CSIRT as a Service / CSIRT Rapid Response

Nessuna impresa può considerarsi al riparo dagli incidenti di sicurezza. Per gestire questi eventi è necessario un Cybersecurity Incident Response Team (CSIRT) composto da specialisti, proprio come per estinguere un incendio servono i pompieri.

L'elevata interconnessione e la crescente complessità delle imprese moderne fa aumentare drasticamente le potenziali vulnerabilità – e quindi il rischio di rimanere vittime di un cyberattacco.

Che cos'è CSIRT as a Service/Rapid Response?

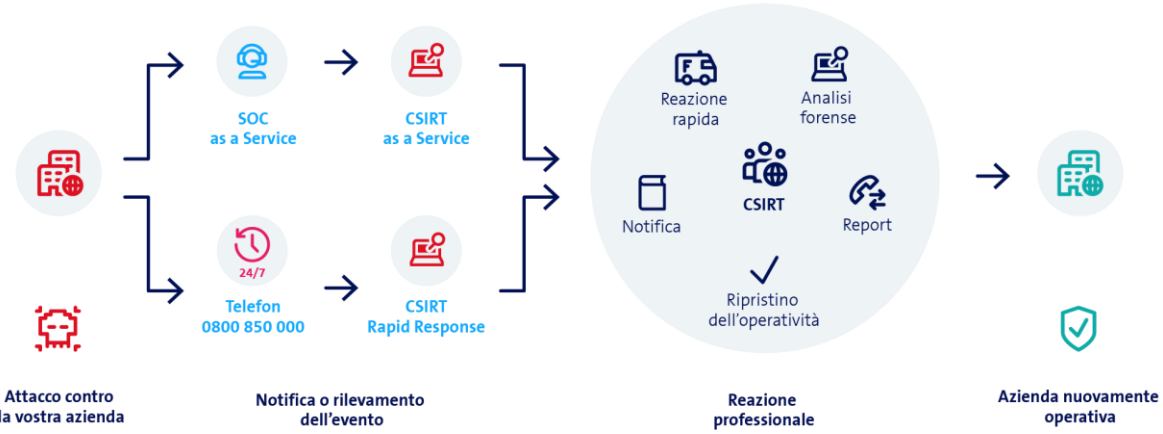
Gli incidenti di sicurezza possono avere un impatto significativo sul business e, purtroppo, non è sempre possibile prevenirli. Ecco perché è decisiva la reazione rapida e professionale di un Cybersecurity Incident Response Team, abbreviato CSIRT.

Prendendo in carico l'incidente di sicurezza verificato, il team aiuta il cliente a reagire all'evento eliminando il software dannoso e ripristinando l'attività operativa. La prestazione di base è disponibile in due versioni.

I vantaggi di CSIRT as a Service/Rapid Response

- **Risposta rapida ai cyberattacchi**
  Reazione veloce e professionale agli incidenti di sicurezza.
- **Specialisti di Security con esperienza e competenza al vostro servizio**
  Specialisti altamente qualificati con una vasta esperienza pluriennale.
- **Verifica dettagliata della sicurezza dei sistemi compromessi**
  Analisi rapida dei vettori d'attacco e isolamento dei sistemi colpiti.
- **Supporto nel ripristino dell'attività regolare**
  Assistenza nel reintegro dei sistemi colpiti nell'ambiente produttivo.

Come funziona CSIRT as a Service / Rapid Response



swisscom

Facts & Figures

Prestazioni di base	CSIRT as a Service con contratto di servizio e SLA: Ricorrete agli specialisti Swisscom nelle fasi di analisi e risposta. Gestiamo il processo di security incident management, in remoto oppure da voi in azienda, e vi assistiamo nelle fasi di raccolta delle prove e comunicazione con clienti e partner.
	CSIRT Rapid Response senza SLA: Rapid Response è equivalente alla prestazione di base di CSIRTaaS. La differenza è che, quando si verifica un incidente, telefonate al numero 0800 850 000 senza alcun contratto di servizio. Tuttavia, il tempo di reazione non è garantito. L'onboarding viene effettuato subito prima dell'intervento, anziché all'inizio della collaborazione come con CSIRT as a Service. Inoltre viene addebitato un forfait per intervento e le tariffe orarie sono maggiori.
Prestazioni opzionali	Report conclusivo personalizzato nei contenuti e nell'aspetto grafico, in tedesco o in inglese.
	Analisi supplementari al di fuori del processo di security incident management (ad es. attribution, ricorso alle vie legali ecc.).
	Verifica preventiva dei sistemi non direttamente colpiti.
	Acquisizione di prove utilizzabili in azioni di diritto penale, civile e pubblico in Svizzera.
	File Analysis Solution (solo per clienti outsourcing), accesso diretto ai file del cliente per analisi approfondite. Senza questa opzione, le direttive aziendali di Swisscom in quanto provider non consentono di accedere direttamente ai file del cliente.
Servizi supplementari	Security Analytics as a Service (SAaaS): Siamo specialisti in fatto di Security e big data e mettiamo a vostra disposizione la nostra affermata infrastruttura per la Security Analytics. Integrate ulteriori fonti di log dal cloud, on premises oppure da un managed provider e ricevete nel dashboard una panoramica dei potenziali incidenti di sicurezza. Analisi e reazione agli incidenti di sicurezza rimangono di vostra competenza.
	SOC as a Service (SOCaaS): Ricevete sul dashboard una panoramica di tutti gli incidenti di sicurezza potenziali e confermati in base alla valutazione di dati di log definiti della vostra azienda nonché analisi con raccomandazioni operative concrete. La reazione agli incidenti di sicurezza critici rimane di vostra competenza.
	Network Detection and Response as a Service (NDRaaS): Integra le funzionalità di rilevamento statiche di SAaaS con una Threat Detection dinamica basata su modelli di machine learning. Il servizio viene fornito insieme a una ditta partner. Offre un valore aggiunto su web (proxy) e rete (DNS, netflow e firewall traffic data), garantendo la massima visibilità.
	Digital Risk Protection as a Service (DRPaaS): Venite informati proattivamente della presenza di informazioni personali e commerciali sensibili della vostra azienda in reti pubbliche e chiuse (ad es. darknet). L'implementazione delle nostre raccomandazioni operative per gli incidenti di sicurezza confermati rimane di vostra competenza.
	Con la loro esperienza, i nostri specialisti ripristinano l'infrastruttura IT come da voi richiesto.

Trovate maggiori informazioni e il contatto con il nostro esperto su **swisscom.ch/csirt**

Swisscom (Svizzera) SA Clienti Commerciali, casella postale,
CH-3050 Berna, Telefono 0800 800 900, www.swisscom.ch/enterprise