ASMENET Calabria S.c.a.r.l.

SERVIZIO PER I COMUNI SOCI

Il primo SOC dei Comuni

Centro Operativo di Sicurezza Informatica

Il centro di riferimento per la difesa dei Comuni dagli attacchi informatici ai dati e ai servizi comunali: un team di professionisti IT e una protezione XDR dei computer, gestita da un'unica console centralizzata, per consentire il rispetto dei livelli minimi di sicurezza.

24 ore su 24, 7 giorni su 7 | **Gratuito per i soci** | **Console centralizzata** | **Supporto 8 ore, 5 giorni**

Che cosa fa il SOC

01
Monitoraggio continuo
Controlla i computer degli Enti associati, rilevando in tempo reale gli eventi di sicurezza e intervenendo nel modo più rapido ed efficace.

02
Valutazione delle vulnerabilità
Individua la vulnerabilità di ciascuna risorsa e controlla la vetustà di apparati e software.

03
Relazione mensile
Un report periodico sullo stato di sicurezza delle workstation comunali.

04
Rischio ridotto al minimo
Supporto efficace e facile da usare per ridurre i rischi informatici al livello più basso.
Predisposizione di procedure operative.

Il quadro normativo

Il Comune è titolare di dati, sistemi informativi e servizi digitali esposti a rischi crescenti di incidenti informatici e ha l'esigenza di rafforzare le proprie capacità di prevenzione, rilevazione e risposta, in coerenza con le prescrizioni dettate dalla L. 90/2024 sulla cybersicurezza, dal D.Lgs. 82/2005 (Codice dell'amministrazione digitale) e da tutti i regolamenti e le linee guida emanati dall'ACN (Agenzia per la cybersicurezza nazionale) e dall'AgID (Agenzia per l'Italia digitale).

Asmenet mette a disposizione una potente piattaforma di cybersecurity con la quale è possibile aumentare la sicurezza di tutti i dispositivi e computer degli uffici comunali, proteggendoli dalle minacce quali ransomware, virus, malware, ecc. Grazie all'intelligenza artificiale, inoltre, è progettata per adattarsi alle sfide moderne della sicurezza e proteggere da minacce come phishing e attacchi sofisticati.

In aggiunta a tali regolamenti e linee guida, il recepimento della Direttiva UE «NIS 2» attraverso il D.Lgs. 138/2024 costituisce un riferimento anche per i soggetti non obbligati alle prescrizioni della Direttiva.

1. Governo e gestione della cybersecurity: I Comuni devono adottare misure di gestione e controllo della sicurezza informatica, in linea con le disposizioni stabilite dal «Sistema di prevenzione e difesa cybernazionale». Le PA devono garantire che i loro sistemi informatici siano protetti contro le minacce informatiche.

2. Notifica di incidenti: È previsto l'obbligo per le PA di notificare gli incidenti di sicurezza informatica al «Centro di Valutazione e Certificazione Nazionale» e ad altre autorità competenti. Questa notifica deve avvenire in modo tempestivo e secondo le procedure stabilite.

LA PIATTAFORMA

Protezione XDR dei computer, da un'unica console

Basata sulla tecnologia di piattaforma leader di mercato, con sede nell'Unione Euorpea, gestita dal SOC e visibile in tempo reale sul cruscotto. Può essere gestita centralmente da Asmenet oppure localmente dal Responsabile della Transizione Digitale del Comune. Rafforza la postura rispetto al GDPR (accountability).

Protezione attiva
Antivirus, anti-malware e anti-ransomware; traccia e corregge attivamente le vulnerabilità.

Intelligenza artificiale
Ricerca in modo proattivo le minacce su ogni computer, anche le più sfuggenti.

Ransomware e zero-day
Difesa grazie alla tecnologia di sandboxing basata sul cloud.

Patch automatizzate
Valutazione delle vulnerabilità del software di terze parti, con patch gestite in automatico.

Posta elettronica
Anti-spam, anti-phishing e anti-malware.

Cruscotto
Stato di ogni computer dell'Ente: agenti, infezioni, isolamento e rischio, aggiornati automaticamente.

OPZIONALE

Rilevamento anomalie con IA
Analizza traffico di rete, log di sistema e log dei servizi principali (web server, database, Active Directory o LDAP, Exchange e altri) per alleggerire il lavoro degli analisti e dare supporto immediato al personale del Comune.

Il portale SOC: oltre il monitoraggio

Percorso NIS2 guidato
Scoping, checklist delle misure ed evidenze, con il supporto del team di sicurezza.

Ticketing con SLA
Ticket dal portale con priorità e tempi di risposta garantiti: da 4 ore per le criticità.

Incident response
Triage, contenimento con isolamento del device e post-mortem documentato.

Formazione
Corsi video e dispense sulla sicurezza di base, incidenti e adempimenti NIS2.

Cruscotto sincronizzato ogni 5 minuti · Dati trattati nel Polo Strategico Nazionale

Come funziona

1 Convenzione
Sottoscrizione e invio delle credenziali della piattaforma al responsabile comunale.

2 Installazione
Il programma di protezione viene inviato per l'installazione su tutti i computer.

3 Monitoraggio
Il SOC monitora i computer e gli incidenti; l'Ente segue tutto dal cruscotto.

4 Assistenza e formazione
Ticket con SLA, incident response assistito e corsi di formazione.

ASMENET Calabria S.c.a.r.l.
Via Giorgio Pinna, 29 - Lamezia Terme (CZ)
Tel: +39 0968 412104 - Fax: +39 0968 418792
servizicst@asmecal.it | info@asmenetcalabria.it | asmenetcalabria@asmepec.it
https://asmecal.it/

Certificazioni
9001 · 27001 · 37001