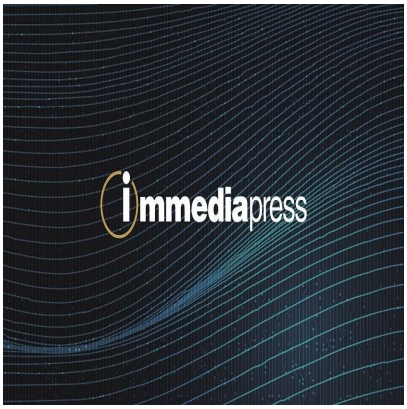

Kaspersky potenzia le funzionalitÃ di rilevamento e risposta di rete con KATA 8.0

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Kaspersky ha annunciato un importante aggiornamento di Kaspersky Anti Targeted Attack 8.0 (KATA 8.0), progettato per aiutare le aziende a migliorare la visibilitÃ sulle proprie reti e a rilevare in modo piÃ¹ tempestivo minacce informatiche sofisticate.

Con la continua espansione della superficie di attacco e la progressiva dissoluzione dei perimetri di rete tradizionali, i team di sicurezza devono affrontare sfide sempre piÃ¹ complesse nel controllo del traffico di rete. KATA 8.0 risponde a queste esigenze introducendo nuove tecnologie di rilevamento, una maggiore osservabilitÃ della rete e unâ??integrazione piÃ¹ stretta con lâ??ecosistema di sicurezza Kaspersky e con soluzioni di terze parti.

Tecnologie di rilevamento avanzate per minacce moderne

KATA 8.0 introduce diverse nuove funzionalitÃ di rilevamento, progettate per migliorare lâ??individuazione delle minacce riducendo allo stesso tempo lâ??affaticamento causato dagli allarmi.

La nuova tecnologia di rilevamento
delle anomalie individua comportamenti sospetti della rete analizzando i protocolli chiave comunemente utilizzati negli attacchi informatici, come DNS, HTTP e Kerberos. Invece di ispezionare lâ??intero traffico di rete, la tecnologia si concentra sulle deviazioni specifiche dei protocolli, tenendo conto dellâ??infrastruttura e dei modelli di utilizzo dellâ??organizzazione. Questo approccio migliora significativamente lâ??accuratezza del rilevamento e contribuisce a ridurre i falsi positivi.

Grazie al rilevamento dello shadow IT, KATA 8.0 consente alle aziende di identificare lâ??utilizzo di servizi pubblici non autorizzati. La soluzione supporta oltre 5.000 servizi esterni, tra cui le principali piattaforme di archiviazione cloud e collaborazione, aiutando i team di sicurezza a migliorare la visibilitÃ della rete e a riacquisire il controllo sui flussi di dati aziendali.

KATA 8.0 introduce inoltre la scansione retrospettiva delle copie del traffico caricate dagli utenti. I team di sicurezza possono ora caricare file PCAP manualmente o automaticamente da altri sistemi di sicurezza e analizzarli utilizzando le piÃ¹ recenti regole di rilevamento e gli aggiornamenti disponibili nei motori anti-malware, sandbox, IDS e in altri motori Kaspersky. Questo consente indagini piÃ¹ approfondite e lâ??individuazione di minacce che potrebbero essere sfuggite al momento dellâ??incidente.

Inoltre, KATA Ã¨ ora in grado di raccogliere tutti i dati osservabili dal traffico di rete, inclusi nomi di file, URL e hash, non solo quelli associati a oggetti dannosi ma anche quelli considerati sicuri. Questo permette agli analisti di individuare utenti potenzialmente compromessi e attivitÃ sospette anche quando gli oggetti appaiono inizialmente puliti, offrendo una prospettiva di sicurezza piÃ¹ ampia e proattiva.

Integrazioni piÃ¹ solide per indagini e risposte piÃ¹ rapide

KATA 8.0 migliora ulteriormente lâ??integrazione con altre soluzioni Kaspersky e con piattaforme esterne, semplificando le indagini e migliorando i tempi di risposta.

Lâ??integrazione con Kaspersky Security for Mail Server (KSMS) consente la scansione dinamica degli allegati e-mail protetti da password nella sandbox KATA, mentre gli avvisi KATA arricchiti includono ora la visibilitÃ completa delle azioni intraprese da KSMS, come il blocco o lâ??eliminazione di contenuti sospetti.

Per le aziende che utilizzano Managed Detection and Response (MDR), KATA 8.0 funge da sensore di rete fornendo telemetria direttamente al cloud MDR. Gli analisti MDR possono richiedere ulteriori informazioni contestuali direttamente a KATA tramite lâ??interfaccia MDR, senza coinvolgere il cliente, accelerando notevolmente le indagini.

La soluzione supporta inoltre lâ??invio automatico di file da Kaspersky Endpoint Security (KES) alla sandbox KATA, consentendo unâ??analisi piÃ¹ approfondita dei file sospetti rilevati sugli endpoint e azioni di risposta piÃ¹ rapide quando i risultati malevoli vengono confermati.

Per rafforzare le capacitÃ di risposta attiva, KATA 8.0 introduce nuovi connettori per Check Point NGFW, permettendo alla soluzione di generare automaticamente regole di blocco basate sulle attivitÃ di rete dannose rilevate e di applicarle a livello di firewall quasi in tempo reale.

Ilya Markelov, Head of Unified Platform Product Line di Kaspersky, ha affermato: Kaspersky Anti Targeted Attack 8.0 Ã¨ stato progettato per offrire un elevato livello di visibilitÃ , consentendo il rilevamento proattivo delle minacce, indagini piÃ¹ approfondite e decisioni di risposta piÃ¹ affidabili grazie ad analisi avanzate e a una stretta integrazione con la protezione degli endpoint, la sicurezza della posta elettronica, MDR e altri prodotti e servizi. Nellâ??ambito della nostra strategia di sviluppo a lungo termine, nelle versioni future prevediamo di trasferire KATA sulla piattaforma Open Single Management Platform (OSMP). Questo permetterÃ unâ??integrazione completa con piÃ¹ soluzioni Kaspersky e componenti di terze parti attraverso una console web unificata, supportando NDR, EDR, SIEM, XDR e altro ancora allâ??interno di un unico ecosistema di sicurezzaâ?•.

Ulteriori informazioni su Kaspersky Anti Targeted Attack, sono disponibili al seguente link.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Febbraio 18, 2026
Autore
redazione