|  |  |  |
| --- | --- | --- |
| **ID REQ** | **Taula de requeriments de seguretat** | **SI** |
|  | **Tècnics i operatius** |  |
| **REQ001** | Detecció i bloqueig d'atacs a nivell Web i Infraestructura |  |
| **REQ002** | Bloqueig de connexions d'entrada i de sortida cap a IPs potencialment malicioses |  |
| **REQ003** | Bloqueig de comunicacions que continguin un fitxer maliciós en base al seu Hash |  |
| **REQ004** | Realització de captures de trànsit (PCAP) en cas d'atac, estigui o no bloquejat, i visualització del contingut de les comunicacions etiquetades com a malicioses |  |
| **REQ005** | Identificació i filtrat de tràfic a nivell d’aplicació |  |
| **REQ006** | Implementació de firmes manualment (Snort) per la detecció i bloquejat d'atacs |  |
| **REQ007** | Cerca d'atacs a partir d'origens i destins, visualització de tota la informació dels atacs (si està bloquejat o no) i extracció de la informació en format CSV |  |
| **REQ008** | Recepció d'actualitzacions de firmes per la mitigació d'atacs per part del fabricant en breu interval de temps des de que es descobreix la vulnerabilitat |  |
| **REQ009** | Integració amb eines d'anàlisi de vulnerabilitats de tercers |  |
| **REQ010** | Protecció en front atacs de DDoS |  |
| **REQ011** | Interpretació i generació de IOC’s en el format STIX/TAXII del MITRE |  |
| **REQ012** | Capacitat per monitorar i filtrar el trànsit de xarxa en temps real |  |
| **REQ013** | Proporcionar una visibilitat clara i determinista dels esdeveniments de seguretat en una única consola central |  |
| **REQ014** | Captura, emmagatzematge i extracció d’evidències de trànsit il·lícit vàlid en cas d’estar relacionat amb un procés judicial |  |
| **REQ015** | Realització de whitelists des de les màquines d'anàlisis per no bloquejar atacs legítims que es realitzen des d'aquestes |  |
| **REQ016** | Realització de llistats de blacklist per categories com aplicacions, usuaris, urls,etc. |  |
| **REQ017** | Configuració de regles de permís d'accés o bloqueig personalitzades per xarxa/subreu |  |
| **REQ018** | Capacitat de creació d'interfícies de xarxa per VPN (tenir la possibilitat a futur, no es demana que estigui operativa). |  |
| **REQ019** | L'acompliment de l'eina ha de ser mínimament degradat amb l'activació de totes les funcions de seguretat incloses. |  |
| **REQ020** | Configuració d' interfícies que permeti organitzar xarxes i subxarxes |  |
| **REQ021** | Ha de comptar amb Machine Learning avançat o similar per augmentar la detecció i prevenció de malware |  |
| **REQ022** | App and URL filltering avançat que proporcioni configuració d'alertes i respostes a elles en viu. |  |
| **REQ023** | Reducció avançada en local i en general de Falsos positius |  |
| **REQ024** | Cobertura de seguretat avançada per a DNS entre les característiques de la pròpia solució. |  |
| **REQ052** | Capacitat Sandbox |  |
| **REQ053** | Capacitat de configuració de Proxy explícit per Interface, amb la funcionalitat de Proxy chaining en cas necessari, a més de capacitat de caching. |  |
| **REQ054** | Inspeccionar tràfic encriptat |  |
| **ID REQ** | **Descripció del requeriment** | **Compleix** |
|  | Arquitectura |  |
| **REQ025** | La solució proposada ha de donar resposta a un arquitectura de xarxa redundada. |  |
| **REQ026** | La solució proposada ha de connectar-se a la xarxa sense produir cap tipus d’afectació del trànsit lícit, o afegir endarreriment que pugui afectar l’eficiència de la xarxa principalment d’entorns de sensibles. |  |
| **REQ027** | La solució ha de ser escalable per a tenir capacitat per monitorar a totes les velocitats suportades per la topologia existent. |  |
|  | **Fonts d'Informació/Integració** |  |
| **REQ028** | Integració dels logs de seguretat amb un SIEM i Data Lake. |  |
| **REQ029** | Integració amb un posible SOAR |  |
| **REQ030** | Integració amb Active Directory o proveïdor de identitats. |  |
| **REQ031** | Integració amb mitjans físics o virtuals amb sandbox o sandbox integrat en la pròpia solució. |  |
| **REQ032** | Integració amb CASB de nova generació |  |
|  | **Reports i Dashboards** |  |
| **REQ033** | Visualització del top d'IPs d'atacants |  |
| **REQ034** | Visualització del top d'atacs |  |
| **REQ035** | Visualització del top d'aplicacions i protocols que reben peticions |  |
| **REQ036** | Visualització del top destins |  |
| **REQ037** | Visualització del top del malware detectat |  |
| **REQ038** | Monitoratge Healthy del sistemes: ús de CPU, memòria, xarxa i estat de les interfícies |  |
| **REQ039** | Monitoratge Healthy del sistemes: logs d'auditoria i els canvis realitzats per altres usuaris |  |
| **REQ040** | Monitoratge Healthy del sistemes: connexions/atacs detectats |  |
| **REQ041** | Extracció de reports d'acord amb cerques realitzades dins l'apartat de casos d'ús |  |
| **REQ042** | Realització d' informes personalitzats en períodes de temps i en diferents categories de tràfic i interfícies |  |
| **REQ043** | Visualització de la data de caducitat dels certificats SSL que s'instal·lin |  |
|  | **Disponibilitat** |  |
| **REQ044** | La solució proposada ha de funcionar en mode d’alta disponibilitat, modes Actiu/Actiu i Actiu/Passiu. |  |
| **REQ045** | Disposar d’interfícies amb suport de bypass en front qualsevol fallida de l’equip, configurables en format “fail-open”, “fail-close”. |  |
| **REQ046** | Els elements han de contemplar mecanismes de control de falla. |  |
| **REQ047** | La solució ha d’assegurar La continuïtat de l’operació mitjançant proves automàtiques que permetin determinar que s’està treballant dins dels límits de funcionament especificats. |  |
| **REQ048** | L’actualització de La solució en cas que sigui necessari s’ha de poder realitzar sense produir cap tipus de tall de servei o impacto mínimo. |  |
| **ID REQ** | **Descripció del requeriment** | **Compleix** |
|  | **Disponibilitat** |  |
| **REQ049** | La solució ha de poder generar recolzament de La configuració aplicada per a una ràpida recuperació en cas de falla. |  |
| **REQ050** | La solució ha de proporcionar redundància en l’emmagatzemament de les dades considerades com a essencials o crítiques per l’Operació. |  |
| **REQ051** | La solució ha de tenir capacitat per a una configuració jeràrquica a nivell de nodes o similar que permeti segmentar entorns de negoci, actius de xarxa o d’aplicació a protegir (VIDS/VIPS/VWAF,etc.). |  |