OptiCom
IT RISINĀJUMI JŪSU BIZNESAM

OT SISTĒMU DROŠĪBAS PĀRBAUDE

Vēsturiski OT (Operational Technology) sistēmas ir bijušas izolētas, tāpēc to izstrādes procesā nav paredzēta komunikācijas drošība un noturība pret ievainojamībām. Mūsdienās OT sistēmas tiek arvien vairāk pievienotas interneta tīklam, kas atver tāda paša veida ievainojamības kā IT sistēmās.

OT drošības draudi:

Iekārtu operētājsistēmu neatjaunināšana
Windows XP ir vairāk ievainojamību kā caurumu Šveices sieram

Nepārredzams tīkls
Nav informācijas par to, kas notiek OT tīklā

Cilvēciskā faktora kļūdas
Atnesta no mājām *flash*-atmiņa var apturēt uzņēmuma darbību

Ir iespēja pieslēgties OT sistēmām attālināti
Ja Jūs varat pieslēgties attālināti, kāpēc lai to nevarētu citi?

No IT tīkla neatdalīts vai nepareizi izolēts OT tīkls
Jebkurš IT drauds ir OT drauds

Vai Jums ir IT sadarbības partneris, kas spēj palīdzēt OT drošības incidenta gadījumā?

OptiCom OT sistēmu drošības pārbaudē ietilpst:

- **Esošās iekārtu vai industriālās tehnoloģijas pieejas kontroles sistēmas novērtēšana**
- **Iekārtu inventarizācija atkarībā no OT komunikācijas protokola**
- **Industriālā tīkla loģiskās topoloģijas noteikšana (shēmas izstrāde)**
- **IT un industriālo tīklu saskares punktu noteikšana**
- **Ārējās piekļuves pie OT esamības un pieslēgšanās iespēju pārbaude**

Rezultātā saņemsiet:

- **Atskaiti par ievainojamību klātbūtni industriālajā tīklā**
- **Industriālā tīkla loģisko shēmu**
- **Atrasto ievainojamību novēršanas un darbības optimizācijas rekomendācijas**

OptiCom
IT RISINĀJUMI JŪSU BIZNESAM

OptiCom sertificētie IT speciālisti nodrošina OT sistēmu drošības pārbaudes ieviešanu sadarbībā ar pasaules vadošajiem ražotājiem

CLAROTY

Check Point SOFTWARE TECHNOLOGIES LTD.

Claroty risinājumi dod iespēju klientiem izmantot esošo IT drošības infrastruktūru, integrējot ar Check Point ugunsmūri, lai aizsargātu savus OT aktīvus un tīklus. Claroty platforma ir pilnībā integrēts risinājums, kas tiek pievienots OT tīklam, neizmantojot aģentus.

- Nodrošina reāllaika izpratni par tīkla trafiku un dziļu redzamību ICS (Industrial Control Systems) tīklos
- Palīdz aizsargāt iekārtas, kuras nav iespējams atjaunināt, izmantojot Virtual Patching funkciju
- Ātri un viegli ieviešams, nav ietekmes uz tīklu, neietekmē rūpniecisko procesu integritāti

NOZOMI NETWORKS

FORTINET

Nozomi Networks ir OT un IoT drošības un pārredzamības līderis. Kopš 2013. gada uzņēmums ir veicinājis mašīnmācīšanās un mākslīgā intelekta (AI) izmantošanu, kas nodrošina kritiskās infrastruktūras darbību un drošību.

- Lieliski integrējams un savienojams ar Fortigate ugunsmūriem
- Nodrošina vienu risinājumu ar reāllaika ICS uzraudzību, hibrīdu draudu noteikšanu un procesu anomāliju noteikšanu
- Veic rūpnieciskā tīkla vizualizāciju, aktīvu uzskaiti un ievainojamības novērtēšanu

txOne networks

TREND MICRO

TXOne Networks ir uzņēmums, ko izveidoja Trend Micro un Moxa. TXOne piedāvā kiberdrošības risinājumus, lai aizsargātu Jūsu rūpnieciskās vadības sistēmas un nodrošinātu tās pret kiberuzbrukumiem, kas vērsti pret OT tīklu. Piedāvā risinājumus, lai novērstu drošības vājās vietas, kas izplatītas rūpnieciskajā vidē.

- TXOne Networks produktu portfolio piedāvā gan tīkla, gan galapunktu aizsardzības produktus
- Mērķis ir ne tikai palielināt ICS aizsardzību, bet arī uzturēt biznesa nepārtrauktību
- Dod iespēju bloķēt nevēlamu OT tīkla trafiku, pirms tas ietekmē iekārtu darbību

Drošības pārbaudes izpildes termiņš 2-4 nedēļas

Industrijas, kurās tiek piedāvāta OT sistēmu drošības pārbaude

Enerģētika | Transports | Medicīna | Rūpniecība | Siltumapgāde | Ūdensapgāde

Pieteikties konsultācijai un sīkākas informācijas saņemšanai

sales@opticom.lv
+371 67331878