecnologie VPN, web, Server di posta e apparati di rete.
- Vogliono avere un controllo totale sulla propria rete.

// benefici

- **Risorse e competenze** specialistiche a disposizione del cliente
- **Nessuna conoscenza** tecnica richiesta da parte del personale del cliente
- **Impatto Limitato:** viene installato presso il cliente un sensore software sul proxy/firewall di collegamento con la rete pubblica.
- **Controllo completo di sistemi e servizi** grazie alla varietà e numerosità delle tipologie di traffico analizzato.
- **Notifica in real time** tramite email o sms all'amministratore di sistema di eventuali comportamenti sospetti individuati.

// servizi opzionali

- **Black Box Interna:** è possibile introdurre all'interno del network aziendale una black-box digitaltrust in grado di effettuare il monitoraggio della rete LAN interna all'azienda

// modalità di erogazione

In base al **Service Level Agreement** sottoscritto è possibile demandare a **digitaltrust**® la completa gestione degli alert del sistema o monitorare internamente le rilevazioni effettuate dal sistema attraverso la extranet allestita ad-hoc.








Digitaltrust offre tre livelli di agreement per rispondere alle richieste di qualsiasi tipologia di organizzazione:

- **SLA – “monitor”**: un accordo che prevede la completa gestione di trustsensor da parte di digitaltrust, al cliente viene fornito l'accesso alla extranet personalizzata per poter monitorare 24x7x365 i propri sistemi senza possibilità di intervento e configurazione sul sistema IDS. Gli alert vengono notificati unicamente allo staff tecnico digitaltrust che dopo una rapida analisi provvede nel caso ad avvertire telefonicamente o via email il cliente.
 - *Un servizio MSP completo in completo outsourcing*
 - *Adatto alle organizzazioni che non hanno competenze interne per la gestione della sicurezza*
- **SLA – “alert”**: oltre ai servizi offerti dal contratto “monitor” viene fornita la gestione degli alert gestibile in autonomia da cliente.
 - *Un servizio MSP con l'interazione del cliente*
 - *Adatto a chi vuole partecipare attivamente alla gestione della sicurezza*
- **SLA – “full control”**: viene implementato un sistema ad uso unico del cliente dove l'amministratore ha completa gestione del sistema e degli alert. **digitaltrust**® provvede unicamente a verificare il corretto funzionamento del sistema e ad aggiornare e monitorare il sistema stesso in gestione presso il cliente.
 - *Un servizio gestito internamente all'azienda cliente*
 - *Adatto alle grandi organizzazioni che sono hanno risorse e competenze per gestire le problematiche di security internamente*

// sistemi supportati

- Windows NT/95/98/200/XP, tutti i dialetti Unix, BSD, Linux, ecc.

// screenshot

Monitored Files	
All monitored files	
Alerts (Last 6 Hrs)	
4 PM (35)	
3 PM (1281)	
2 PM (777)	
1 PM (44)	
12 PM (34)	
11 AM (46)	
% Alerts/Sensor	
main.digitaltrust.it (3%)	
pingu.itp.com (<1%)	
pinga.itp.com (82%)	
ns.ice2k.com (15%)	
Protocol Breakdown	
TCP (94%)	
UDP (0%)	
ICMP (5%)	
Top 6 Src IPs	
213.155.198.131	(8751)
209.61.188.34	(993)
151.99.219.10	(197)
213.155.198.132	(94)
195.219.114.221	(85)
212.100.65.68	(59)
Top 6 Dst IPs	
212.100.224.168	(8950)
209.61.188.34	(1479)
192.168.2.10	(279)
217.35.247.34	(24)
206.117.161.80	(23)
212.100.224.163	(23)

security is not an option

digitaltrust

è la divisione aziendale dedicata alla
sicurezza informatica di:
Internet Centre of Excellence SpA
Via Tazzoli, 6 Milano
Tel: +39 02-29061262
Fax: +39 02-6598897
info@digitaltrust.biz