Digital Assets REmediation (DARE)

Analisi one-shot o periodica per una bonifica completa dei propri asset digitali dalle minacce di ultima generazione note e non note

PROPOSTA DI PROGETTO

Preparato per:

Gennaio 2017

Il malware oggi in circolazione possono essere facilmente utilizzati per attacchi mirati a persone e società

Caratteristiche principali dei malware attuali

I nuovi malware sono progettati per bypassare i tradizionali sistemi di sicurezza:

- usano tecniche innovative per evitare il rilevamento dei tradizionali antivirus,
- sono basati tipicamente su variant di malware noti,
- fanno leva sulle debolezze delle persone,
- tipicamente rimangono silenti sui target infettati per lungo tempo, aspettando di ricevere le istruzioni dai centri di commando e controllo,
- analizzano il comportamento delle vittime e cercano di infettare altri dispositivi (movimento laterale).

Il servizio Digital Assets REmediation (DARE) permette al cliente di rilevare e bonificare il suo ambiente digitale

DARE analizza computer, server e dispositivi mobili rilevando la presenza di infezioni

Le fasi del servizio DARE

Il servizio DARE è progettato per identificare e rimuovere le sofisticate infezioni dei cyber attacchi mirati, inclusi gli APT (Advanced Persistent Threats), gli zero-day, e I malware (trojans, rootkits e spyware), senza bloccare né modificare l'infrastruttura IT esistente.

Setup dell'ambiente	Analisi delle minacce Cyber	Rimozione e bonifica delle minacce
• Connessione del server DARE alla rete interna del cliente • Configurazione di rete afinché il server possa raggiungere gli endpoint target • Attribuzione dei privilgi di local admin • Aggancio del server DARE alle sorgenti di cyber intelligence	• Scanning degli endpoint raggiungibili • Monitoring passivo del traffico di rete (addizionale) • Scanning degli endpoint di terze parti attraverso l'agente DARE (addizionale) • Rilevamento delle anomalie e delle minacce	• Alerting delle infezioni rilevate • Rimozione dei malware • Bonifica delle minacce • Reporting

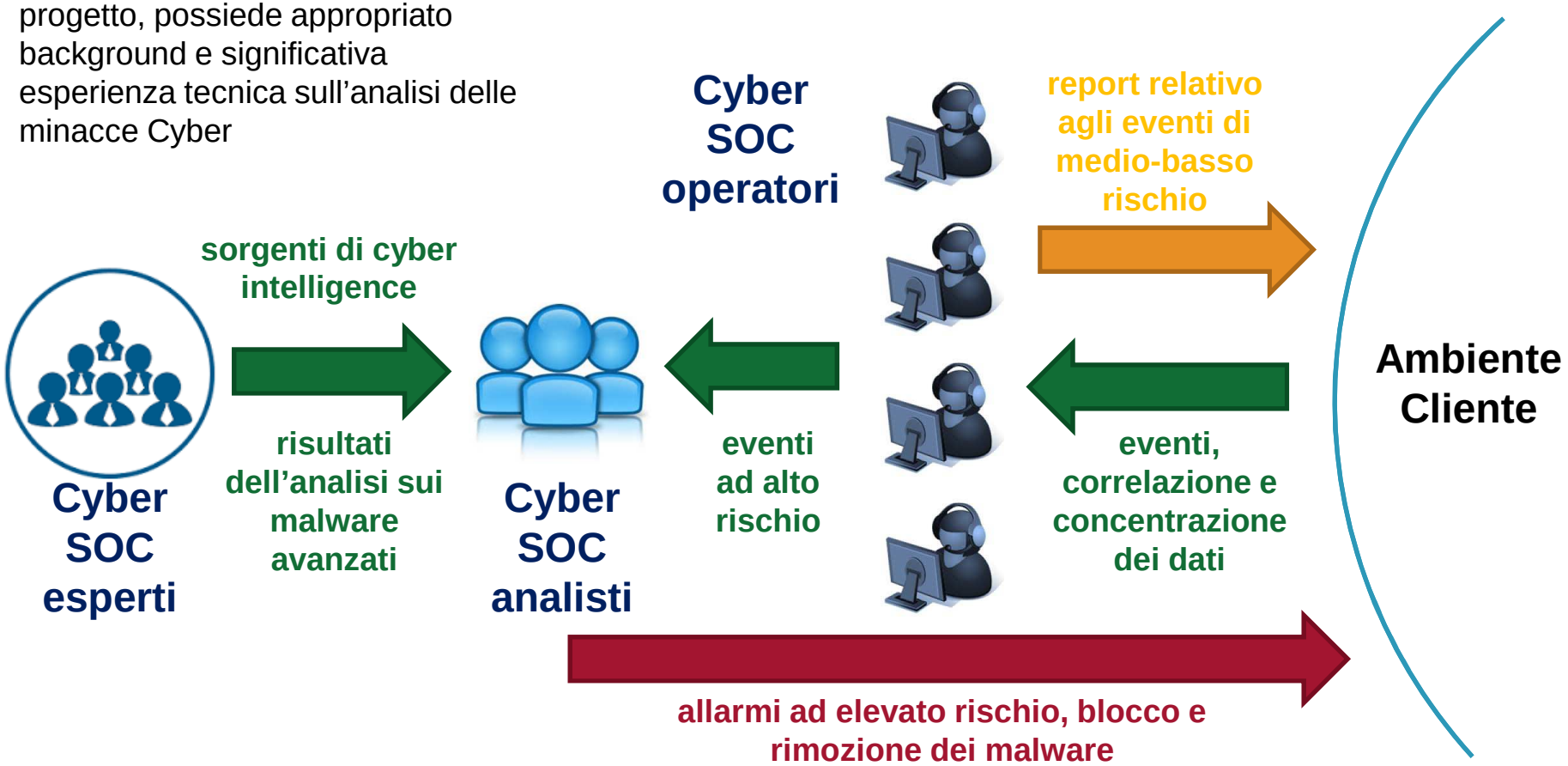
Non è necessario:

- **installare agent**
- **inserire dispositivi di rete**
- **accedere ai dati e alle informazioni del cliente**
- **Interrompere alcun servizio**

Un team riservato ed ampio opera in Xecurity per erogare il servizio DARE

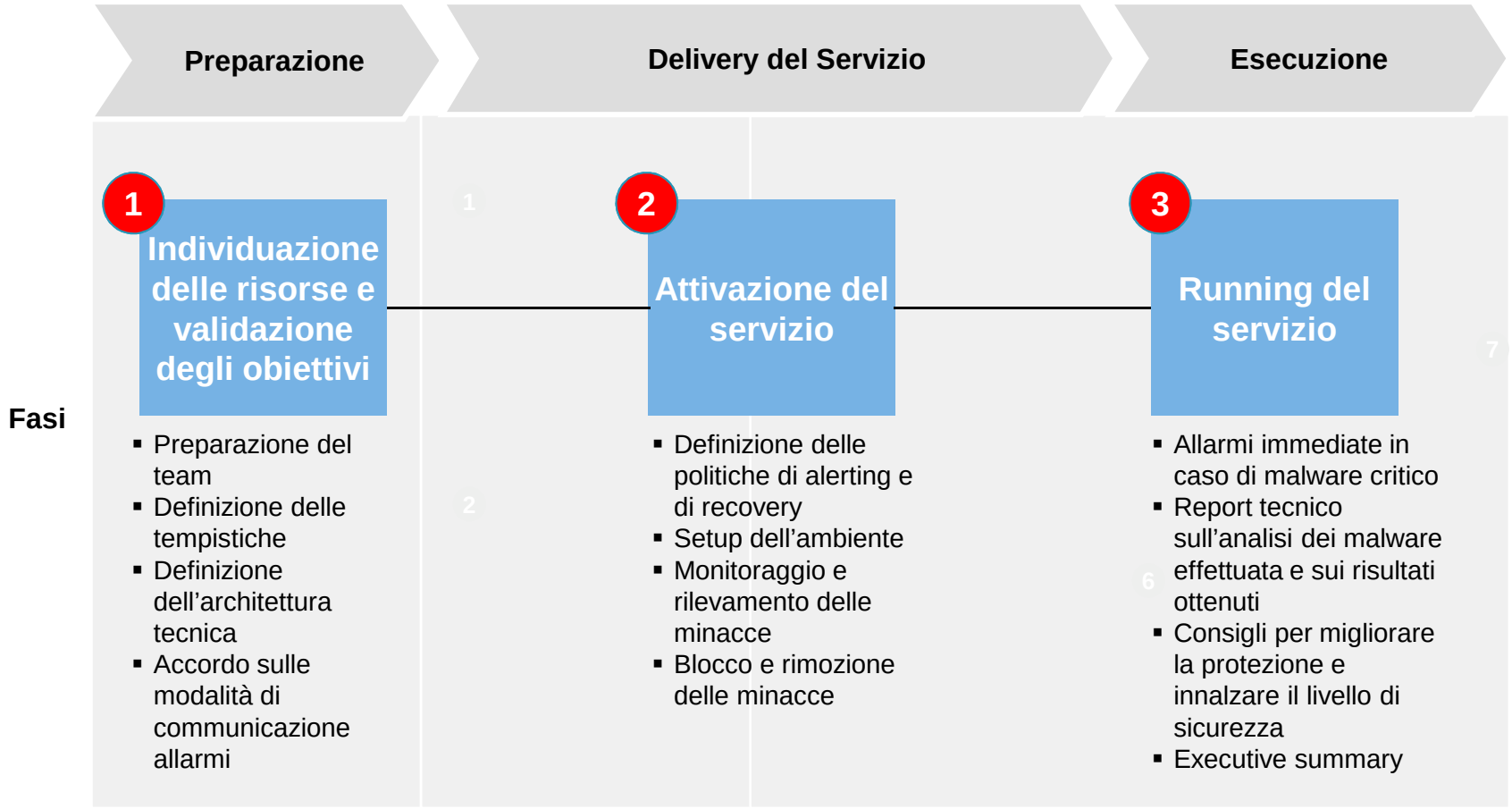
Descrizione dell'organizzazione del servizio DARE

Il team di DARE è dedicato al progetto, possiede appropriato background e significativa esperienza tecnica sull'analisi delle minacce Cyber



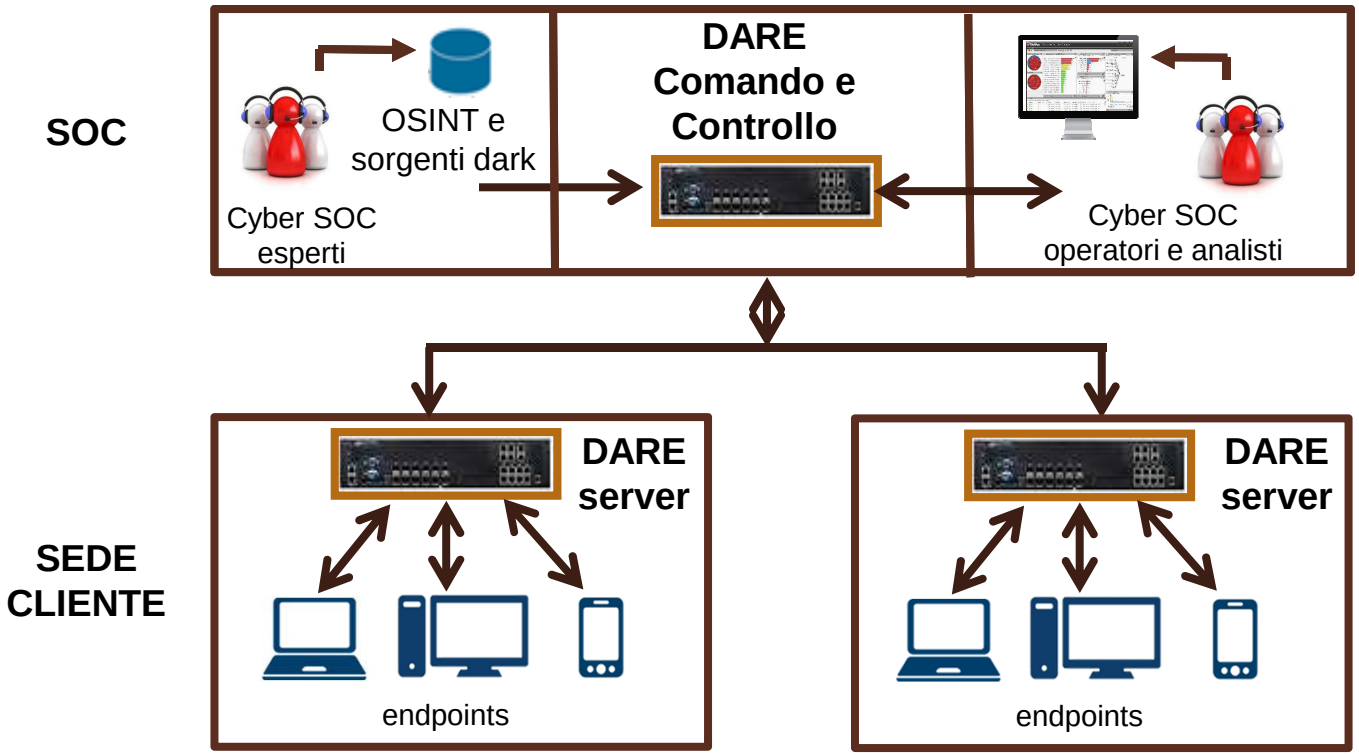
Il servizio DARE può essere erogato completamente seguendo un approccio caratterizzato dalle seguenti 3 fasi

Sviluppo del servizio DARE in una corporate



La piattaforma DARE può essere installata anche stabilmente per assicurare una protezione continuativa

Descrizione dell'architettura on premises del servizio DARE



- La centrale di commando e controllo di DARE può risiedere all'interno del SOC di Xecurity oppure all'interno del SOC del cliente

- Il o i server DARE possono essere installati nella sede o nelle sedi del cliente
- I server DARE collezionano informazioni provenienti dalle scansioni eseguite sugli endpoint e dal monitoraggio passivo effettuato sulla rete


XECURITY