

Riigivõrgu turvarikete hajutatud jälgimissüsteem S4A

Kliendi vajadus

Eesti riigivõrgus asetleidvate turvaintsidentide käsitlemisel abistab kohalikke administraatoreid CERT-EE, kes puutub kokku mitmete probleemidega.

– Mõnede riigivõrgu osade haldajatele on tegeliku turvarikke põhjustaja tuvastamine töömahukas.

– Tulemüüri taga asuvates kohalikes võrkudes toimuvate turvaintsidentide kohta on keeruline saada täpsemat infot.

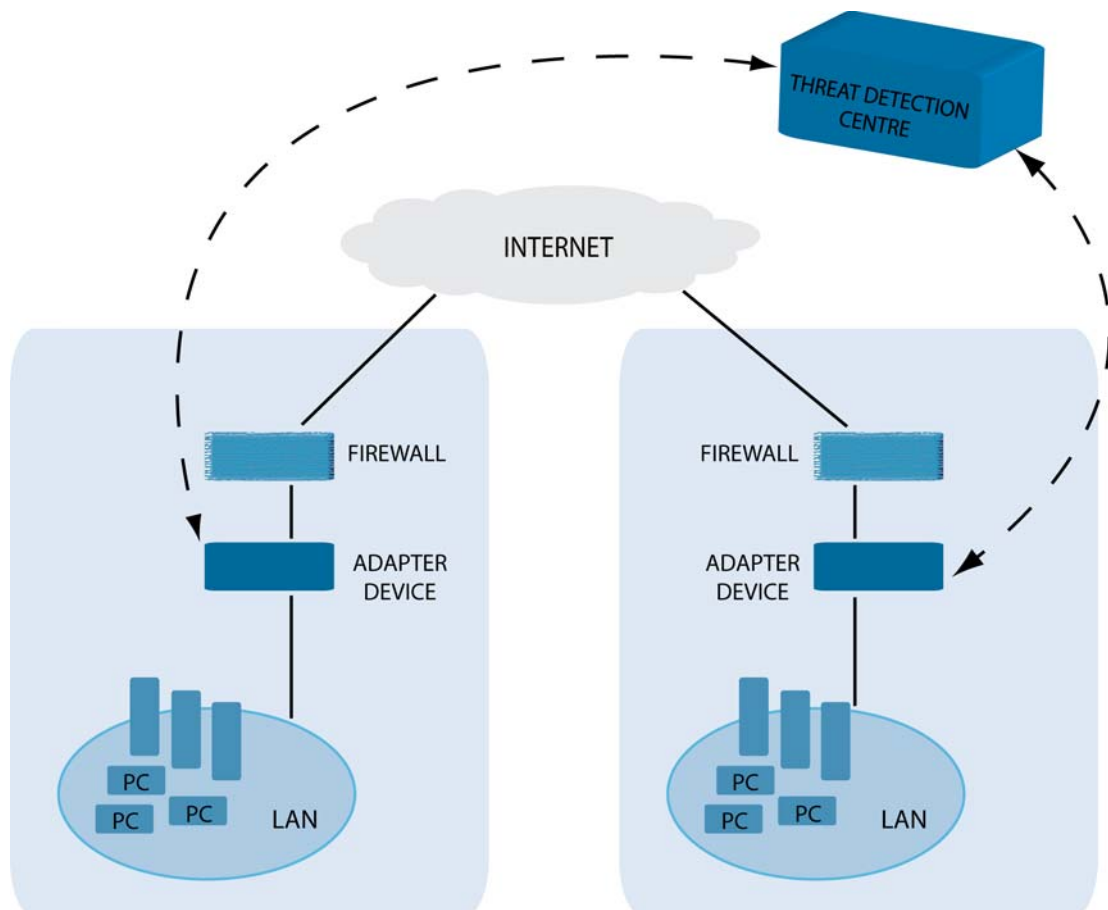
Vaja on abivahendit, mis aitaks lokaalvõrkude administraatoritel rikkeid tuvastada ning CERT-EE'le rikete statistikat edastada samal ajal kohtvõrgu topoloogiat avalikustamata.

Jälgimissüsteemi kirjeldus

S4A on võrguliikluse analüsaatori ja ründeprofiilide baasil töötav avatud lähtekoodiga tarkvara OpenBSD platvormile, mis koosneb tuvastajast, keskusest, sertkeskusest ja reeglite haldamise tarkvarast. Tarkvara võimaldab koguda keskselt statistikat võrguaadresside transleerimist (NAT) kasutatavates sisevõrkudes esinevate turvarikete kohta, samas nende võrkude ehitust statistiku eest salajasse jättes.

CERT-EE'le annab S4A ülevaatliku pildi Eesti riigivõrgus aset leidvatest turvariketest.

Kohaliku võrgu administraatorile annab S4A detailse pildi kohtvõrgus aset leidvatest turvariketest ning lihtsustab rikete lähtekoha leidmist tunduvalt.



Joonis 1. S4A jälgimissüsteemi arhitektuur

Tehnoloogiad

IDS, perl, php, Javascript, OpenBSD