TESORION

Halcyon: Ransomware resilience

Bescherming tegen ransomware tijdens elke fase in de aanvalsketen

Ransomwaregroeperingen slagen vaak in hun opzet om data te gijzelen of te exfiltreren doordat ze in staat zijn om traditionele beveiligingsoplossingen uit te schakelen en back-ups te vernietigen. Zelfs bedrijven met de nieuwste antivirus- en endpointprotectieoplossingen worden nog steeds geraakt. Het garanderen van bedrijfscontinuïteit vereist daarom een proactieve, gelaagde beveiliging.

Halcyon is gespecialiseerd in ransomware resilience. De techniek is specifiek gebouwd om aanvallen in elke fase van de aanvalsketen te verstoren. Van pre-executie tot datadiefstal en encryptie: de technologie grijpt direct in. Het doel is simpel: losgeldbetalingen overbodig maken, downtime minimaliseren en data-exfiltratie voorkomen.

Onze missie

Tesorion zet zich in voor een samenleving waarin digitale veiligheid vanzelfsprekend is. Dat doen wij door organisaties te helpen hun continuiteit te waarborgen.

Veranderend aanvalsoppervlak

De technologie van Halcyon focust uitsluitend op de unieke gedragskenmerken van ransomware; van de eerste inbreuk tot de uiteindelijke encryptiepoging. Dit levert een robuuste, gelaagde beveiliging op tegen gijzeling van data en waarborgt de operationele continuïteit.

Wil je meer weten over deze oplossing, neem dan contact met ons op. Wij helpen je graag verder.

Ransomwarefeiten

- **Aanvallen steeds succesvoller**
  De afgelopen twee jaar is het percentage succesvolle aanvallen met 104% gestegen
- **Hersteltijd neemt toe**
  De gemiddelde hersteltijd voor organisaties na een ransomware-aanval is 22 dagen
- **Organisaties overschatten veiligheid**
  Uit analyse blijkt dat 69% van de slachtoffers dacht goed voorbereid te zijn

Ravenswade 2A, 3439 LD Nieuwegein, Nederland | 088 - 274 78 80 | info@tesorion.nl | www.tesorion.nl

TESORION

Doelgerichte ransomware resilience

Halcyon ransomware resilience vervangt de huidige security-stack niet, maar versterkt deze. De oplossing is gebouwd vanuit een ransomware-first aanpak, waardoor de technologie als een extra, autonome beschermingslaag op de endpoints fungeert.

Daarnaast voedt Halcyon het Tesorion Security Operations Center (T-SOC) continu met gerichte Threat Intelligence zodat onze analisten sneller en effectiever threat hunting en incidentmanagement kunnen uitvoeren bij geavanceerde ransomware-dreigingen.

Blokkeren data-exfiltratie
Beschermt organisaties end-to-end tegen data-exfiltratie, encryptie en afpersing.

24/7 ROC
Ransomware Operations Center voorkomt dat organisaties overspoeld worden met alerts.

Geavanceerd sleutelherstel
Onderschept encryptiesleutels om direct gegevens te ontsleutelen, zelfs zonder backups.

Controle en inzicht met Halcyon ransomware resilience

- **EDR Tamper beveiliging**
  Bewaakt proactief de bestaande security stack en voorkomt uitschakeling door aanvallers.
- **Gespecialiseerde AI & Gedragsdetectie**
  Gebruik van detectiemodellen die exclusief zijn getraind op actuele ransomware TTP's (Tactics, Techniques and Procedures) en praktijkervaringen uit incidentmanagement.
- **Herstellen versleutelde bestanden**
  Onderschept tijdens een ransomware-aanval de encryptiesleutel, waardoor organisaties hun versleutelde bestanden binnen enkele uren kunnen herstellen zonder losgeld te betalen of afhankelijk te zijn van back-ups.
- **BYOVD (Bring Your Own Vulnerable Driver) - detectie**
  Voorkomt het misbruik van kwetsbare maar legitieme drivers door BYOVD-aanvallen te blokkeren voordat aanvallers kernel-toegang kunnen misbruiken.