
8.500+
SMART
SCHOOL
SECURITY
SmartSchoolSecurity
CYBER RISK ASSESSMENT
THREAT RESPONSE CENTER
8.500+

La Scuola è il nuovo bersaglio. I dati parlano chiaro.

Nel 2025, le scuole italiane affrontano una media di oltre **8.500 tentativi** di attacco cyber settimanali per singolo istituto (Fonte: Orizzonte Scuola Notizie). Un dato allarmante che impone una seria riflessione a ogni dirigente scolastico e docente.

Questa non è un'emergenza isolata: a livello nazionale, gli attacchi informatici nel settore dell'istruzione sono cresciuti del 37% rispetto al 2023, con l'Italia che supera del 53% la media mondiale (Fonte: Orizzonte Scuola, Securityopenlab).

Questi numeri confermano che gli istituti scolastici sono diventati un bersaglio privilegiato, a causa dell'enorme quantità di dati sensibili di studenti, famiglie e personale che gestiscono.

Minacce come ransomware, phishing e violazioni della privacy non sono più un'eventualità, ma un pericolo quotidiano e concreto che può compromettere la continuità didattica, causare danni reputazionali ingenti e portare a pesanti sanzioni.

Per rispondere a questa sfida, Nikitena ha creato l'iniziativa **"Smart School Security"**, un'offerta flessibile che permette a ogni istituto di adottare le migliori tecnologie di cybersecurity in modo mirato e sostenibile.

Costruisci la tua sicurezza: I pilastri della nostra offerta

La nostra proposta si basa su tre componenti fondamentali che combinati creano un ecosistema di difesa completo e su misura per leesigenze di ogni singolo istituto.

Nikitena S.R.L. - Via Tommaso Campanella, 55 - 88100 Catanzaro (CZ) – ITALY - Tel. 0961557839 – Website: https://nikitena.it/ - Email: info@nikitena.it

Fase 1: Consulenza specialistica e progettazione

Prima di installare qualsiasi tecnologia, è fondamentale capire il contesto. In questa fase preliminare, i nostri esperti di cybersecurity lavorano a stretto contatto con il Dirigente e le figure tecniche di riferimento (DSGA, Animatore Digitale). Insieme, procediamo alla mappatura completa dell'infrastruttura IT (dalla rete ai servizi cloud) e all'analisi delle policy di sicurezza in uso. Identifichiamo le criticità e i dati da proteggere con priorità, consolidando il tutto in un Piano di Sicurezza Personalizzato. Questo approccio strategico assicura un investimento ottimizzato, evitando soluzioni generiche e garantendo che le tecnologie di protezione successive siano perfettamente calibrate sulla Vostra realtà.

Fase 2: ACSIA CRA (Cyber Risk Assessment)

Questa piattaforma agisce come un "radar" esterno che vi dice quali sono i vostri punti deboli prima che un hacker possa trovarli. In pratica, ACSIA CRA si occupa di:

- **Scoprire le "porte aperte" sulla rete:** Analizza dall'esterno il sito web, i server di posta e tutti i servizi online della scuola per identificare le vulnerabilità tecniche e gli errori di configurazione che potrebbero essere sfruttati per un attacco.
- **Verificare le password a rischio:** Controlla costantemente se le email e le password del personale scolastico (docenti, ATA) sono state rubate in passato e sono finite sul Dark Web, prima che possano essere usate per accessi illegali.

Nikitena S.R.L. - Via Tommaso Campanella, 55 - 88100 Catanzaro (CZ) – ITALY - Tel. 0961557839 – Website: https://nikitena.it/ - Email: info@nikitena.it

- **Fornire un punteggio di sicurezza chiaro:** Traduce complesse analisi tecniche in un report comprensibile e in un punteggio di rischio (simile a un voto scolastico) per farvi capire subito il vostro livello di sicurezza e dove è più urgente intervenire.

Fase 3: ACSIA SOS (XDR Plus - Rilevamento e Risposta Esteso)

Se ACSIA CRA è il sistema di allarme, ACSIA SOS è lo scudo attivo che protegge la rete dall'interno. Agisce come un sistema di difesa intelligente per tutti i computer e i server della scuola. Nello specifico, ACSIA SOS permette di:

- **Bloccare le minacce in tempo reale:** Funziona come un antivirus di nuova generazione che non si limita a riconoscere i malware già noti, ma è in grado di bloccare anche i comportamenti sospetti e gli attacchi sconosciuti (zero-day) prima che facciano danni.
- **Reagire in automatico 24 ore su 24:** Se un computer della rete viene infettato, il sistema può isolarlo immediatamente in automatico per evitare che il virus si diffonda al resto della scuola. Questo avviene anche di notte o nei weekend, senza bisogno di un intervento umano.
- **Semplificare la gestione della sicurezza:** Offre una console unica e intuitiva da cui è possibile monitorare lo stato di salute di tutta la rete. Questo riduce i falsi allarmi e permette di avere sempre il pieno controllo della situazione, senza sovraccaricare il personale.

Nikitena S.R.L. - Via Tommaso Campanella, 55 - 88100 Catanzaro (CZ) – ITALY - Tel. 0961557839 – Website: https://nikitena.it/ - Email: info@nikitena.it

Offerta esclusiva per gli Istituti scolastici

La seguente struttura di costi è stata pensata esclusivamente per le esigenze e le capacità di budget del settore scolastico.

SERVIZIO	DESCRIZIONE	TIPOLOGIA DI COSTO	PREZZO (iVA esclusa)
ACSIA CRA	Piattaforma di analisi del rischio esterno	Canone annuale per Istituto	4.000,00€
ACSIA SOS	Piattaforma di protezione proattiva della rete	Canone annuale per dispositivo	75,00€

Contattateci per una dimostrazione **gratuita** e per ricevere un preventivo dettagliato e personalizzato. Un nostro Cyber Analyst sarà a Vostra completa disposizione per analizzare le esigenze del Vostro Istituto e costruire insieme la soluzione di sicurezza più adatta.

Nikitena S.R.L. - Via Tommaso Campanella, 55 - 88100 Catanzaro (CZ) – ITALY - Tel. 0961557839 – Website: https://nikitena.it/ - Email: info@nikitena.it