AVANGATE SECURITY

# HTS

## ISO 27001 e gestione dei log

18/04/2024

HTS
HI-TECH SERVICES

# LOG: cosa sono e la loro importanza

# Cosa sono i LOG

**COSA SONO:**
I log sono file di testo all'interno dei quali vengono memorizzate, in ordine cronologico, le operazioni compiute dai sistemi informatici (es: accessi ai computer, operazioni eseguite dagli utenti all'interno di applicazioni software, parametri di funzionamento dei sistemi hardware, ecc.).

**CHI LI PRODUCE:**
Ogni sistema informatico registra i log delle proprie attività.

**A COSA SERVONO**
Una corretta gestione dei log concorre a garantire la sicurezza dell'infrastruttura informatica e il controllo della liceità della gestione dei dati personali.

# Log & Normative

I **LOG** sono un **obbligo normativo**

Alcune delle normative recenti di interesse per il log management:

| | |
|---|---|
| GDPR | 25/05/2018 |
| AGID – MISURE MINIME PA | 31/12/2017 |
| AGID – SPID | DAL 2015-2016 |
| D.LGS 196 – ADS | DAL 15/12/2009 |
| … | |

# Log & Normative

I LOG sono un obbligo normativo… **ma non solo questo!**

- CERTIFICAZIONI (ES: ISO 27001)
- STANDARD DI SETTORE (ES: PCI-DSS)
- SICUREZZA DI TUTTI I SISTEMI E DI TUTTI I DATI (NON SOLO PRIVACY)
- ESIGENZE INTERNE DI VERIFICA E CONTROLLO
- NIS/NIS II
- …

## ISO/IEC 27001:2022 e ISO/IEC 27002:2022

### 5.1 - Organizational controls > Policies for information security

**CONTROLLO (CONTROL):**
Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

**SCOPO (PURPOSE):**
To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with **business, legal, statutory, regulatory and contractual requirements**.

## ISO/IEC 27001:2022 e ISO/IEC 27002:2022

### 8.15 - Technological controls > Logging

**CONTROLLO (CONTROL):**
Logs that record activities, exceptions, faults and other relevant events should be **produced, stored, protected and analysed**.

**SCOPO (PURPOSE):**
To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.

## ISO/IEC 27001:2022 e ISO/IEC 27002:2022

### 8.16 - Technological controls > Monitoring activities

**CONTROLLO (CONTROL):**
Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

**SCOPO (PURPOSE):**
To detect anomalous behaviour and potential information security incidents.

## ISO/IEC 27001:2022 e ISO/IEC 27002:2022

Altri controlli:

| | |
|---|---|
| 7.2 | Physical entry |
| 8.4 | Access to source code |
| 8.5 | Secure authentication |
| 8.19 | Installation of software on operational systems |
| 8.28 | Secure coding |

[...]

# Quale soluzione?
# Utilizzi di LOGBOX

# Come gestire i LOG

## CRITICITA' DEI LOG:

- Ogni sistema ha una propria tipologia di log con specifiche caratteristiche
- Quantità elevate…anche milioni di righe di log al giorno.
- Difficilmente leggibili e interpretabili
- Sono distribuiti su tutti i sistemi
- «Non sono protetti»….

## COME FARE?

Le soluzioni di LOG MANAGEMENT consentono di acquisire, centralizzare e analizzare grandi quantità di log e di rendere il contenuto dei log facilmente interpretabile.

**LOG MANAGEMENT: DA OBBLIGO A VALORE AGGIUNTO**

# Soluzioni di log management


- SOLUZIONE CLOUD
- MULTI-TENANT – RESELLER/CLIENTE FINALE
- ORIENTATO ALLA COMPLIANCE NORMATIVA
- FOCUS: ADS E GDPR
- ANALISI LOG: REPORT E ALLARMI


- SOLUZIONE ON PREMISE (HW / VM)
- ENTERPRISE
- ANALISI REAL-TIME E ON DEMAND: RICERCA FULL TEXT, DASHBOARD, REPORT E ALLARMI

# Altri esempi di utilizzo

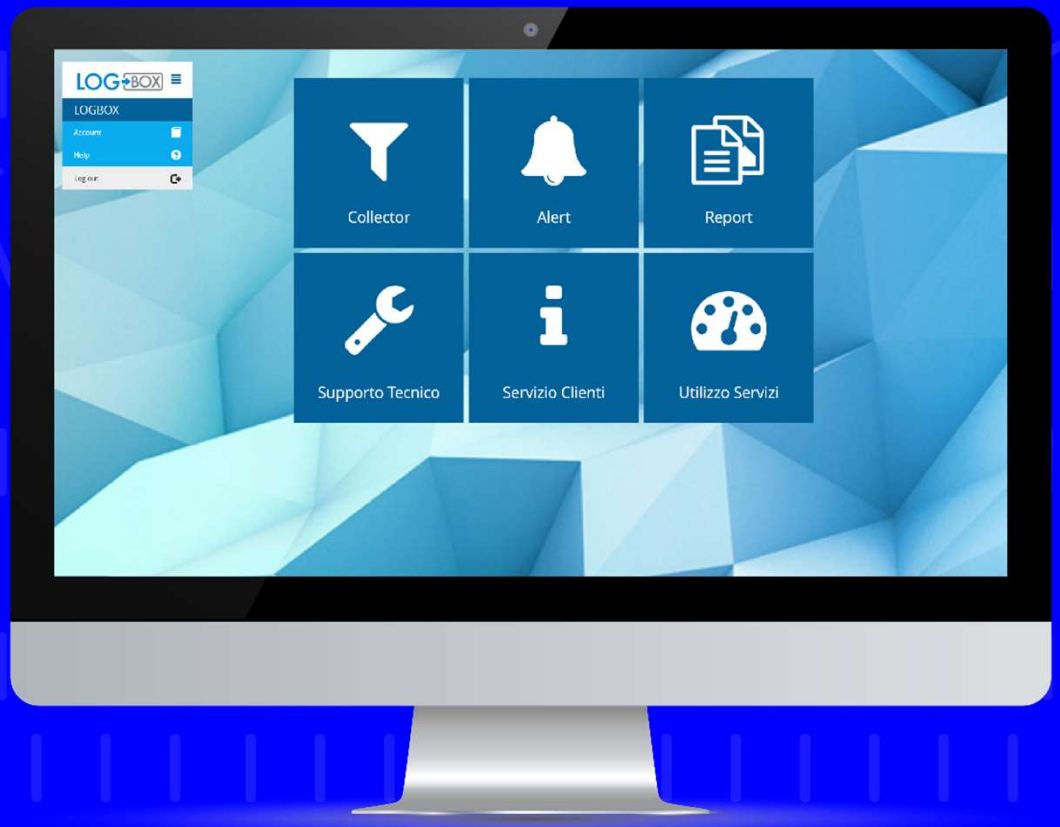
## ALTRE ESIGENZE: SECURITY, CERTIFICAZIONI, ANALISI INTERNE


- Audit certificazioni: ISO 27001, PCI DSS, …
- Monitoraggio file e cartelle (GDPR)
- Alert e monitoraggio accessi remoti (VPN, FW, …)
- Conservazione log e report anomalie per sistemi industriali (es: celle frigorifere)
- Report attività utenti (Richieste autorità)
- Verifiche e monitoraggio Smart Working
- Analisi sistemi per correzioni vulnerabilità (LDAP/LDAPS)

# HTS LOGBOX

HI-TECH SERVICES

La soluzione cloud per
l'adeguamento al GDPR.

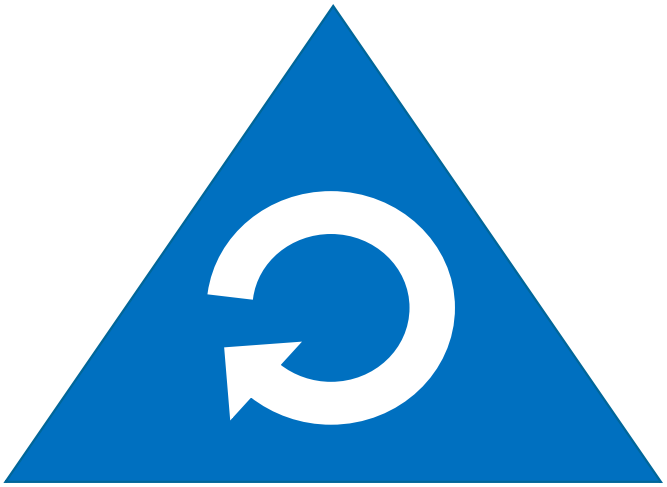


HTS LOGBOX
HI-TECH SERVICES

AVANGATE
SECURITY

# Gestione Log

CENTRALIZZAZIONE E
ARCHIVIAZIONE



REPORT
ALLARMI

MESSA IN
SICUREZZA

HTS LOGBOX
HI-TECH SERVICES

AVANGATE
SECURITY

# Funzionalità

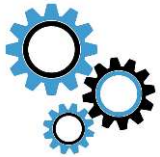
ACQUISIZIONE
REAL TIME

SICUREZZA
DATI

INTERFACCIA
WEB

REPORT


LOG BOX



CONFIGURAZIONI
AVANZATE


RETENTION

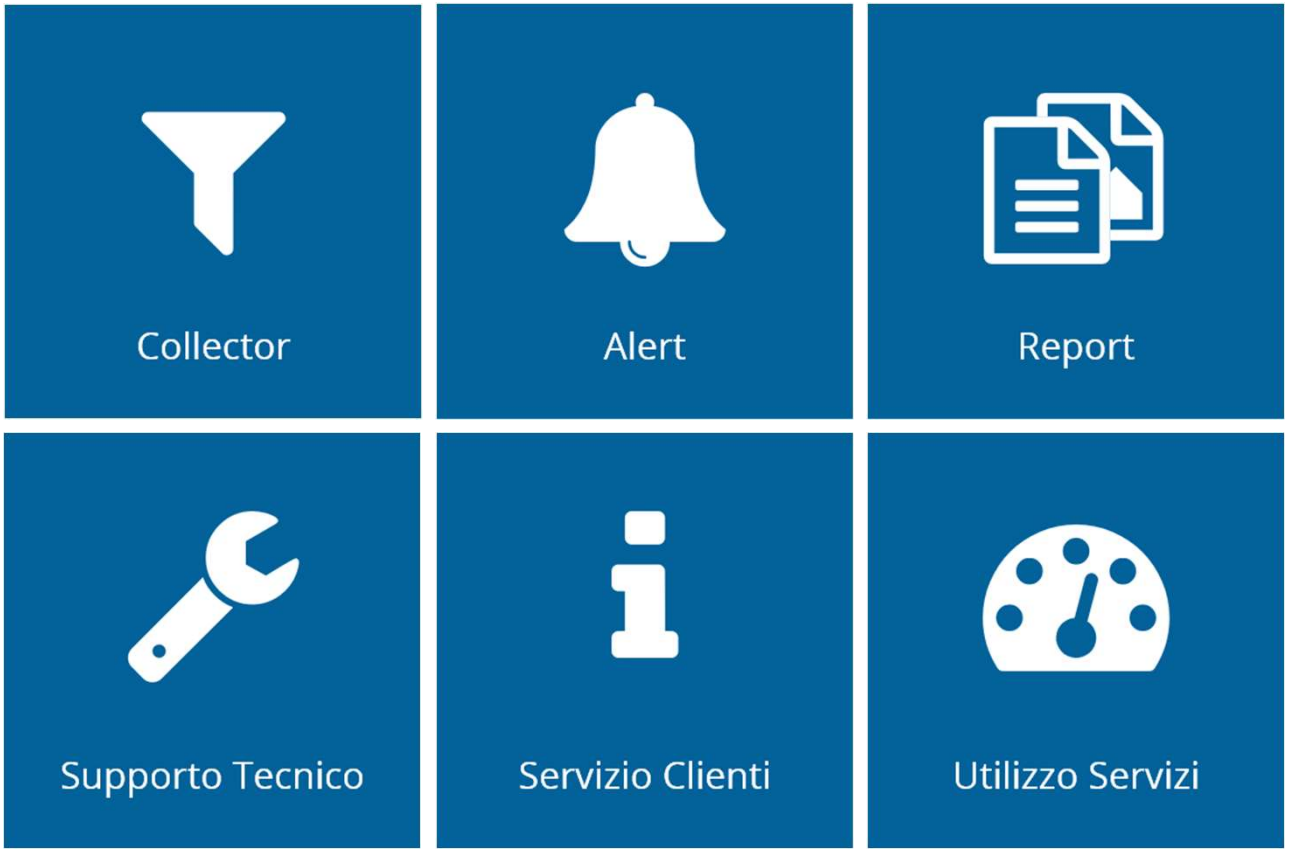
ALLARMI

LOG INTERNI

HTS LOGBOX
HI-TECH SERVICES

AVANGATE
SECURITY

# Moduli



HTS LOGBOX
HI-TECH SERVICES

AVANGATE
SECURITY

# Collector


Scopo: compliance

Acquisizione

Centralizzazione

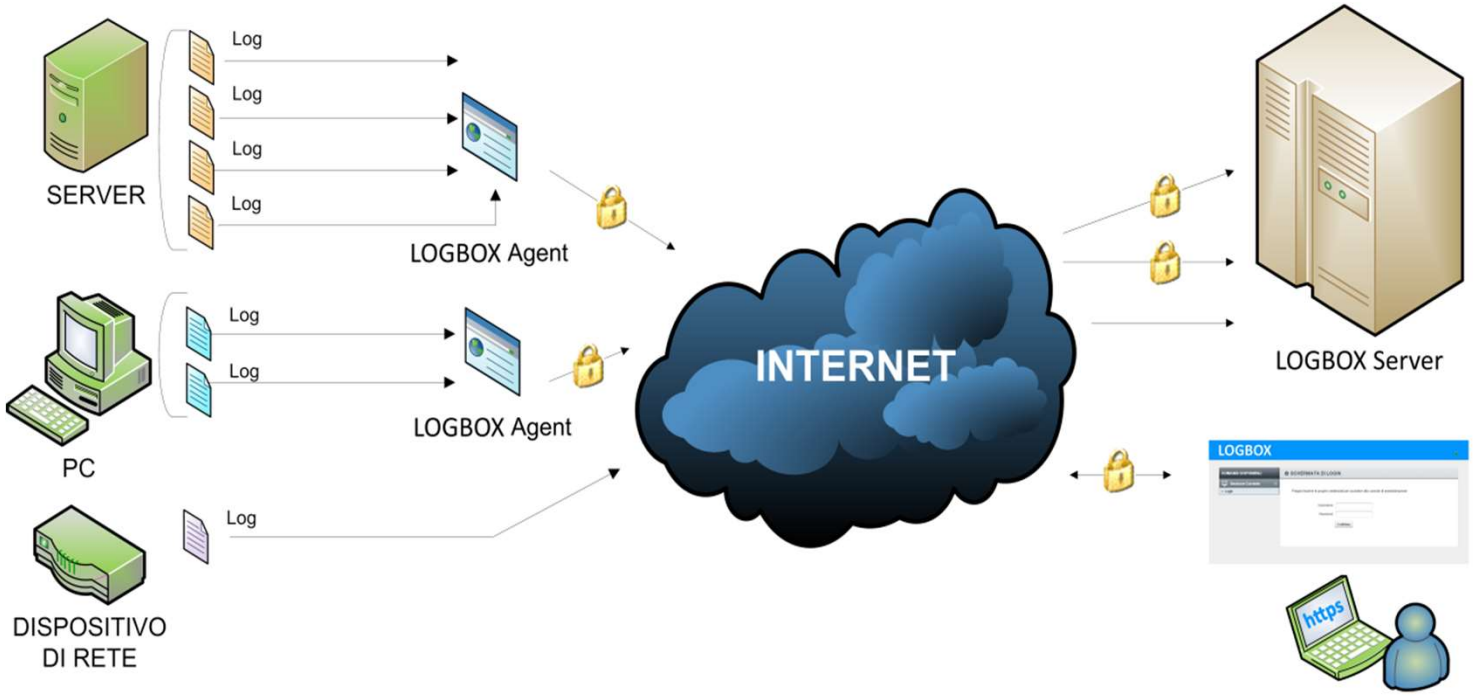
Archiviazione

Messa in sicurezza

HTS LOGBOX
HI-TECH SERVICES

AVANGATE
SECURITY

# Collector



# Collector


## ACQUISIZIONE LOG

- Acquisizione in tempo reale dei LOG mediante un agente software o diretta (syslog, syslog-ng, ftp, ecc…).
- Acquisizione log **raw**
- Possibilità di concentratore opzionale per ottimizzazione dell'occupazione di banda e buffering log in caso di mancanza di connettività oppure per trasferimento protetto dei syslog. (progetti ad hoc).

# Collector


## ACQUISIZIONE LOG: AGENT

- Acquisizione e trasferimento REAL TIME
- Protocollo cifrato con controlli sicurezza e verifiche trasferimento dati.
- Ogni agent può monitorare molteplici sorgenti di log.
- Cache locale cifrata
- Segnali keep-alive tra agent e server Logbox
- Schedulazione invio log opzionale
- Filtri eventID/regex (Windows)

HTS LOGBOX HI-TECH SERVICES AVANGATE SECURITY

# Collector


SICUREZZA DEI DATI

- Sistema chiuso (dall'acquisizione)
- Filesystem cifrato (AES 256)
- https://.... (interfaccia web)
- Autenticazione e ACL utenti
- Log interni non modificabili (accessi e operazioni sul sistema)
- Segnali keep-alive tra agent e server Logbox
- Allarmi di sistema su stato e funzionamento del sistema
- Cache cifrata (agent)
- Protocollo sicuro per trasferimento dati tra agent e server Logbox

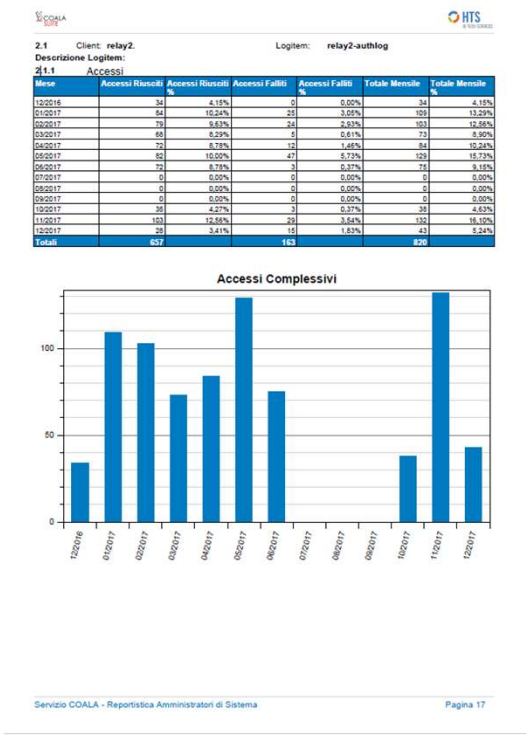
# Report


- Gestione Report in autonomia
- Report on demand
- Report pianificati (schedulati e periodici)
- Report automatici (AdS annuale/semestrale)
- Modello report AdS incluso
- Modelli di report personalizzati (NO personalizzabili)
- Archivio storico report

HTS LOGBOX HI-TECH SERVICES

AVANGATE SECURITY

# Report



2.1 Client: relay2. Logitem: relay2-authlog

Descrizione Logitem:

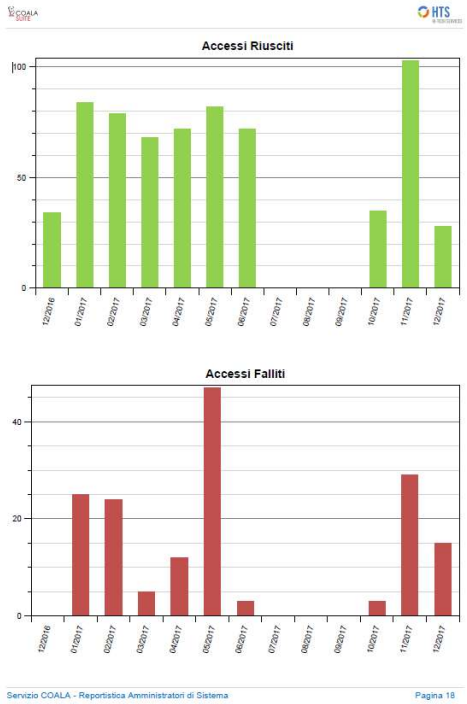
2.1.1 Accessi

| Mese | Accessi Riusciti | Accessi Riusciti % | Accessi Falliti | Accessi Falliti % | Totale Mensile | Totale Mensile % |
|---|---|---|---|---|---|---|
| 12/2016 | 34 | 4,15% | 0 | 0,00% | 34 | 4,15% |
| 01/2017 | 84 | 10,24% | 25 | 3,05% | 109 | 13,29% |
| 02/2017 | 79 | 9,63% | 24 | 2,93% | 103 | 12,56% |
| 03/2017 | 68 | 8,29% | 5 | 0,61% | 73 | 8,90% |
| 04/2017 | 72 | 8,78% | 12 | 1,46% | 84 | 10,24% |
| 05/2017 | 82 | 10,00% | 47 | 5,73% | 129 | 15,73% |
| 06/2017 | 72 | 8,78% | 3 | 0,37% | 75 | 9,15% |
| 07/2017 | 0 | 0,00% | 0 | 0,00% | 0 | 0,00% |
| 08/2017 | 0 | 0,00% | 0 | 0,00% | 0 | 0,00% |
| 09/2017 | 0 | 0,00% | 0 | 0,00% | 0 | 0,00% |
| 10/2017 | 36 | 4,27% | 3 | 0,37% | 39 | 4,63% |
| 11/2017 | 103 | 12,56% | 29 | 3,54% | 132 | 16,10% |
| 12/2017 | 28 | 3,41% | 15 | 1,83% | 43 | 5,24% |
| Totali | 657 | | 163 | | 820 | |

Accessi Complessivi







Accessi Riusciti



Accessi Falliti





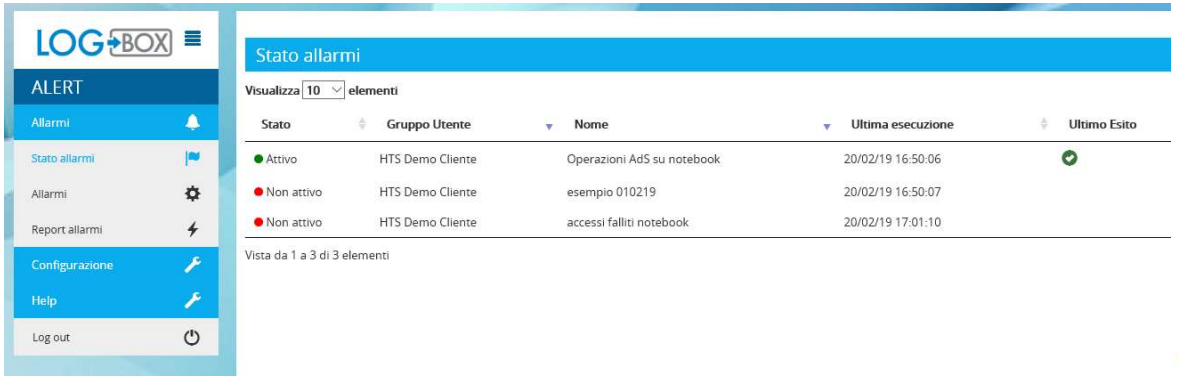
2.1.3 Accessi riusciti per singolo utente

Accessi per Utente

HTS LOGBOX HI-TECH SERVICES AVANGATE SECURITY

# Alert


- Gestione Allarmi in autonomia
- Allarmi «manuali» e da catalogo
- Catalogo AdS incluso
- Catalogo allarmi personalizzati
- Archivio storico allarmi
- Allarmi con testo «parametrico»



HTS LOGBOX
HI-TECH SERVICES

AVANGATE
SECURITY

# Utilizzo Servizi


Moduli attivi

Scadenze licenza (singoli moduli)

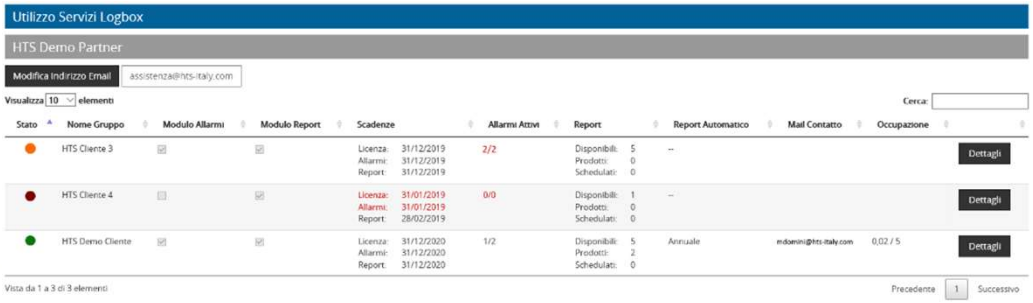
Utilizzo Allarmi (attivi/disponibili)

Utilizzo Report (prodotti/schedulati/disponibili/automatici)

Occupazione storage (attuale/disponibile, andamento ultimo anno)

Volumi log archiviati (mensili con storico ultimo anno)

Notifiche via email



# Perché LOGBOX

# PERCHE' SCEGLIERE LOGBOX O COALA SUITE?

- **Soluzioni facilmente scalabili (possibilità anche di upgrade da Logbox a Coala)**
- **«Pronti all'uso»… non si parte dal foglio bianco! Tempi minimi di messa in esercizio e apprendimento.**
- **Semplicità di utilizzo e costi minimi (risorse/tempo) di gestione.**
- **Soluzione di proprietà… possibilità/disponibilità per customizzazioni e progetti ad hoc.**
- **Soluzione italiana sviluppata a partire dalle normative nazionali ed europee… non adattamenti di soluzioni nate per altri scopi e contesti.**
- **Esperienza e conoscenza dei contesti tecnici e normativi da parte di HTS, supporto a 360°.**
- **Costi chiari…**

# Feedback dai clienti

## ALCUNE CRITICITA' DEI COMPETITOR…

- **Criticità dei servizi di post vendita e di assistenza... non adeguati o difficoltà di comunicazione.**
- **Soluzioni «potenti» ma a livello pratico ingestibili per difficoltà di utilizzo e tempi di apprendimento.**
- **Impossibilità (disponibilità e/o costi) di personalizzazioni.**
- **Costi/Licensing… criticità soprattutto per realtà medio/piccole e/o aumenti significativi dei costi dopo il primo anno.**

# PROPOSTA COMMERCIALE

HTS LOGBOX HI-TECH SERVICES AVANGATE SECURITY

# Licensing

LOGBOX

| MODELLO | VERSIONE | STORAGE [GB] | REPORT (n°) | ALLARMI (n°) |
|---|---|---|---|---|
| **SMART** | 05 | 0,5 | ✓ (1 annuale*) | - |
| | 10 | 10 | | |
| | 50 | 50 | | |
| | 100 | 100 | | |
| **GDPR** | 2S | 2 | ✓ (2 semestrali*) | ✓ (5) |
| | 5S | 5 | | |
| | 10 | 10 | ✓ (1 annuale*) | |
| | 50 | 50 | | |
| | 100 | 100 | | |
| UPGRADE | | | | |
| STORAGE AGGIUNTIVO E UPGRADE SERVIZIO | | 5 | | |
| | | 10 | | |
| SERVIZI OPZIONALI | | | | |
| PACCHETTO REPORT AGGIUNTIVI | | | 1/3/11/ad hoc | |
| PACCHETTO ALLARMI AGGIUNTIVI | | | | 5/10/ad hoc |
| SERVIZIO "SOLO CONSERVAZIONE" | | | | |
| **SOLO CONSERVAZIONE** | - | (6 mesi) | - | - |

*(*) Report automatico annuale/semestrale modello AdS su tutti i log archiviati.*

# Info utili per iniziare

1. Canone Servizio (Modello/Versione)
2. Canone Assistenza
3. Formazione/Installazione (1° anno)

Opzioni principali:

1. Pacchetti aggiuntivi (storage/allarmi/report)

INFORMAZIONI UTILI:

Normative
Esigenze

⇨ MODELLO

N° Server
N° Utenti
N° AdS

⇨ VERSIONE

AVANGATE SECURITY

# Grazie

www.hts-italy.com

HTS

HI-TECH SERVICES