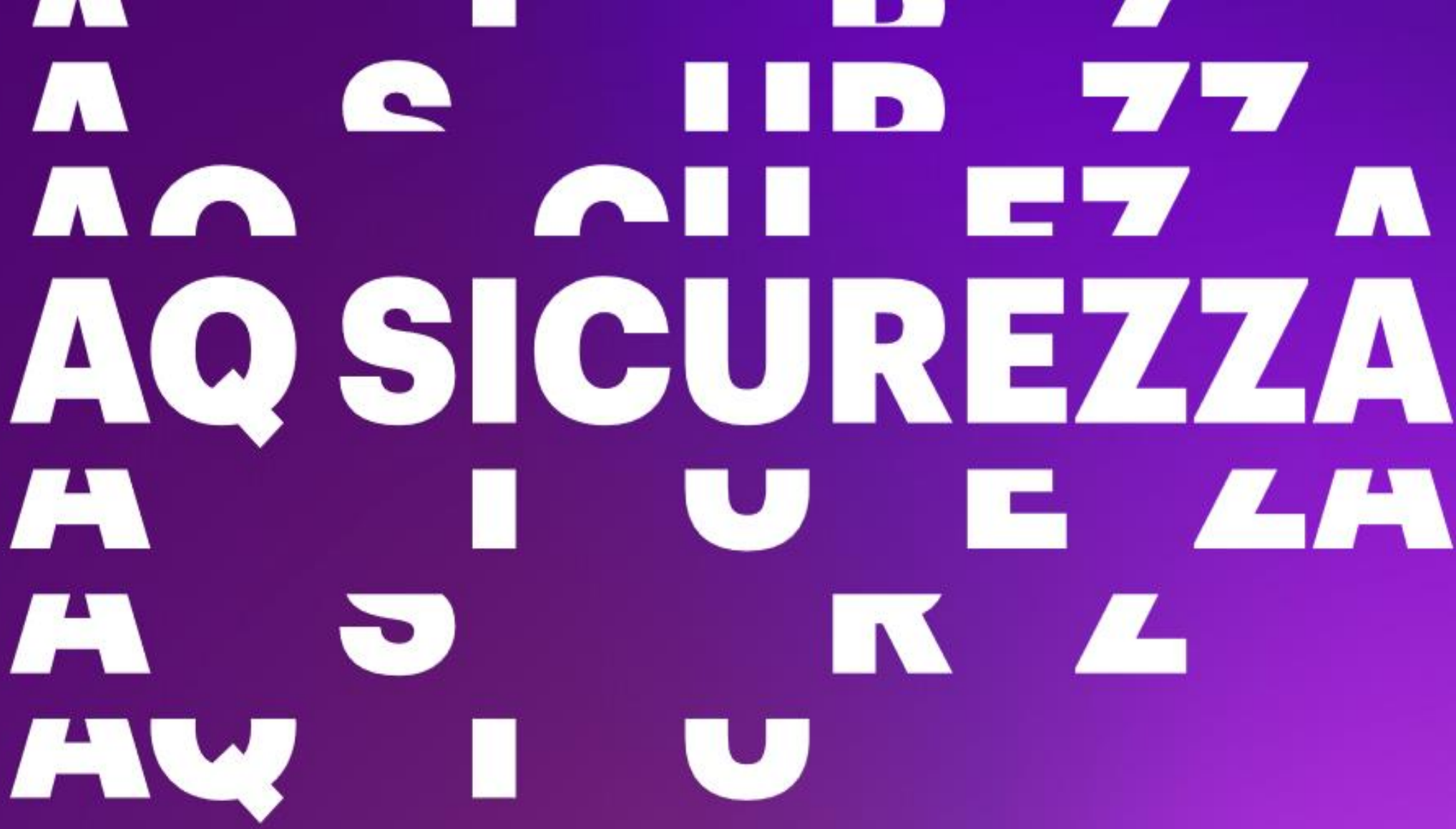
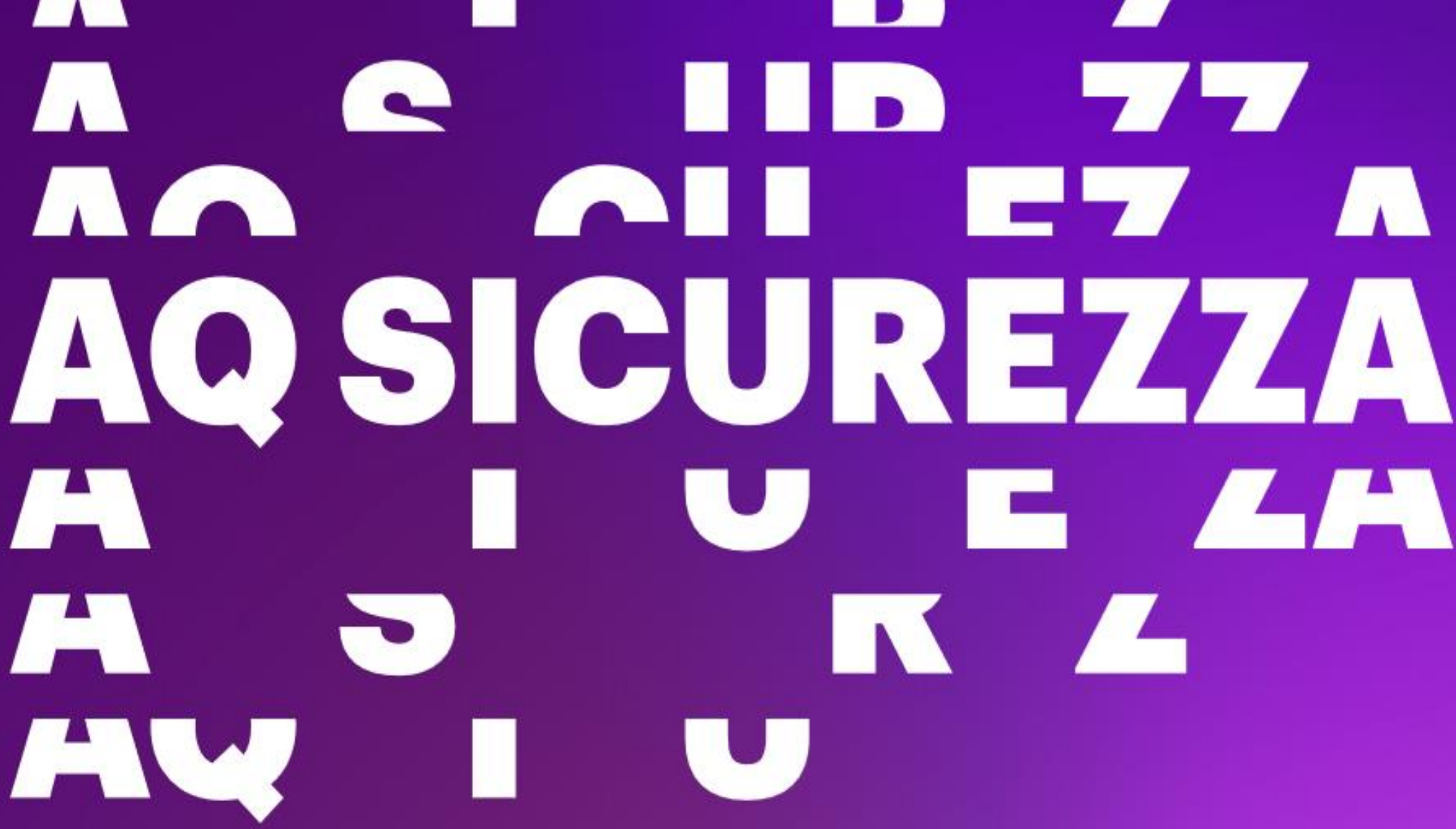


ID 2296 - SERVIZI DI SICUREZZA DA REMOTO PER LA PUBBLICA AMMINISTRAZIONE LOCALE



I - L’ACCORDO QUADRO

L'ACCORDO QUADRO

PRESENTAZIONE E OBIETTIVI DELL'ACCORDO

Il Lotto **di servizi di Sicurezza da remoto (Lotto 1)** ha l'obiettivo di mettere a disposizione delle Amministrazioni un **insieme di servizi di sicurezza - erogati da remoto e in logica continuativa - per la protezione delle infrastrutture, delle applicazioni e dei dati**

I servizi in perimetro sono relativi alle seguenti aree:

- **Prevenzione** e **gestione** delle **minacce**
- **Autenticazione** degli **accessi** e **validità probatoria**
- **Supporto** al **delivery** e alla **migrazione** dei **servizi**

L'affidamento dei servizi oggetto dell'Accordo Quadro avviene tramite lo svolgimento di due fasi procedimentali:

I PRIMA FASE PROCEDIMENTALE

Riguarda le **condizioni generali del contratto,** è stato gestito da Consip che ha stipulato un contratto con i Raggruppamenti aggiudicatari (1° aggiudicatario – contratti PAL; 2° aggiudicatario – contratti PAC)

II SECONDA FASE PROCEDIMENTALE

Prevede la stipula con le Amministrazioni contraenti di **singoli Contratti esecutivi**.
L'affidamento avviene secondo i termini e le condizioni dell'Accordo Quadro senza riaprire il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro (**AQ a condizioni tutte fissate**)

L'ACCORDO QUADRO

I BENEFICIARI

È previsto che al Lotto 1 – 1° aggiudicatario possano accedere **tutte le Pubbliche Amministrazioni Locali** presenti sul territorio italiano.

Con il duplice obiettivo di:

- **garantire la continuità e l'evoluzione dei servizi** già previsti nella precedente **iniziativa SPC Cloud** – **Lotto 2** avente ad oggetto servizi di sicurezza volti alla protezione dei sistemi informativi in favore delle Pubbliche Amministrazioni, nell'ambito del Sistema pubblico di connettività;
- **rendere disponibili** alle Amministrazioni **servizi con carattere di innovazione tecnologica** per l'**attuazione** del **Codice dell'Amministrazione Digitale**, nonché del **Piano Triennale ICT della PA**.

L'ACCORDO QUADRO
IL RTI

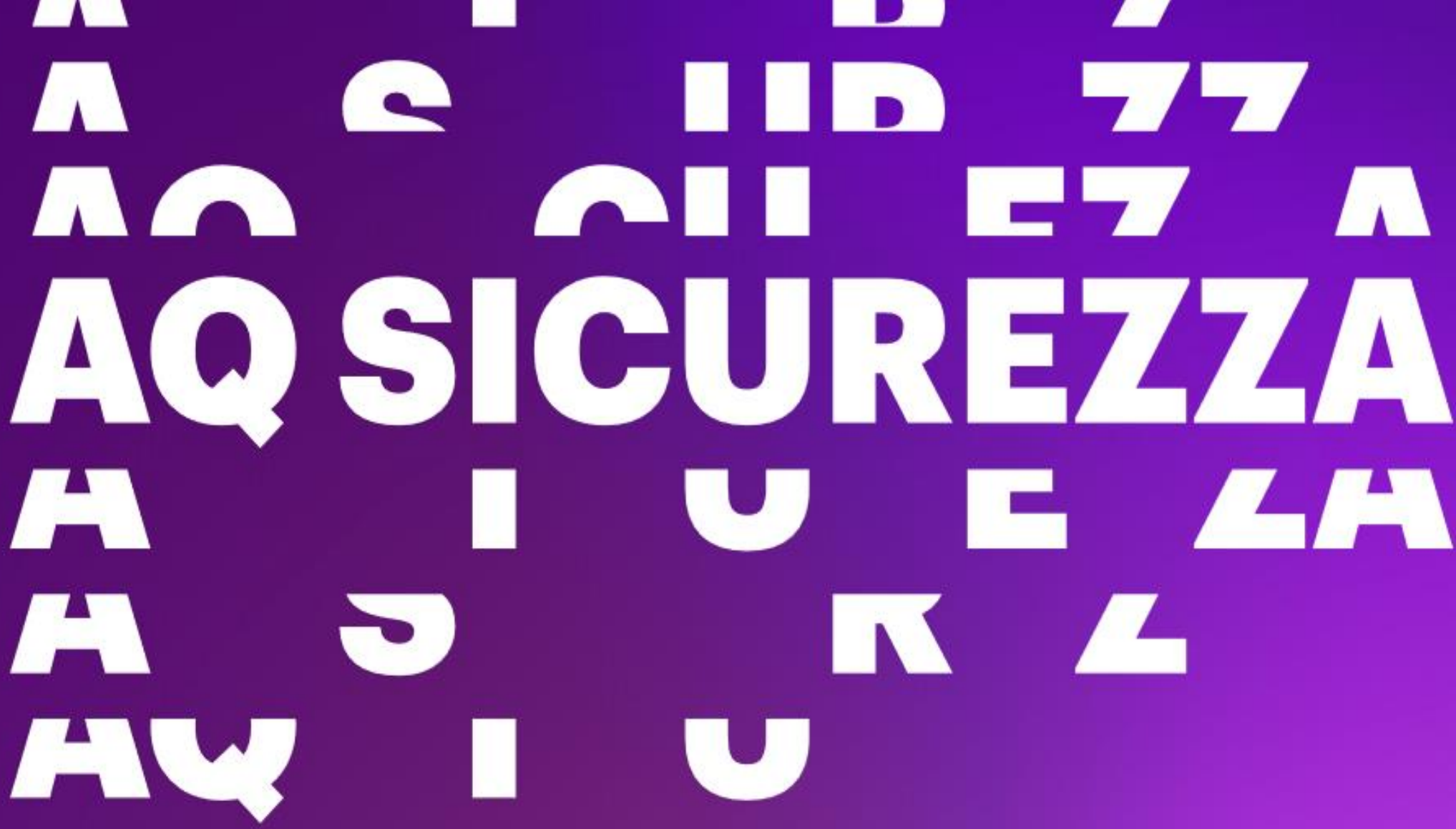
*Il **RTI** ha riportato il **massimo punteggio** posizionandosi al **1° posto** e aggiudicandosi la Pubblica Amministrazione Locale (PAL)*

ACCENTURE, **primo fornitore di Cyber Security in Italia**, con più di 1000 professionisti in Italia ed una rete internazionale di più di 8000 professionisti che supporta quotidianamente i suoi Clienti nella **gestione ed evoluzione della proprie soluzioni e servizi di sicurezza**

FASTWEB, uno dei **principali operatori di telecomunicazioni** in Italia con una strategia infrastrutturale basata su approccio integrato di asset strategici che abilitano **servizi sempre più avanzati di Cyber Security**

DEAS SPA, **PMI innovativa specializzata in Cyber Security e AI**, in grado di fornire soluzioni tecnologiche con gli **standard più alti del settore in ambito sicurezza informatica**, intelligenza artificiale, GDPR, modelli di governance, soluzioni di continuità operativa.

FINCANTIERI NEX TECH, società tecnologica di eccellenza tutta italiana attiva principalmente nello **sviluppo di soluzioni per la Difesa e la Sicurezza**, capace di offrire prodotti e servizi cutting edge nel campo della Cyber Security



IV – COME ADERIRE

MODALITÀ DI ATTIVAZIONE

1 PIANO DEI FABBISOGNI

- *Template disponibile sul sito di Consip*
- *Tramite invio PEC (sicurezza.remotolotto1.pec@legalmail.it)*

2 PIANO OPERATIVO

- *Reso disponibile entro **15 gg lavorativi** dal Piano fabbisogni*
- *Tramite invio PEC (sicurezza.remotolotto1.pec@legalmail.it)*

3 CONTRATTO ESECUTIVO

*Richiesta di modifiche / approvazione entro **30 giorni solari***

CONTATTI

PORTALE FORNITURA

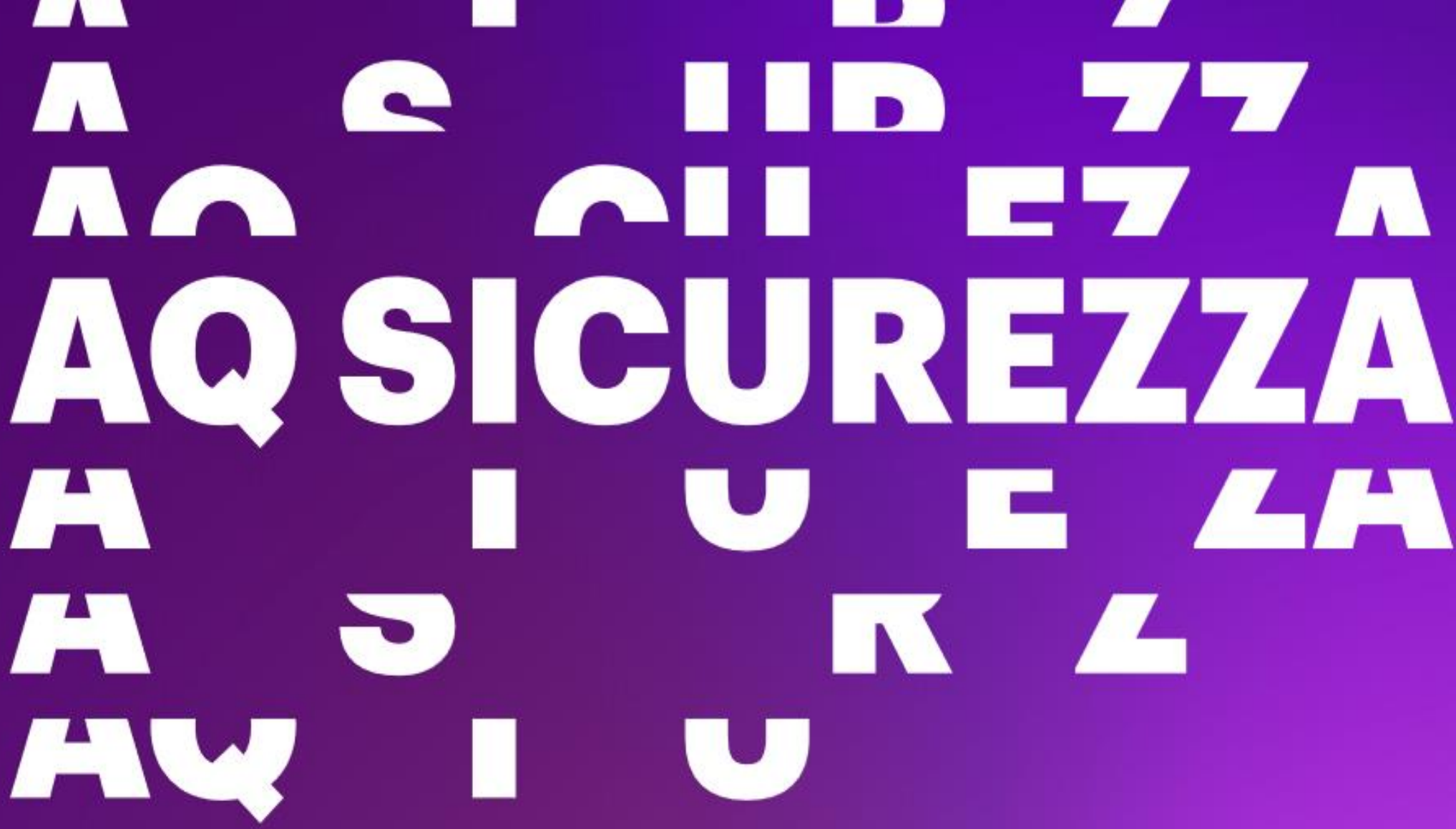
aqsicurezzalotto1pal.it

PEC Lotto 1

sicurezza.remotolotto1.pec@legalmail.it

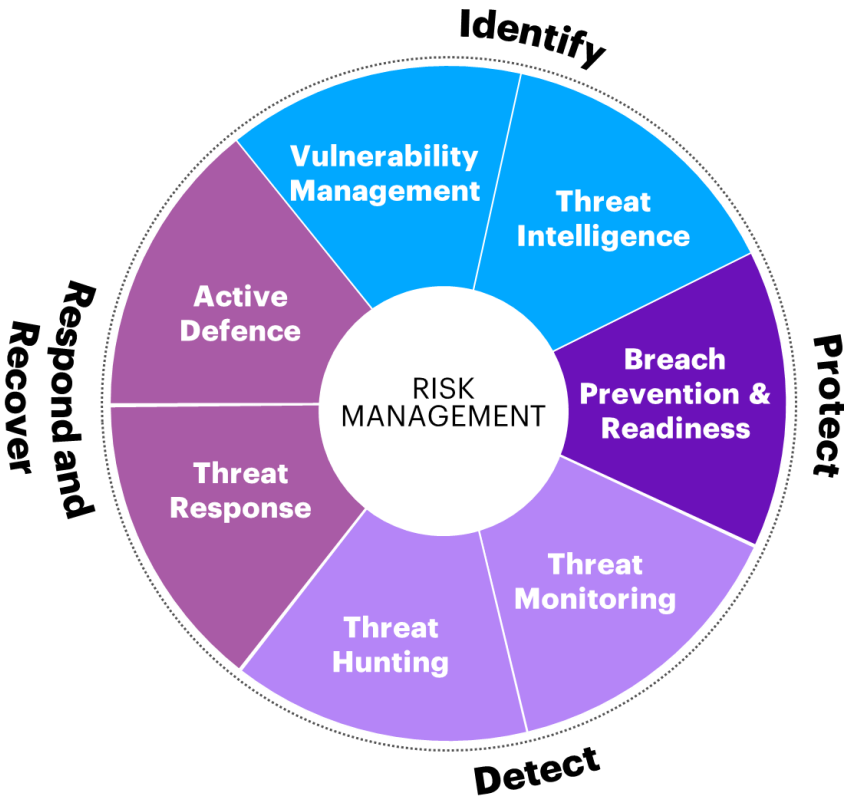
Email Lotto 1

sicurezza.remotoL1@accenture.com



II - I SERVIZI OFFERTI

OVERVIEW DEI SERVIZI OFFERTI



L1.S1 - Security Operation Center (SOC)
paloalto splunk>

L1.S2 – Next Generation Firewall
FORTINET

L1.S3 – Web Application Firewall
FORTINET

L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza
tenable

L1.S5 – Threat Intelligence & Vulnerability Data Feed
iDefense

L1.S6 – Protezione Navigazione Internet e Posta Elettronica
FORTINET

L1.S7 – Protezione Endpoint
TREND MICRO

L1.S8 – Certificati SSL
ENTRUST

L1.S9 – Formazione e Security Awareness
Accenture Security Training

L1.S10 – Gestione delle Identità e Accesso dell'Utente

L1.S11 – Firma Digitale Remota
uanataca trust service provider

L1.S12 – Sigillo Elettronico
uanataca trust service provider

L1.S13 – Timbro Elettronico
bluenet

L1.S14 – Validazione Temp. Elettronica Qualificata
uanataca trust service provider

L1.S15 – Servizi Specialistici

Il nostro RTI è grado di adattarsi dinamicamente alle necessità della singola PA per cui le **tecnologie proposte** possono **variare** in base al **contesto tecnologico**, alla **dimensione** e alla **maturità** della stessa in ambito cybersecurity.

OVERVIEW DEI SERVIZI OFFERTI

MAPPATURA CON IL FRAMEWORK NIST

IDENTIFY		PROTECT			DETECT		RESPOND & RECOVER	
Vulnerability Management	Threat Intelligence	Breach Prevention & Readiness			Threat Monitoring	Threat Hunting	Threat Response	Active Defence
HELP DESK								
Prevenzione e gestione delle minacce								
L1.S4 Gestione continua delle vulnerabilità di sicurezza	**L1.S5** Threat Intelligence & Vulnerability Data feed	**L1. S2** Next Generation Firewall	**L1.S3** Web Application Firewall	**L1.S6** Protezione navigazione internet e posta elettronica	**L1.S1** Security Operation Center			
		L1.S7 Protezione end point	**L1.S8** Certificati SSL	**L1.S9** Formazione e security awareness				
Autenticazione accessi e validità probatoria								
		L1.S10 Gestione identità e accesso utente	**L1.S11** Firma digitale remota	**L1.S12** Sigillo elettronico				
			L1.S13 Timbro elettronico	**L1.S14** Validazione temporale elettronica qualificata				
Supporto al delivery e alla migrazione dei servizi								
L1.S15 Servizi specialistici								

FOCUS SERVIZI 1/3

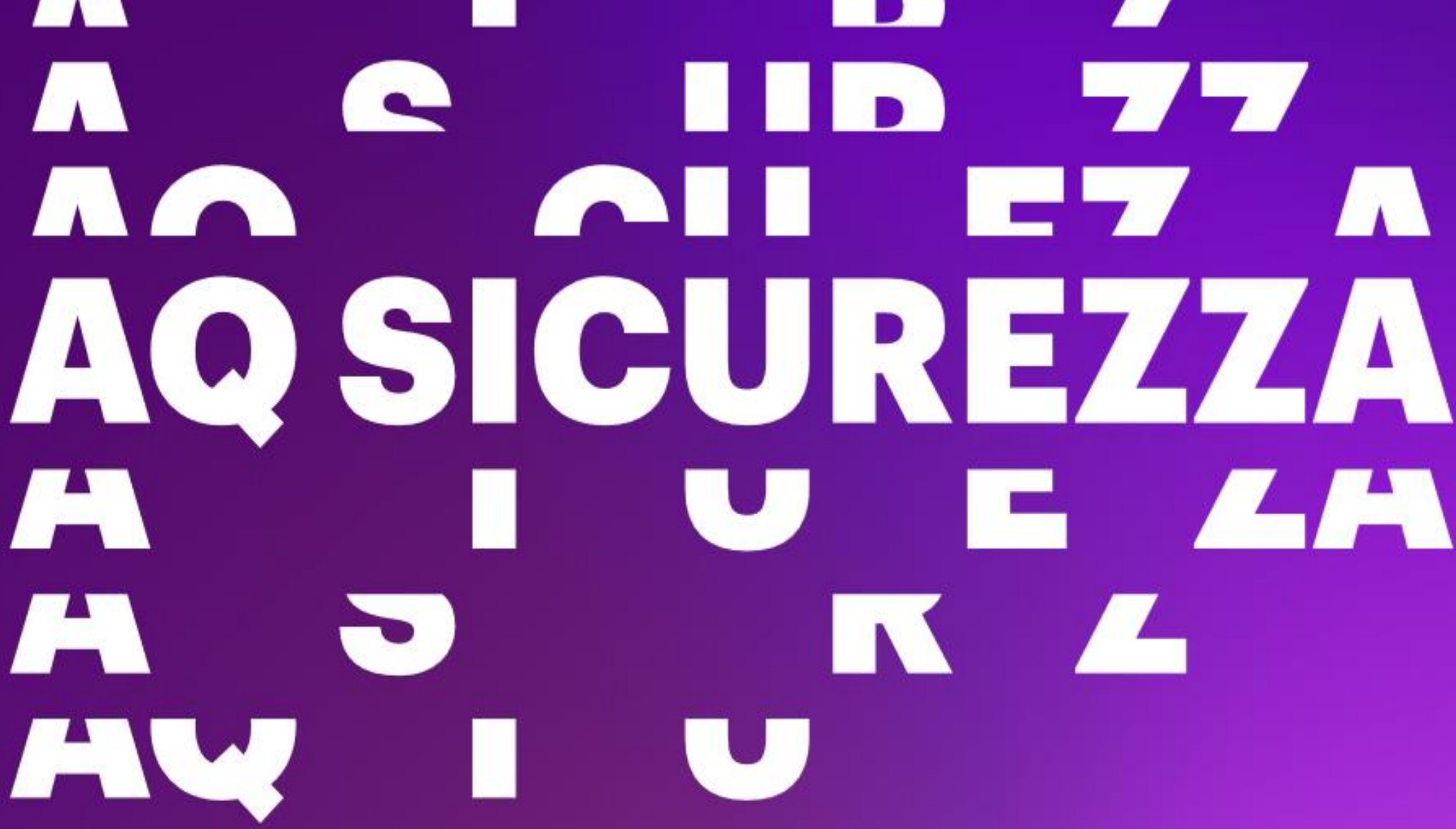
Servizi	Descrizione
L1.S1 - Security Operation Center (SOC)	Centro da cui vengono erogati servizi alle Amministrazioni per assicurare il corretto funzionamento dei sistemi attraverso **la prevenzione, la gestione, il monitoraggio, l'analisi, la risoluzione di eventuali criticità di sicurezza** che possano degradare il servizio. Include il processo di **gestione degli incidenti di sicurezza**, attivato al fine di evitare o ridurre al minimo la compromissione di dati e servizi dell'Amministrazione: dopo aver segnalato un incidente di sicurezza all'Helpdesk, il Fornitore identifica e analizza un incidente, identifica le azioni di contenimento, trasmette l'evidenza digitale dell'incidente e valuta l'incidente verso un miglioramento continuo.
L1.S2 – Next Generation Firewall	Servizio che permette di **filtrare tutto il traffico** che i dispositivi di rete scambiano sia internamente che esternamente rispetto ad un determinato perimetro, **limitando o bloccando eventi** quali accessi non autorizzati, malware o servizi non consentiti, attraverso un insieme definito di regole di controllo (policy) accessi e tramite l'orchestrazione di più livelli di sicurezza, ciascuno dedicato a una specifica funzione di controllo.
L1.S3 – Web Application Firewall	Servizio che consente di **filtrare, monitorare e bloccare il traffico HTTP** da e verso un servizio web, esaminando il traffico, utilizzando regole, analisi e firme per rilevare gli attacchi incorporati nei dati trasmessi dalle applicazioni web.
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	Processo automatico di valutazione della vulnerabilità il cui obiettivo è ottenere un'istantanea del **livello e della gravità del rischio** a cui, in quel momento, sono esposti i sistemi informativi dell'Amministrazione. Il servizio si avvarrà di uno scanner che produrrà un **report con specifiche indicazioni di rischio** relative alle vulnerabilità rilevate.
L1.S5 – Threat Intelligence & Vulnerability Data Feed	Servizio che consente di ricevere un flusso continuo di dati relativi alle **minacce e alle vulnerabilità di sicurezza** del Sistema Informativo, consentendo di **prevedere/prevenire le minacce** prima che entrino in azione, migliorando i controlli attuali e le funzioni forensi.

FOCUS SERVIZI 2/3

Servizi	Descrizione
L1.S6 – Protezione Navigazione Internet e Posta Elettronica	Servizio che consente di bloccare l'accesso a **siti potenzialmente dannosi**, controllare le **applicazioni Web** e rilevare e filtrare il **codice dannoso**. Nel caso delle e-mail, il servizio aiuta a proteggere dai contenuti dannosi nelle e-mail impedendo loro di raggiungere il destinatario previsto.
L1.S7 – Protezione Endpoint	Servizio che protegge i dispositivi connessi alla rete aziendale (es. pc desktop, laptop, smartphone, tablet) **da accessi non autorizzati** o dall'esecuzione di **software dannoso**, garantendo che i dispositivi raggiungano un **livello di sicurezza** definito e rispettino i requisiti di compliance dell'Amministrazione.
L1.S8 – Certificati SSL	I protocolli di sicurezza standard (SSL e il suo successore TLS) garantiscono l'**affidabilità** e la **sicurezza della comunicazione** tra i componenti client e server di un'applicazione Internet, assicurando che le informazioni sensibili fornite dagli utenti sul Web rimangano riservate.
L1.S9 – Formazione e Security Awareness	Servizio che mira a sensibilizzare l'Amministrazione sui vari aspetti della sicurezza delle informazioni, aumentando il **livello di consapevolezza** dei dipendenti e quindi elevando il livello di sicurezza dell'Organizzazione. L'obiettivo è sviluppare negli utenti le competenze, le tecniche ei metodi fondamentali per prevenire il più possibile gli **incidenti di sicurezza** e per reagire al meglio a fronte di eventuali problemi..
L1.S10 – Gestione delle Identità e Accesso dell'Utente	Servizio che consente la gestione completa delle attività di **identificazione, autenticazione e autorizzazione** prima dell'accesso da parte di utenti esterni al portale di Amministrazione o ai servizi da essa erogati in rete.

FOCUS SERVIZI 3/3

Servizi	Descrizione
L1.S11 – Firma Digitale Remota	Servizio che permette di conferire **efficacia probatoria** a documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali. La firma digitale garantisce l'autenticità, l'integrità e il non ripudio dei documenti informatici.
L1.S12 – Sigillo Elettronico	Servizio che permette di conferire **efficacia probatoria** a documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.
L1.S13 – Timbro Elettronico	Servizio che consente alle Amministrazioni la creazione di documenti informatici che possano conservare la medesima **validità legale** anche dopo essere stati stampati su supporto cartaceo.
L1.S14 – Validazione Temporanea Elettronica Qualificata	Servizio che fornisce alle Amministrazioni, mediante un **Certificatore accreditato**, di associare data e ora, certe e legalmente valide, a un documento informatico, permettendo una **validazione temporale** del documento opponibile a terzi.
L1.S15 – Servizi Specialistici	Supporto tecnico connesso all'attivazione di servizi da remoto da erogare attraverso la fornitura di **figure professionali** in grado di fornire supporto nell'ambito della **migrazione** dei **servizi di sicurezza**, **erogazione**, **monitoraggio continuo** delle vulnerabilità di sicurezza.



III – DETTAGLIO DEI SERVIZI

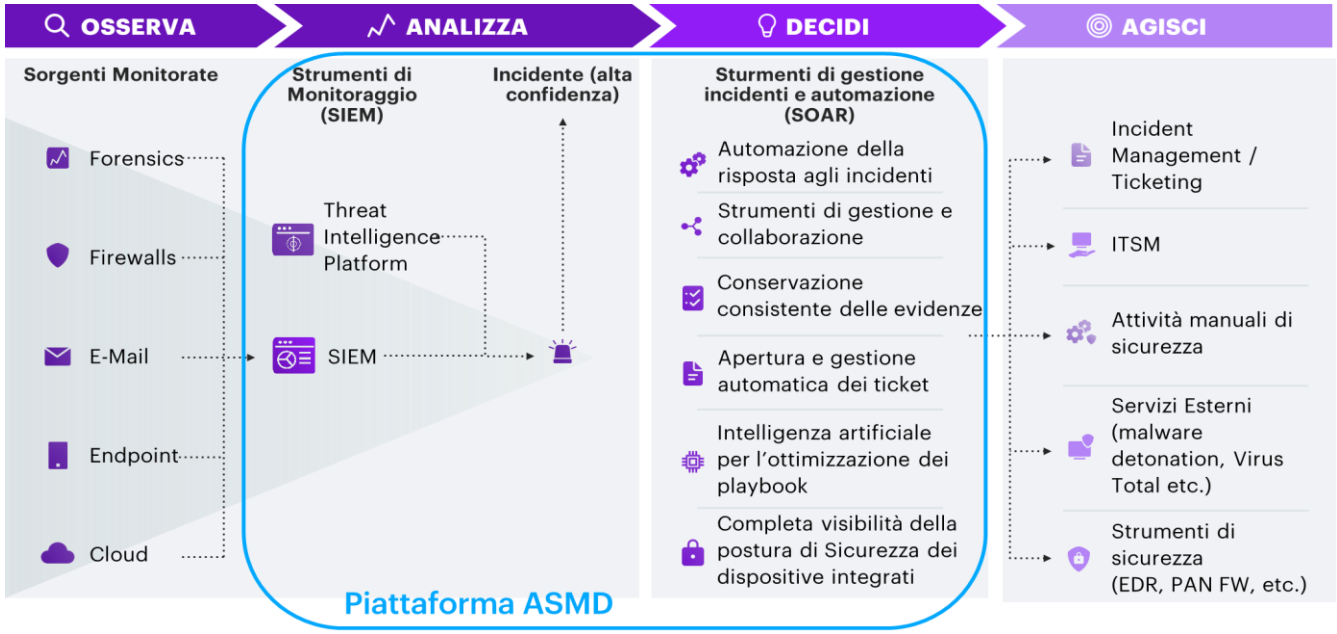
SECURITY OPERATION CENTER (SOC)

Il Modello di "**Next Generation Security Operation Center (NG-SOC)**" è basato sulla **piattaforma tecnologica di Accenture** denominata "**Advanced Security Monitoring & Detection (ASMD)**"

Integrazioni

- **Splunk** per la parte di "Security Information & Event Management (**SIEM**)"
- **PaloAlto Cortex XSOAR** per la parte di "Security Orchestration, Automation & Response (**SOAR**)", entrambi **leader di mercato** (Gartner / Forrester

La soluzione opera in modalità **24x7x365** e viene erogata **dai SOC di Napoli e Milano, operanti all'interno dei Centri Servizi** in ambito di gara



FULL STACK DEFENDER

- *Contestualizzazione e arricchimento eventi*
- *Use Case Tuning & Improvement*
- *Full Stack Defender*
- *Contenimento automatico delle minacce*
- *Case Management Assistito*
- *Threat Intelligence & Vulnerability Data Feed*

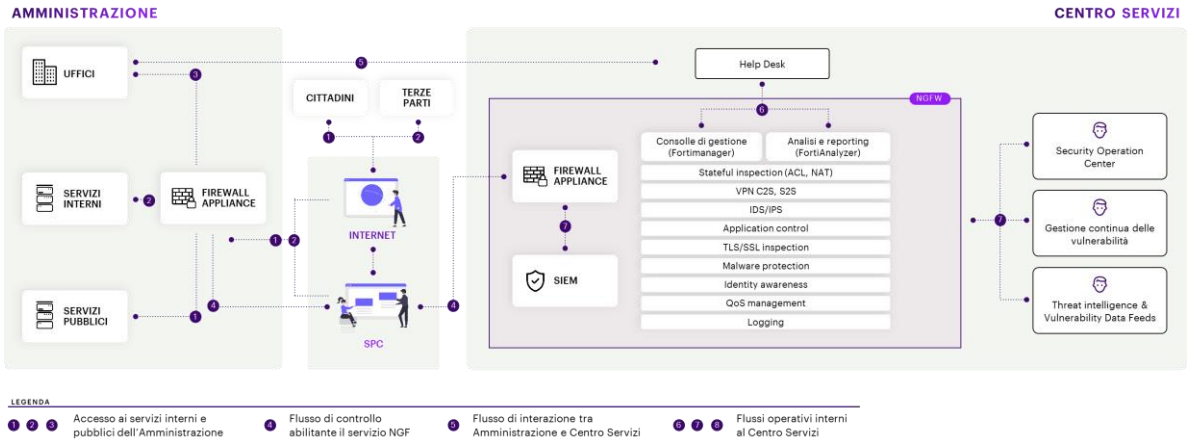
- ***Case Mgmt assistito***
- ***Gestione accessi***
- ***Arricchimento e TI***
- ***E-mail Gateway***
- ***Forensics e Malware Analysis***
- ***Endpoint Protection e contenimento minacce***
- ***Firewall, IDPS, Web Gateway***
- ***Vulnerability Management***

NEXT GENERATION FIREWALL

Controlli di sicurezza essenziali alla protezione di rete, disponibili come security profile: **Intrusion Prevention, Antivirus, Cloud Sandbox, Application Control** e **Web Filtering**.

Tecnologia e integrazioni

- Soluzione basata **su tecnologia Fortinet**
- **Integrazione del NGFW** (o gateway), nella sua forma fisica o virtuale, localmente presso la singola PA oppure remotamente presso il Centro Servizi (scelta subordinata agli accordi con la PA contraente).
- Console di gestione centrale, **FortiManager**, con visibilità generale sullo stato dei singoli gateway, e configurazione della soluzione e relativo monitoraggio anche grazie all'integrazione con la soluzione SIEM, gli Active Directory o altri user repository



Specifiche e servizi inclusi

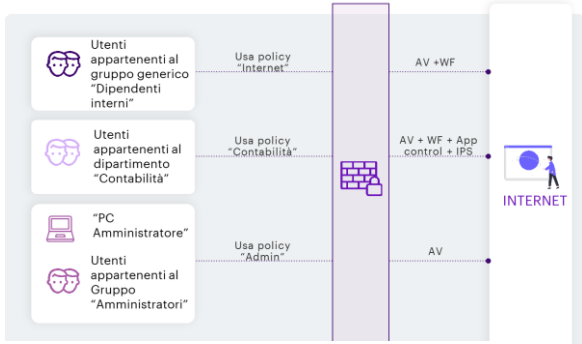
Controlli di sicurezza essenziali alla protezione di rete, disponibili come security profile:

- ✓ **Intrusion Prevention,**
- ✓ **Antivirus, Cloud Sandbox,**
- ✓ **Application Control,**
- ✓ **Web Filtering**.

Controllo puntuale delle operazioni ammesse agli utenti (in linea con il modello Zero Trust) e possibilità di analizzare i flussi di traffico sia a scopi di reportistica sia per esecuzione di indagini forensi a seguito di incidenti di cybersecurity, mediante le tecnologie:

- ✓ **Fortinet Single Sign-On (FSSO)**
- ✓ **FortiAnalyzer**.

- ***Gestione politiche*** *e* ***configurazioni***
- ***Stima*** *degli* ***impatti*** *e misura del* ***rischio***
- ***Rilevamento avanzato*** *del* ***malware***
- ***Analisi predittiva*** *della sfruttabilità delle vulnerabilità*



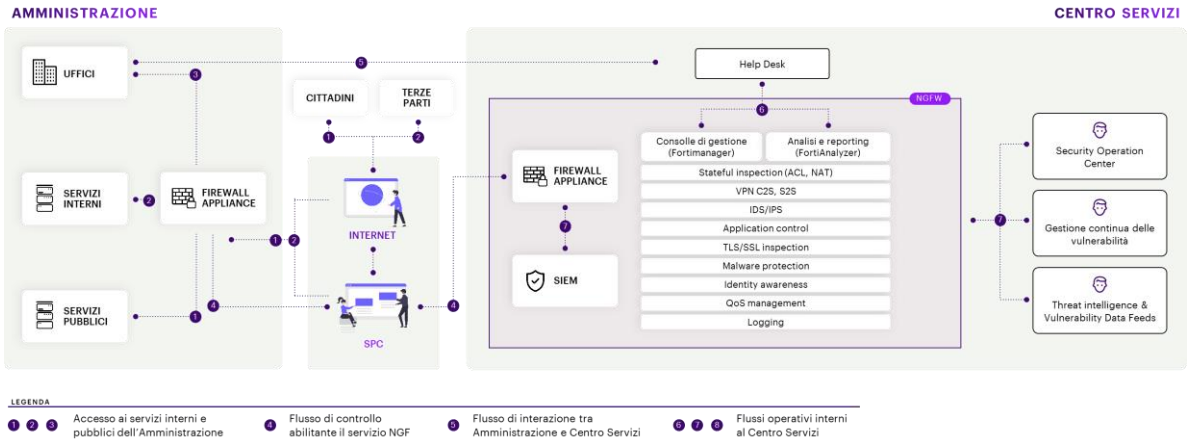
Esempio della dashboard di analisi per erogare "IDS e IPS"

WEB APPLICATION FIREWALL

Le vulnerabilità delle **Applicazioni Web** possono portare a violazioni dei dati o al blocco di sistemi **mission-critical** per la PA, motivo per cui il servizio WAF proposto vuole **superare i limiti** dei normali Intrusion Detection System e dei tradizionali sistemi WAF che si affidano all'apprendimento delle applicazioni (manuale o automatico) per il rilevamento di anomalie e minacce.

Tecnologia e integrazioni

- Soluzione basata **su tecnologia Fortinet**
- **Integrazione del NGFW** (o gateway), nella sua forma fisica o virtuale, localmente presso la singola PA oppure remotamente presso il Centro Servizi (scelta subordinata agli accordi con la PA contraente).
- La gestione degli apparati WAF avviene mediante la console di gestione centrale FortiManager e l'ulteriore elemento centrale di analisi, logging e reporting, **FortiAnalyzer**



Specifiche e servizi inclusi

- ✓ **Motore di apprendimento automatico (ML)** per costruire e aggiornare autonomamente un **modello di comportamento dell'utente (Behavioral Analytics)** ed utilizzare tale modello per discriminare il traffico lecito da quello malevolo, permettendo di bloccare in modo molto più efficace anche le minacce sconosciute (**exploit zero-day**)
- ✓ **Due livelli di apprendimento automatico**, uno basato sull'**AI** ed uno sulle **probabilità statistiche** per rilevare anomalie e minacce separatamente e funzionalità, fondamentali per la protezione da exploit zero-day: **ML, Rilevamento bot e Sandbox**
- ✓ Funzionalità di **full SSL inspection (Deep Inspection)** al fine di garantire che anche il contenuto crittografato venga ispezionato
- ✓ Interazione con tutti gli altri elementi dell'infrastruttura e **modello operativo integrato**

- ***Stima degli impatti e misura del rischio***
- ***Rilevamento avanzato del malware***
- ***Analisi predittiva della sfruttabilità delle vulnerabilità***

GEST. CONTINUA VULN. SICUREZZA

Tecnologia e integrazioni

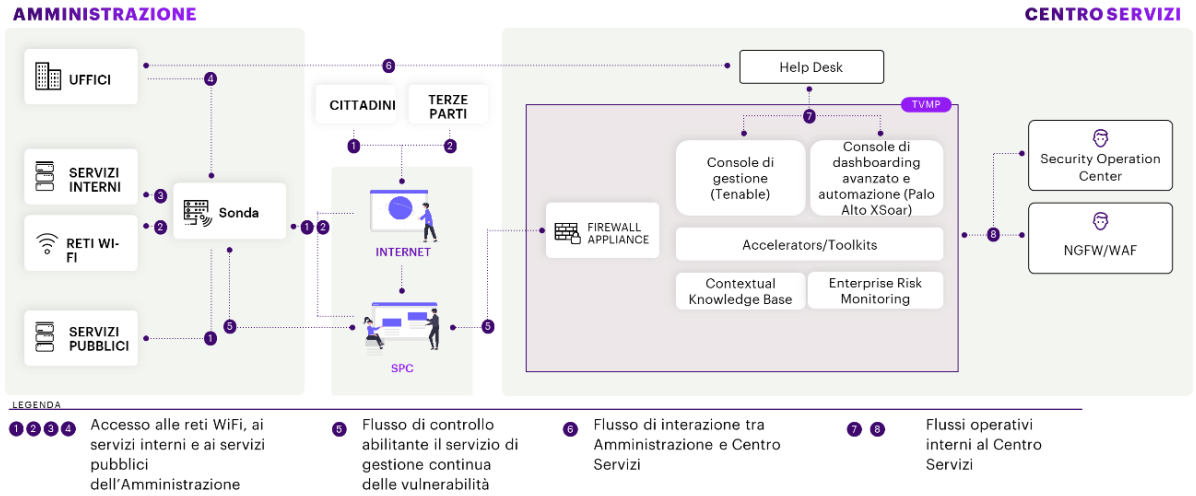
Modello di servizio proprietario che permette la **gestione dell'intero ciclo di vita delle vulnerabilità** attraverso l'adozione di una piattaforma TVMP (**Threat and Vulnerability Management Platform**), dispiegata c/o il Centro Servizi e integrata con altri sistemi di controllo, a cui accede esclusivamente personale altamente qualificato e certificato e prevede:

- Una **console di gestione**
- Una **console** per il **dashboarding** avanzato e l'automazione
- Un **modulo di supporto**
- Un modulo di **monitoraggio del rischio**
- **Knowledge base** contestualizzata

Servizi

- ✓ ***Gestione** dei **piani** e **configurazione scansioni***
- ✓ ***Conduzione** del **Servizio***
- ✓ ***Rendicontazione** direzionale e rapporti tecnici*
- ✓ ***Analisi e correlazione** di vulnerabilità*
- ✓ ***Classificazione dinamica** degli asset*
- ✓ ***Stima degli impatti** e misura del rischio*
- ✓ ***Rilevamento avanzato** del **malware***
- ✓ ***Analisi predittiva** della sfruttabilità della vulnerabilità*

«**Cruscotti dinamici personalizzabili**» sullo stato della sicurezza, personalizzabili in base alle esigenze e accessibili da una console centralizzata della TVMP con apporto del TVM team per la realizzazione e l'aggiornamento di un **cruscotto aggiuntivo di 'Enterprise Risk Monitoring'** per la singola PA



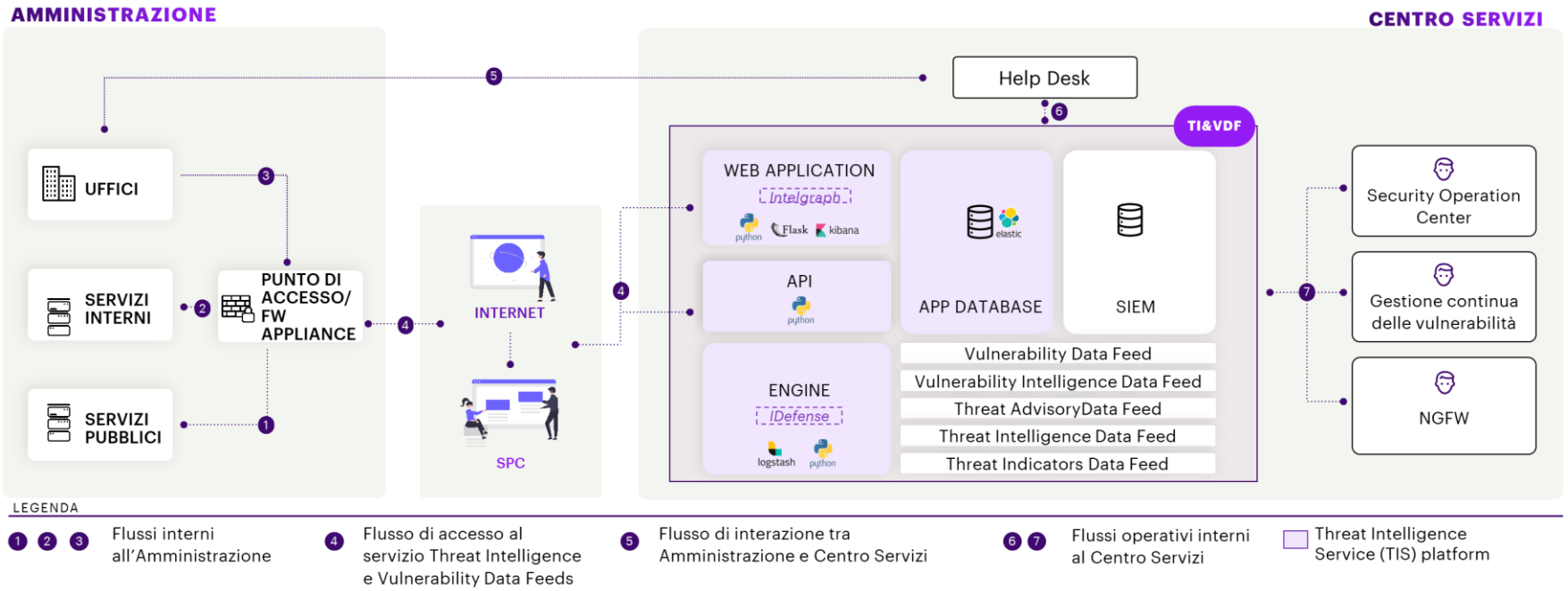
TI & VULNERABILITY DATA FEED

Servizio erogato dal Centro Servizi avvalendosi della **piattaforma Threat Intelligence Service (TIS), sviluppata e gestita da Accenture** e che integra il **servizio specialistico iDefense di Accenture** che prevede l'accesso tramite interfaccia Intelgraph e API alle **informazioni di intelligence** che coprono le vulnerabilità di oltre 1.000 vendor, **strumenti e tecniche malware**, Indicatori di Compromissione, organizzazioni target, threat actor e loro motivazioni, campagne di phishing e minacce pertinenti l'organizzazione aziendale.

Il servizio è reso disponibile tramite una **interfaccia web e accesso API**

iDefense

- ***Accesso web***
- ***Personalizzazione delle informazioni***
- ***Intelligence***
- ***Analisi / Prioritizzazione***
- ***Interazioni con i servizi Gestione Continua delle vulnerabilità e Next Generation Firewall***

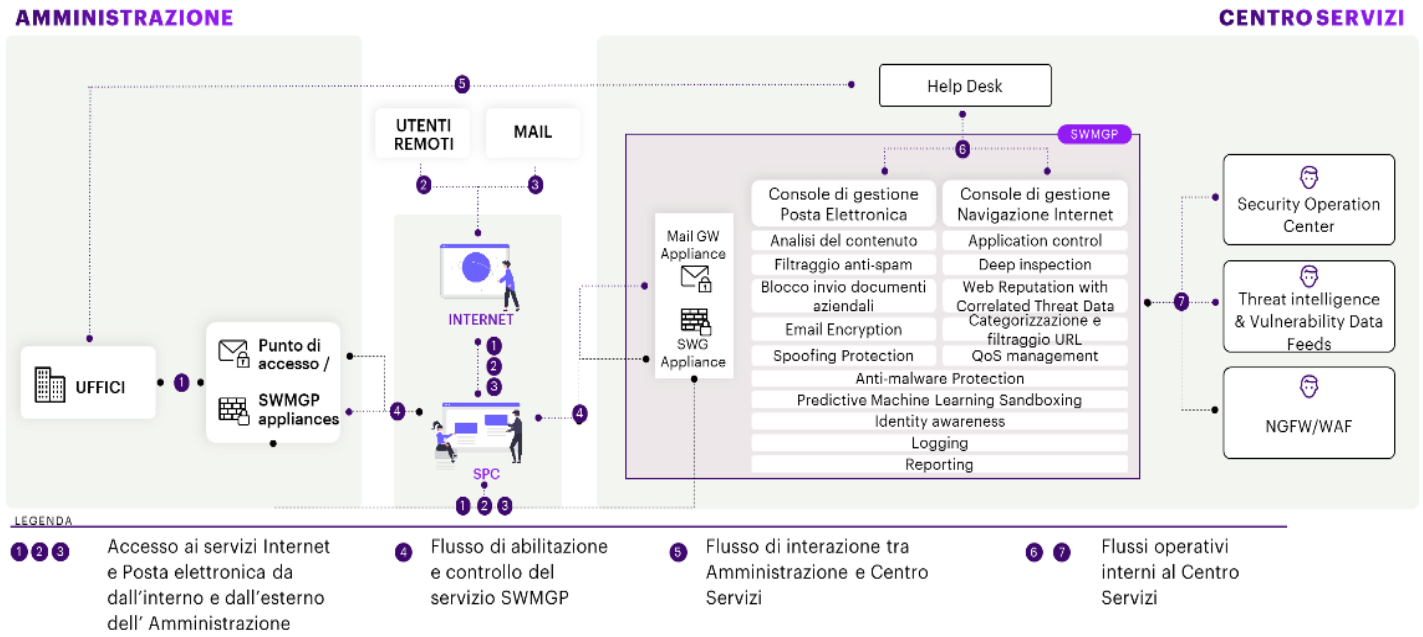


La piattaforma si basa su **tecnologie open source** quali:

- **Stack Elastilk** (ELK) che include (i) Elasticsearch, (ii) Logstash, (iii) Kibana;
- **Python**, un linguaggio di programmazione adattabile e largamente utilizzato per numerosi progetti anche in ambito cyber security;
- **Flask**, un micro web framework scritto in Python utilizzato per la costruzione di applicazioni web

PROTEZIONE NAVIGAZIONE INTERNET E POSTA ELETTRONICA

Il servizio ha lo scopo di **proteggere gli utenti e i sistemi delle PA da minacce esterne di natura cyber provenienti da web e/o email** e di preservare affidabilità, disponibilità, riservatezza e integrità delle comunicazione tra le componenti client e server del patrimonio informativo posto in perimetro



- ***Predictive Machine Learning Sandboxing***
- ***Adaptive Trust Engineering***
- ***Business Email Compromise e Impersonation Attack Protection***
- ***Reporting***
- ***ML Integrato con Threat Intelligence Dissemination***
- ***Integrazione con Threat Intelligence & Vulnerability Data Feed***
- ***On demand investigation***

Modello di servizio proprietario che arricchisce, attraverso l'adozione della **piattaforma SWMGP** (Secure Web and Mail Gateway Platform), dispiegata c/o il Centro Servizi e integrata con altri **sistemi di controllo attivo e passivo** (SIEM/SOAR, TIS, FWM), alla quale accede esclusivamente personale esperto, altamente qualificato e certificato. La SWMGP integra tecnologie leader di settore (**FortiGate SWG, FortiMail**) e strumenti e acceleratori proprietari del RTI.

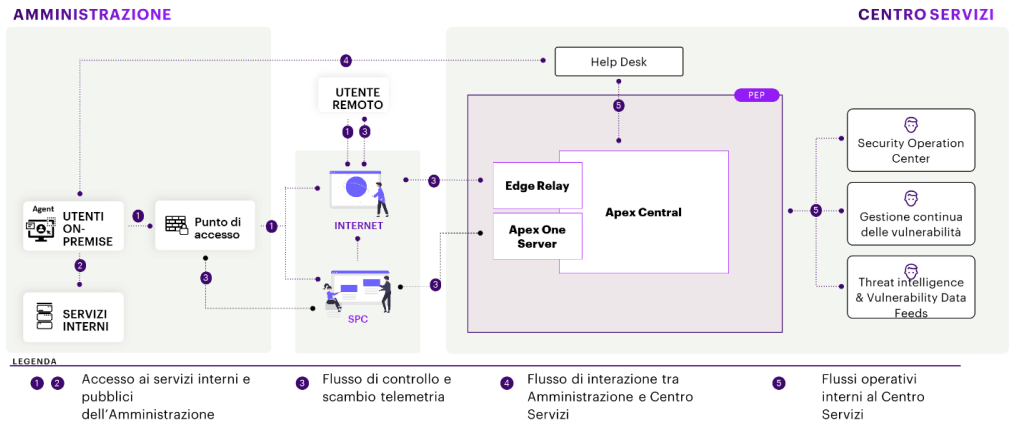
Il Centro Servizi del RTI si avvale, peraltro, della rete di **CyberFusion Center** resa disponibile da Accenture e altamente specializzata sia nella *"deep inspection"* del codice scaricato da internet che nel rilevamento di accessi ad applicazioni Cloud (SaaS) non conformi alle politiche delle PAL contraenti, così come della **rete di monitoraggio del traffico internet** resa disponibile da Fastweb attraverso le proprie infrastrutture di sicurezza.

PROTEZIONE DEGLI END POINT

Uno degli elementi chiave forniti dal Centro Servizi per garantire la sicurezza delle infrastrutture delle PA, **operando direttamente sui dispositivi in uso agli utenti** abilitando sia l'**identificazione di anomalie** di processo che le **azioni di contenimento e reazione** da implementare **in caso di violazione**

Tecnologia e integrazioni

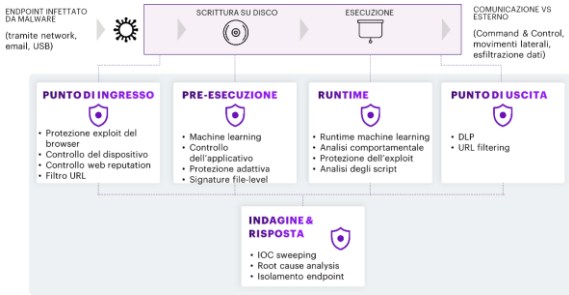
La soluzione tecnologica di Endpoint Protection proposta è **basata su tecnologia TrendMicro ApexOne**, riconosciuta come **leader sul mercato** da **Gartner** nel Magic Quadrant 2021 di Endpoint Protection Platform.



Specifiche e servizi inclusi

- ✓ **Sistema automatizzato avanzato** di rilevamento e risposta a una varietà sempre più ampia di minacce, tra cui fileless e ransomware
- ✓ **Approfondimento delle informazioni**, **capacità investigative ampliate** e **visibilità centralizzata** tramite una forte integrazione SIEM e l'adozione di un set di API aperto
- ✓ **Protezione integrata** gestita da un singolo agente per rilevamento, risposta e indagine delle minacce, riducendo l'effort di gestione da parte delle singole PA
- ✓ Applicazione di **azioni di contenimento** fra loro **complementari**

- ***Antimalware Avanzato***
- ***Risk-based evaluation***
- ***Sandboxing***
- ***Reporting***
- ***Interazioni con i servizi Gestione continua delle vulnerabilità di sicurezza e di Threat Intelligence & Vulnerability Data Feed***



Schema della soluzione tecnologica

CERTIFICATI SSL

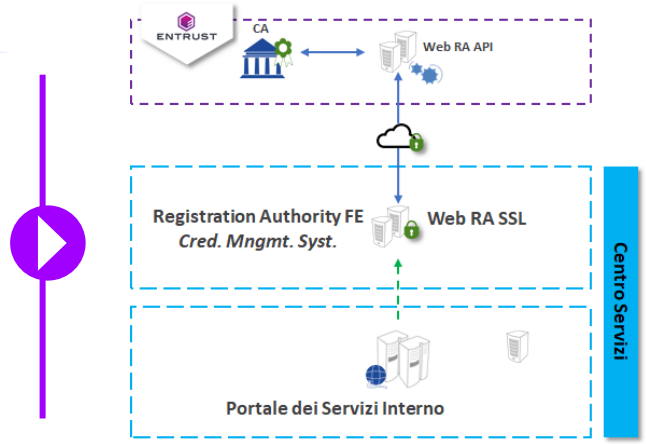
Il certificato **SSL (Secure Sockets Layer)** e i l suo successore TLS (Transport Layer Security), sono protocolli standard necessari a garantire affidabilità e sicurezza della comunicazione tra le componenti client e server di un'applicazione internet. Esso assicura che le **informazioni sensibili** fornite dagli utenti **sul web rimangano riservate** e non vengano in alcun modo intercettate da terze parti (comunicazione criptata tra il client server e il server web).

Funzionalità Minime

- **Utilizzo di certificati digitali** sia lato server che, se richiesto, lato client
- **Emissione da una Certification Authority (CA)** accreditata al CA/Browser Forum (CAB Forum)(*)
- **Disponibilità** alle Amministrazioni **di tutte le tipologie di certificati SSL** Server per soddisfare tutte le esigenze
- Possibilità per le Amministrazioni di richiedere certificati per la firma del codice, detti **«CodeSigning»**

Specifiche e servizi inclusi

- ✓ **Integrazione** dell'emissione dei certificati nei processi dell'Organizzazione senza alterare la user experience e/o i workflow
- ✓ **Applicazione Web** intuitiva per l'emissione dei certificati digitali
- ✓ **Integrazione tramite API,** servizio di assistenza tecnica gratuita e personalizzata



Esempio architettura e workflow

(*) Valido e riconosciuto world-wide dai principali browser e sistemi operativi

FORMAZIONE E SEC. AWARENESS

L'obiettivo del servizio è quello di sensibilizzare il **personale** delle PA sulle **tematiche inerenti alla sicurezza** delle informazioni ed evitare che comportamenti non adeguati dei singoli soggetti possano compromettere la sicurezza dell'intero sistema e **sviluppare negli utenti le competenze essenziali**, le tecniche e i metodi fondamentali **per prevenire il più possibile gli incidenti di sicurezza** e reagire al meglio a fronte di eventuali problemi

Training online

«Corsi in aula»

Newsletter e eCards

Webinair

Flyer e brochure

Quiz

Simulazioni

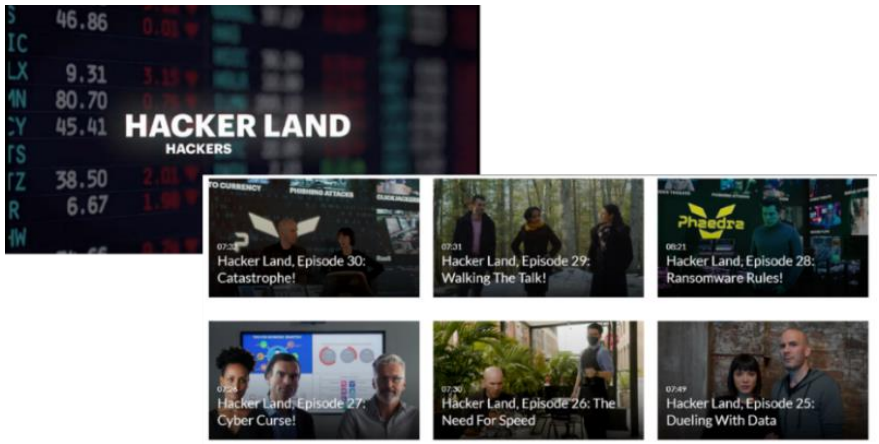
Podcast

«Consigli del giorno»

- ✓ ***Sezione di Awareness*** – *Innovativo sistema integrato di e-learning, coinvolgimento dell'intera Organizzazione con percorsi educativi e stimolanti*
- ✓ ***Sezione Phishing*** – *Innovativo sistema di e-training ideato sulla base di metodologia «training on the job», con peculiarità automatizzate e basate su logiche di ML*
- ✓ ***Sezione Informativa*** – *Percorso di formazione video basato su metodologia induttiva e realizzato con tecniche di produzione avanzata e storytelling particolarmente coinvolgente*

Piattaforma di e-learning "**Accenture Security Training**" verrà installata presso il Centro Servizi e **aggiornata continuativamente** in termini di contenuti informativi.

- ***Training Online***
- ***Corsi in aula***
- ***Newsletter e E-Cards***
- ***Webinar***
- ***Flyer e Brochure***
- ***Quiz***
- ***Campagne di simulazioni***
- ***Podcast***
- ***Consigli del giorno***
- ***Ebook periodici***



GESTIONE IDENTITÀ E ACCESSO

Il servizio consente all'Amministrazione la **completa gestione delle attività di identificazione, autenticazione ed autorizzazione** propedeutiche all'accesso da parte di utenti esterni al portale dell'Amministrazione o ai servizi da essa erogati in rete.

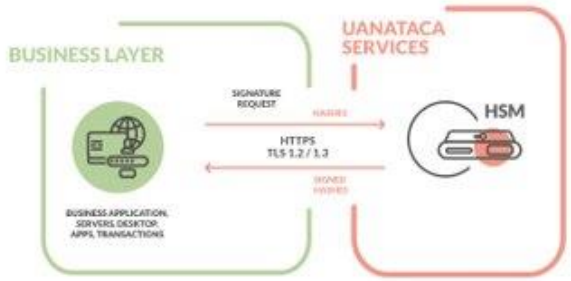
Funzionalità Minime in ambito Certificati SSL

- ***Gestione dei profili (creazione/migrazione):*** *le Pubbliche Amministrazioni potranno aderire alle regole tecniche definite da SPID (specifiche SAML) senza dover realizzare e/o modificare le proprie infrastrutture tecnologiche*
- ***Supporto della politica di "Policy Enforcement"*** *per interfacciarsi con Identity Provider e Attribute Authority al fine di ricevere le richieste per l'applicazione delle policy di sicurezza associate alle risorse*
- ***Supporto della politica di "Policy Decision",*** *in grado di accedere ai i profili degli utenti e alle policy di sicurezza associate alle risorse per la verifica della legittimità della richiesta*
- ***Gestione delle policy di accesso ai servizi e la gestione del ciclo di vita dei profili utente,*** *suddivisione degli utenti in gruppi omogenei tipo Role-based Access Control (RBAC)*
- ***Verifica degli attributi esterni all'Amministrazione*** *ed associati al profilo di un utente a carico di Attribute Authority esterne*
- ***Accesso a interfaccia web*** *con visibilità dei soli dati degli utenti profilati per applicazioni erogate dalla propria Amministrazione e per le quali è referente a livello di Contratto esecutivo*
- ***Su richiesta, presa in carico e migrazione dei profili utente gestiti dall'Amministrazione***

FIRMA DIGITALE REMOTA

Firma elettronica qualificata che permette alle Amministrazioni di dare **efficacia probatoria ai documenti informatici firmati digitalmente,** favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.

1	*Firma digitale in formato CADES, PADES e XADES e conforme allo standard europeo EIDAS.*
2	*Completo controllo delle proprie identità digitali remote attraverso l'utilizzo della Registration autority.*
3	*Disponibilità di software desktop per l'apposizione della Firma e Verifica (FIRMA 4 NG)*
4	*Disponibilità di APP mobile per Android e IOS per l'apposizione della Firma e Verifica (SignCloud) – OPZIONALE*
5	*Disponibilità di applicazione web per la verifica dei documenti (Validatore On-Line)*
6	*Possibilità di integrazione della firma elettronica nei processi esistenti senza alterare la «user experience» attraverso l'utilizzo delle API REST.*

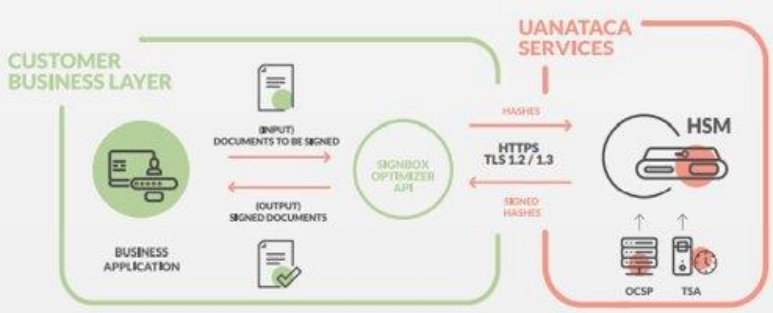


Il servizio di firma digitale remota semplifica la user experience dell'utente evitando l'utilizzo di dispositivi fisici e mantenendo lo stesso livello di sicurezza (Sign AnyWhere).

SIGILLO ELETTRONICO

Al pari del servizio precedente, consente alle Amministrazioni di dare **efficacia probatoria ai documenti informatici firmati digitalmente**, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.

1	*Integrazione firma elettronica nei processi senza alterare la «user experience»*
2	*Integrazione via API, disponibilità ambienti di test*
3	*Supporto tecnico personalizzato*
4	*Conformità a Eidas e GDPR*



*Il servizio **«Bulk Electronic Signature»** permette la firma automatica di documenti, sia tramite l'integrazione **l'API SignBox** Uanataca, sia mediante l'utilizzo dell'applicazione SignBox del cliente.*

TIMBRO ELETTRONICO

Il servizio consente alle Amministrazioni di creare **documenti informatici** che possano conservare la **medesima validità legale** anche dopo essere stati stampati su **supporto cartaceo.**

Funzionalità Minime garantite

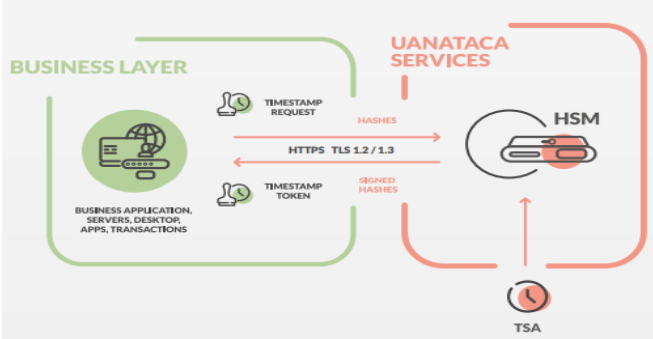
- ***Creazione ed emissione*** *del Timbro Elettronico*
- ***Verifica del Timbro Elettronico*** *e* ***della conformità*** *del documento stampato rispetto all'originale informatico*
- ***Gestione delle credenziali e creazione di specifici profili*** *deputati all'apposizione del timbro*

- ✓ ***Tmbrel™ –*** *Sistema di Gestione dei Sigilli Digitali di Bluenet*
- ✓ ***Timbro crittografico*** *codificato insieme alle caratteristiche del documento sotto forma di codice a barre bidimensionale (2D), stampato sul documento stesso*
- ✓ ***Flessibilità ed adattabilità*** *a molteplici applicazioni*
- ✓ ***Conformità AgID****, poiché appositamente progettato per essere utilizzato nel contesto della Pubblica Amministrazione Italiana*

VALIDAZIONE TEMP. EL. CERTIFICATA

Servizio volto a fornire alle Amministrazioni, mediante un Certificatore accreditato, di **associare data e ora, certe e legalmente valide**, a un documento informatico, permettendo una validazione temporale del documento opponibile a terzi.

1. *Integrazione firma elettronica nei processi senza alterare la «user experience»*
2. *Integrazione via API, disponibilità ambienti di test*
3. *Supporto tecnico personalizzato*
4. *Conformità a Eidas e GDPR*



*Il servizio **«Qualified Time Stamping»** di Uanataca permette di certificare la data e l'ora in modo affidabile, garantendo anche l'integrità delle informazioni contenute.*

SERVIZI SPECIALISTICI

Il servizio è volto a fornire all'Amministrazione un **supporto tecnico** connesso all'attivazione dei servizi da remoto oggetto di fornitura e include, a titolo esemplificativo e non esaustivo:

- ***Supporto alla migrazione*** *dei servizi di sicurezza dell'Amministrazione di tipo "on premise" verso i servizi oggetto di fornitura, nelle fasi di analisi e configurazione*
- ***Attività di delivery dei servizi oggetto di fornitura*** *durante le operazioni di migrazione*
- ***Supporto nella definizione, configurazione ed erogazione del servizio di monitoraggio continuo delle vulnerabilità*** *di sicurezza con particolare riferimento all'analisi dei deliverable raccolti a seguito dell'esecuzione da parte del fornitore delle sessioni di vulnerability assessment previsto nel servizio L1.S4*

Il Team di servizio sarà composto dai seguenti Profili Professionali:

SECURITY PRINCIPAL

Definisce, implementa e gestisce progetti dal concepimento iniziale alla consegna finale.
Responsabile dell'ottenimento di **risultati ottimali**, **conformi agli standard di qualità, sicurezza e sostenibilità** nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.

SECURITY SOLUTION ARCHITECT

Progetta, costruisce, esegue test e implementa i sistemi di sicurezza all'interno della rete IT di un'organizzazione. Ha l'obiettivo di **anticipare tutte le potenziali mosse e tattiche** che eventuali criminali possono utilizzare per cercare di ottenere l'accesso non autorizzato al sistema informatico tramite la progettazione di un'architettura di rete sicura.

SENIOR INFORMATION SECURITY CONSULTANT

Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità.
Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni.
Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.

JUNIOR INFORMATION SECURITY CONSULTANT

Contribuisce nell'attuazione della strategia definita all'interno del suo ambito di responsabilità.
Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni.
Attua misure di sicurezza per proteggere le reti e i sistemi informatici di una organizzazione