FITSEC CTI
CYBER THREAT INTELLIGENCE

USEILLA FORMAATEILLA:

- VECTRA NDR
- PALOALTO
- MISP
- TAXII
- STIX
- CSV
- OPEN IOC
- FORTIGATE
- MICROSOFT E5

80 % APC-IOC:STAMME
(HYÖKKÄYKSEN TUNNISTEET) OVAT AINUTLAATUISIA, EIVÄTKÄ LÖYDY KILPAILIJOILTA

ENNAKOIVASTI HAVAITSE UHAT, JOTKA KOHDISTUVAT OMAISUUTEESI

KILPAILUEDUT

HELPPO KÄYTTÖÖNOTTO:

FITSEC TOIMITTAA DATAN ASIAKKAAN TARVITSEMASSA TAI HALUAMASSA MUODOSSA ILMAN LISÄKUSTANNUKSIA

MIKSI FITSECIN SYÖTE ON PAREMPI KUIN KILPAILIJOIDEN?

Kilpailevia tuotteita käytettäessä asiakkaan on nähtävä paljon vaivaa integroidakseen data omiin järjestelmiinsä.
Fitsec toimittaa datan oikeassa muodossa vaivattomasti

KAIKKI YHDESSÄ -RATKAISU:

ASIAKKAAN EI TARVITSE PÄÄTTÄÄ, MITÄ UHKIEN OSA-ALUETTA HÄN HALUAA KATTAA - ME TARJOAMME KAIKEN

- APT
- DDOS
- SINKHOLE
- SANDBOX
- APT PLATFORM

Fitsecin ratkaisu sisältää eksklusiivisen APT-alustan, jossa APT-toimijat ja niiden toimintatavat näkyvät visuaalisesti ilman lisäkustannuksia

MIKSI FITSECIN SYÖTE ON PAREMPI KUIN KILPAILIJOIDEN?

MERKITTÄVÄ OSA DATASTAMME ON FITSECIN ASIANTUNTIJOIDEN JATKUVAN TUTKIMUSTYÖN TULOSTA. CTI:TÄ ON TUOTETTU YLI 13 VUODEN AJAN

WHY IS FITSEC'S FEED BETTER THAN COMPETITORS'?

Kilpailijat tuottavat datansa pääasiassa automaation avulla, **me tuotamme sen oman tutkimustyömme tuloksena**

VAHVA PAINOTUS APT-HAITTAOHJELMIIN

Kohdennetut hyökkäykset (APT) ovat vaarallisimpia, ja Fitsecin data painottaa vahvasti niitä sekä suojautumista niitä vastaan

MONIPUOLISET KÄYTTÖKOHTEET JA HYÖDYT

UHKATUNNISTUS / ENNALTAEHKÄISY

HAITTAOHJELMIEN TUNNISTUS
HAITTAOHJELMIEN HAVAITSEMINEN JA TORJUNTA

VERKKOLIIKENTEEN VALVONTA
HAITALLISEN VERKKOLIIKENTEEN TUNNISTAMINEN

SÄHKÖPOSTIN PHISHING-SUODATUS
SUOJAUTUMINEN TIETOJENKALASTELUHYÖKKÄYKSILTÄ

DDOS-HYÖKKÄYSTRENDIT
DDOS-HYÖKKÄYSTEN YMMÄRTÄMINEN JA TORJUNTA

PHISHING-YRITYSTEN TUNNISTAMINEN
TYÖKALUT JA KOULUTUS TIETOJENKALASTELUN TUNNISTAMISEEN

TIETOTURVA-AUTOMAATIO JA VALVONTA

TIETOTURVAPROSESSIEN AUTOMATISOINTI
MANUAALISEN TYÖN VÄHENTÄMINEN TIETOTURVATYÖNKULUISSA AUTOMAATION AVULLA

VERKKOLIIKENTEEN VALVONTA
VERKKOTOIMINNAN TARKKAILU POIKKEAMIEN JA UHKIEN HAVAITSEMISEKSI

TIETOTURVATAPAHTUMIEN ANALYSOINTI JA RAPORTOINTI
TARJOAA NÄKEMYKSIÄ TAPAHTUMISTA NOPEAMMAN REAGOINNIN TUEKSI

LAITETURVALLISUUDEN PARANTAMINEN
TOIMENPITEIDEN TOTEUTTAMINEN LAITTEIDEN SUOJAAMISEKSI JA KÄYTTÄJIEN KOULUTTAMISEKSI

INFRASTRUKTUURIN JA DATAN SUOJAUS

KRIITTISEN INFRASTRUKTUURIN SUOJAAMINEN
KESKEISTEN JÄRJESTELMIEN JA PALVELUIDEN TURVAAMINEN KYBERHYÖKKÄYKSILTÄ

TIETOVUOTOJEN ESTÄMINEN (DLP)
VARMISTAMME, ETTEI DATA KATOA, TULE VÄÄRINKÄYTETYKSI/PÄÄDY LUVATTOMILLE KÄYTTÄJILLE

VERKKOSIVUSTOJEN SUOJAAMINEN
VERKKOSIVUJEN SUOJAAMINEN HAAVOITTUVUUKSILTA JA LUVATTOMALTA KÄYTÖLTÄ

PILVIPALVELUIDEN SUOJAAMINEN
PILVIPOHJAISTEN SOVELLUSTEN JA PALVELUIDEN TIETOTURVAN VAHVISTAMINEN

INTEGRAATIO / MONIPUOLISUUS

INTEGROINTI TIETOTURVAJÄRJESTELMIIN
TYÖKALUJEN, KUTEN PALOMUURIEN JA VIRUSTORJUNNAN, YHDISTÄMINEN VAHVEMMAN SUOJAUKSEN JA AUTOMAATTISTEN VASTEIDEN MAHDOLLISTAMISEKSI

MONIPUOLISET KÄYTTÖKOHTEET JA HYÖDYT
MUKAUTUMINEN ERI YMPÄRISTÖIHIN (PILVI, IOT, INFRASTRUKTUURI) TIETOTURVA- JA VAATIMUSTENMUKAISUUSTARPEIDEN TÄYTTÄMISEKSI

100 % SUOMALAISTA TYÖTÄ

PITKÄKESTOINEN KEHITTYNYT UHKA

MINIMOI VAHINGOT ESTÄMÄLLÄ APT-HYÖKKÄYS VARHAISESSA VAIHEESSA

ASIANTUNTIJATIIMIMME ANALYSOI APT-RYHMIEN TOIMINTAA MANUAALISESTI ERI LÄHTEISTÄ JA LUOKITTELEE DATAN ERI INDIKAATTORIKATEGORIOIHIN

KUN UUSIA INDIKAATTOREITA LISÄTÄÄN NE VÄLITETÄÄN AUTOMAATTISESTI JÄRJESTELMÄÄSI

IOCS

- TIETOMURROT
- TALOUDELLISET TAPPIOT
- KYBERVAKOILU
- POLIITTINEN MANIPULOINTI
- TOIMINNAN HÄIRIINTYMINEN
- KANSALLISEN TURVALLISUUS

...JA PALJON MUUTA...

APT-ALUSTA

SELAINPOHJAINEN PALVELU APT-TOIMIJOIDEN JA KAMPANJOIDEN VISUAALISEEN SEURANTAAN MAAILMANLAAJUISESTI

TUNNISTA INDIKAATTORIEN VÄLISET YHTEYDET JA NOPEUTA REAGOINTIA VISUALISOIMALLA NIIHIN LIITTYVÄT TYÖKALUT, TAKTIIKAT JA TOIMINTATAVAT

HYÖKKÄYSKAMPANJAT ↔ TAPAUKSET

APT-TOIMIJAT ON ORGANISOITU RYHMIIN SEKÄ TARKEMPIIN TAPAUKSIIN JA HYÖKKÄYSKAMPANJOIHIN

KÄYTTÄJÄT VOIVAT SAADA SÄHKÖPOSTI-ILMOITUKSIA TAPAUSPÄIVITYKSISTÄ TAI UUSIEN TAPAUSTEN LISÄÄMISESTÄ ALUSTALLE

TAPAUSSIVUT SISÄLTÄVÄT TYÖKALUT, TEKNIIKAT, KOHTEET JA INDIKAATTORIT

KÄYTTÄJÄT VOIVAT HAKEA LISÄTIETOA UHKATOIMIJOISTA SEKÄ NIIDEN KOHTEISTA, TYÖKALUISTA JA TEKNIIKOISTA

DDOS

(hajautettu palvelunestohyökkäys)

Pitää sinut ajan tasalla uusimmista palvelunestohyökkäyksistä

Kuka hyötyy DDOS-feedistä?

- Operaattorit, jotka valvovat verkkojensa tietoturvatilannetta

DDOS-datasyöte sisältää haitalliset ohjauskomennot sekä hyökkäyksen alkuperän reaaliajassa

DDOS-syöte indikaattorit

Aikaleima
alkuperäinen komento
kohdeosoite
lähdeosoite

HYÖDYT

- Reaaliaikainen uhkatietoisuus
- Haitallisten komentojen tunnistus
- Seuraa iskun alkuperää
- Estä liikenne C2-serverille
- Tunnista saastuneet laitteet

CSV

DDoS-syöte on saatavilla helposti käsiteltävässä CSV-muodossa ja integroitavissa useisiin eri järjestelmiin

SANDBOXIOC

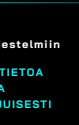
Tunnista saastuneet järjestelmät IOC:ien avulla

Tarjoaa tietoa eri haittaohjelmista ja niiden C2-palvelimista

HYÖTY

Estä liikenne haitallisiin osoitteisiin

SANDBOXIOC INDIKAATTORIT



CSV

SandboxIOC-syöte on saatavilla helposti käsiteltävässä CSV-muodossa ja integroitavissa useisiin eri järjestelmiin

SINKHOLEIOC

Näkyvyys internetissä havaittuihin saastuneisiin järjestelmiin

SINKHOLE-SYÖTE TARJOAA HYÖDYNNETTÄVÄÄ TIETOA SADOISTA TUHANSISTA SAASTUNEISTA JA HAITALLISISTA JÄRJESTELMISTÄ MAAILMANLAAJUISESTI

Kenen tulisi käyttää SinkholeIOC-syötettä?

- Operaattorit
- Viranomaiset

CSV

SinkholeIOC-syöte on saatavilla helposti käsiteltävässä CSV-muodossa ja integroitavissa useisiin eri järjestelmiin

Hyöty

Sinkhole-syötteen avulla voit paikantaa saastuneet laitteet ja estää verkon laitteita kommunikoimasta haitallisiin osoitteisiin

Keskimäärin löydämme päivittäin 700 000 saastunutta IP-osoitetta