GUIDA

Servizi Managed EDR e XDR di Insight

Sfide aziendali

Nel panorama digitale odierno in rapida evoluzione, le aziende si trovano ad affrontare una serie di problematiche complesse in materia di sicurezza informatica. Il blocco costante delle minacce informatiche rappresenta un rischio significativo per le risorse preziose e i dati sensibili. Man mano che i cybercriminali diventano sempre più intenzionali e innovativi, diventa sempre più difficile per le organizzazioni rilevare e rispondere efficacemente a queste minacce.

Le aziende faticano a rispettare i regolamenti più severi, a complicare gli ambienti IT e a mettere a dura prova la scarsità di personale esperto in sicurezza informatica. Tutto ciò implica la necessità di offrire soluzioni di sicurezza informatica complete e proattive, al fine di difendere le aziende dalle minacce più disparate e sofisticate che si trovano ad affrontare ogni giorno.

La preparazione e la resilienza alla sicurezza informatica sono di fondamentale importanza per tutelare la continuità e il successo di qualsiasi azienda moderna.

In che modo Insight può essere d'aiuto

Il nostro Security Operations Centre (SOC) offre due servizi gestiti, che forniscono capacità avanzate di rilevamento, indagine e risposta alle minacce:

- **Managed Endpoint Detection and Response (MEDR)**
  Adatta a computer portatili, desktop e dispositivi portatili.
- **Rilevamento e risposta estesi gestiti (MXDR)**
  L'unione di log e feed provenienti da una vasta gamma di fonti offre la capacità di rivelazione più efficace per il tuo ambiente.

Grazie alla combinazione di tecnologie quali IA, threat intelligence e analisi, il nostro team di esperti di analisi della protezione è in grado di individuare e rispondere in tempo reale alle minacce presenti nel tuo ambiente.

Forniamo supporto per:

- Monitoraggio completo e rilevamento e risposta alle minacce in tempo reale.
- Risposta più rapida agli incidenti e tempi di inattività ridotti.
- Maggiore visibilità sulle attività degli endpoint e sulle potenziali minacce.
- Disponibilità dei servizi.
- Può favorire la conformità ad alcuni requisiti normativi e standard di settore.
- Può essere abbinato ad altri servizi Insight come parte di un servizio di protezioneb end-to-end.

GUIDA

Servizio Managed Endpoint Detection and Response

Un servizio gestito progettato come soluzione di rilevamento e risposta accessibile e conveniente per le organizzazioni con un programma di sicurezza strutturato limitato o inesistente. Il nostro servizio è progettato in base alle tecnologie leader del settore, partendo dallo stack di protezione Microsoft, e si avvale di Microsoft Defender for Endpoint come fulcro delle sue capacità di rilevamento.

I principali elementi del nostro servizio Managed EDR includono:

- **Monitor endpoint:** Strumenti e tecniche all'avanguardia per monitorare gli endpoint 24/7 alla ricerca di indizi di attività sospette, inclusi attacchi fileless, malware e attacchi informatici, e insider threat.
- **Rilevamento minacce:** Utilizziamo una combinazione di dati di intelligence sulle minacce, analisi del comportamento e algoritmi di machine learning per rilevare le minacce avanzate che potrebbero eludere i tradizionali controlli di sicurezza.
- **Indagine e risposta:** I nostri analisti di sicurezza indagano sugli avvisi e ne attribuiscono la giusta priorità, e inviano report dettagliati sugli incidenti al tuo team. Collaboriamo anche con te per sviluppare ed attuare un piano di risposta che miri a mitigare l'impatto di eventuali incidenti.
- **Protezione Endpoint:** La nostra soluzione EDR include opzioni di protezione endpoint all'avanguardia, che includono antivirus, anti-malware e funzionalità HIPS (Host Intrusion Prevention System), per prevenire e bloccare gli attacchi prima che possano causare danni.
- **Threat hunting:** Funzionalità di threat hunting proattivo, per individuare e indagare sulle potenziali minacce che potrebbero essere sfuggite al rilevamento da parte dei sistemi di automazione.

Servizi Managed Extended Detection and Response

Una capacità di rilevamento più efficace che riunisce tutti i log di protezione e i feed in una piattaforma SIEM centralizzata basata sulla tecnologia Sentinel.

I principali elementi del nostro servizio Managed XDR includono:

- **Monitoraggio:** Utilizzare strumenti e tecniche all'avanguardia per monitorare 24/7 la presenza di indizi di attività sospette, inclusi attacchi fileless, malware e insider threat.
- **Raccolta e analisi dei log:** Acquisizione e analisi centralizzate dei dati di log provenienti da varie fonti, inclusi endpoint, dispositivi di rete, applicazioni e servizi cloud.
- **Rilevamento minacce:** Utilizziamo una combinazione di dati di intelligence sulle minacce, analisi del comportamento e algoritmi di machine learning per rilevare le minacce avanzate che potrebbero eludere i tradizionali controlli di sicurezza.
- **Indagine e risposta:** I nostri analisti di sicurezza indagano sugli avvisi e ne attribuiscono la giusta priorità, e inviano report dettagliati sugli incidenti al tuo team. Collaboriamo anche con te per sviluppare ed attuare un piano di risposta che miri a mitigare l'impatto di eventuali incidenti.
- **Protezione Endpoint:** La nostra soluzione EDR include opzioni di protezione endpoint all'avanguardia, che includono antivirus, anti-malware e funzionalità HIPS (Host Intrusion Prevention System), per prevenire e bloccare gli attacchi prima che possano causare danni.
- **Threat hunting:** Funzionalità di threat hunting proattivo, per individuare e indagare sulle potenziali minacce che potrebbero essere sfuggite al rilevamento da parte dei sistemi di automazione.

I risultati dei nostri servizi Managed EDR/XDR

Ti aiuteremo a:

Rilevare e a rispondere proattivamente alle minacce.	Monitoraggio e assistenza 24 ore su 24, 7 giorni su 7	Ridurre i costi	Conformità alle norme
Prevenire le violazioni della sicurezza e a ridurre al minimo gli impatti dei potenziali attacchi	Protezione continua e risposta rapida agli incidenti	Un'alternativa conveniente alla creazione e al mantenimento di un team interno	Contribuire a soddisfare gli standard di protezione e i requisiti di reporting