Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Vilniaus universitetas

SISTEMINIŲ ŽURNALŲ TERMINUOTO SAUGOJIMO PASLAUGA

Paslaugos aprašymas

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą „Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra“ Nr. 09.3.3-ESFA-V-711-01-0003

Kuriame Lietuvos ateitį

2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Vilnius

2018

Turinys

Įvadas

Vienas pagrindinių pažeidimų tyrimo ir išaiškinimo būdų, tiriant kompiuterių tinkle ar sistemose kilusius incidentus - tinkle veikiančios įrangos sisteminių žurnalų (angl. logs) duomenų analizė. Sisteminių žurnalų analizė suteikia galimybes operatyviai spręsti incidentus, atlikti retrospektyvinius saugumo pažeidimų tyrimus, nustatyti grėsmės vektorius ir vykdyti prevenciją. Tam būtina tinkamai ir saugiai kaupti sisteminių žurnalų informaciją ir ją saugoti atskirai nuo pačios įrangos. Be to, reakcijos į incidentus laikui sumažinti būtina kuo labiau automatizuoti grėsmių paieškos sisteminių žurnalų įrašuose procesus.

Paslaugos tikslai

Lietuvos mokslo ir studijų institucijų kompiuterių tinkle (toliau – LITNET) per metus užfiksuoajama tūkstančiai incidentų [1], apie kuriuos dažniausiai praneša trečiosios šalys, t. y. piktybinė veikla dažnu atveju nustatoma po sistemos sukompromitavimo. Kibernetinių atakų įvykdoma daugiau ir sudėtingesnių [2], o įrenginių skaičius kompiuterių tinkle didėja. Norint greičiau aptikti kenkėjišką veiklą ir ją užkardyti, operatyviai reikia surinkti daugiau informacijos, o jos apdorojimui pasitelkti automatizuotas priemones. Būtina atkreipti dėmesį, jog tarp SANS instituto ir Kibernetinio saugumo tarybos siūlomų, o taip pat ir Lietuvos Nacionalinio kibernetinio saugumo centro adaptuotų, kibernetinės saugos valdymo gerųjų praktikų nurodomas „audito žurnalų įrašų stebėjimas, analizė ir saugojimas“ [3].

Paslaugos tikslai:

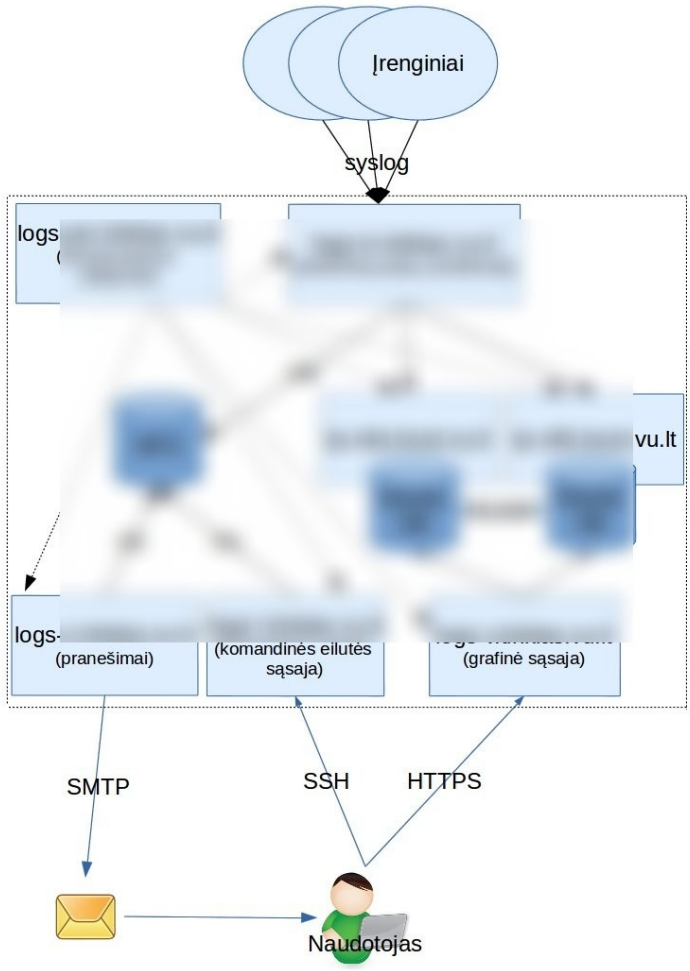
- tinkle veikiančios įrangos ir serverių sisteminių žurnalų duomenų saugojimas dedikuotoje, specialiai tam skirtoje, nuo pakeitimų apsaugotoje vietoje;
- grėsmių ar pažeidimų aptikimas naudojant automatizuotą žurnalų įrašų analizės įrankį ir tinklo įrenginių administratorių informavimas;
- galimybė tinklo įrenginių administratoriams peržiūrėti ir analizuoti žurnalų įrašus naudojant komandinės eilutės sąsajos komandas ir grafinės sąsajos vizualizacijas.

Paslaugos platformos architektūra

Sisteminių žurnalų įrašų valdymo infrastruktūra susideda iš trijų pakopų [4]:

- sisteminių įrašų kūrimo;
- sisteminių įrašų saugojimo;
- sisteminių įrašų peržiūros ir analizavimo.

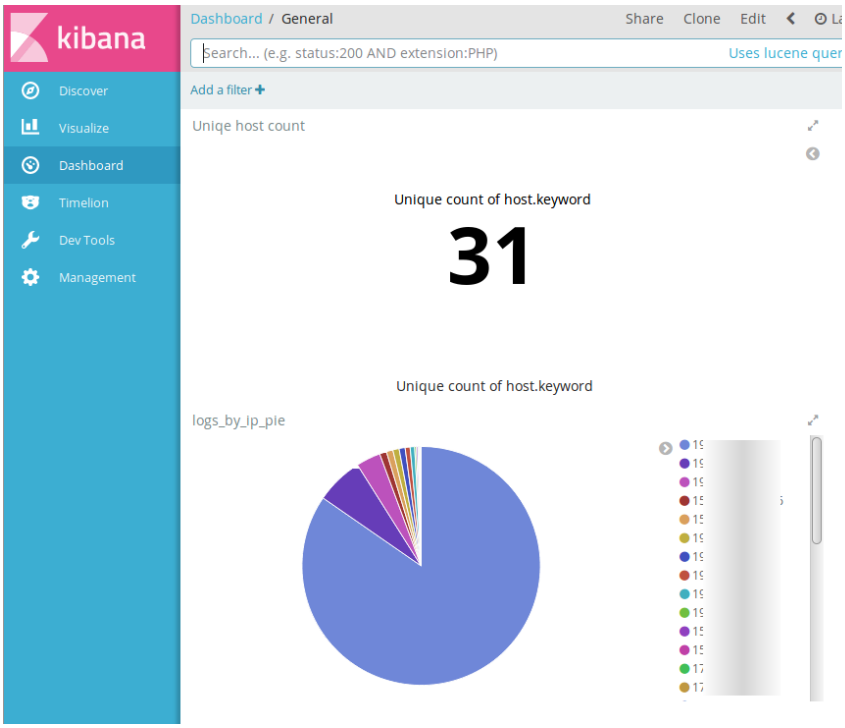
Vadovaujantis šia sisteminių žurnalų valdymo infrastruktūros koncepcija ir pasirinktos atviro kodo programinės įrangos (Linux, Elastic Stack, OSSEC) galimybėmis sukurta sisteminių žurnalų terminuoto saugojimo paslaugos su automatinės grėsmių analizės galimybėmis platformos koncepcinė architektūra (1 pav. ir 1 priedas).



1 pav. Koncepcinė architektūra

Paslaugos platforma sudaryta iš septynių serverių, duomenų saugyklų ir pagalbinės pašto persiuntimo tarnybos (angl. mailrelay):

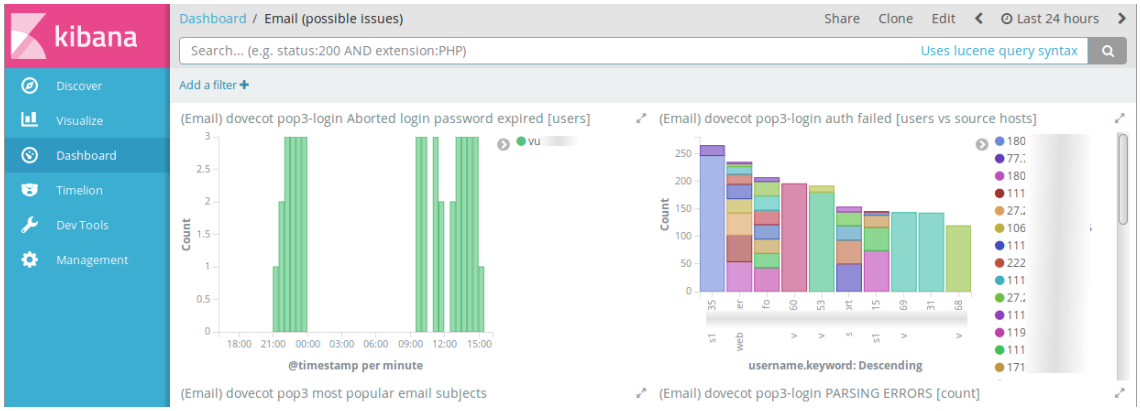
1. LITNET tinkle esantys įrenginiai syslog protokolu siunčia sisteminius įrašus sisteminių įrašų surinkimo serveriui, kuris pagal nustatytas taisykles rūšiuoja įrašus ir nukreipia saugojimui į NFS failinę sistemą bei Elasticsearch duomenų bazes.
2. Elasticsearch sistemų klasteris saugo ir realiu laiku paruošia surinkimo serverio perduodamus sisteminių žurnalų įrašus greitai paieškai.
3. Kritinių įvykių stebėjimo ir informavimo posistemis analizuoja NFS failinėje sistemoje saugomus įrašus ir apie užfiksuotus kritinius įvykius informuoja LITNET tinklo įrenginių administratorius elektroniniu paštu.
4. Prieigos prie įrašų SSH protokolu per komandinę eilutę posistemis suteikia LITNET tinklo įrenginių administratoriams galimybę peržiūrėti ir analizuoti savo įrenginių sisteminius įrašus standartiniu syslog formatu tik skaitymo teisėmis.
5. Įrašų paieškos ir vizualizavimo posistemis leidžia įrenginių administratoriams peržiūrėti ir analizuoti savo įrenginių įrašus per grafinę naršyklės sąsają. Įdiegtas



2 pav. Grafinės sąsajos pavyzdys

grafinis Elasticsearch duomenų bazės klientas Kibana suteikia galimybę įrašus paversti

statistine informacija bei atvaizduoti įvairių tipų ir pjūvių grafikais.



3 pav. Grafinės sąsajos pavyzdys

6. Centralizuota programinės įrangos ir atnaujinimų valdymo posistemis leidžia automatiškai atnaujinanti programinės įrangos saugyklą iš visų sistemose naudojamų šaltinių, suteikia vieningą prieigą diegti ir atnaujinti visus paslaugos platformos komponentus.

Techninė informacija aprašyta šio dokumento 2 ir 3 prieduose „Sistemos sandaros aprašymas“ ir „Techniniai reikalavimai“.

Sisteminių žurnalų terminuoto saugojimo paslaugos su automatinės grėsmių analizės galimybėmis platforma leidžia surinkti sisteminius įrašus standartiniu protokolu, užtikrina jų išsaugojimą įstatymuose numatytą laiką [5], leidžia peržiūrą standartiniu formatu SSH protokolu, atvaizdavimą grafiniais ir statistiniais pavidalais, informuos administratorius apie kritinius įvykius.

Informacijos saugojimas

Sisteminių žurnalų įrašai saugomi LITNET duomenų centruose – sistemos serveriai ir duomenų saugykla VU duomenų centre, atsarginių kopijų saugykla VGTU duomenų centre.

Prieiga prie sistemų apribota ugniasienėmis ir sisteminėmis prieigos kontrolės priemonėmis (ACL, file permissions, Search Guard).

Administratoriai gali pasiekti tik savo administruojamų sistemų sisteminius įrašus ir tik šifruotais protokolais.

Paslaugos naudojimas

Sisteminių žurnalų terminuoto saugojimo paslauga gali naudotis LITNET tinklo

administratoriai, savo administruojamuose įrenginiuose sukonfigūravę siųsti sisteminių žurnalo įrašus į įrašų surinkimo serverį.

Administratorius gali peržiūrėti ir gauti pranešimus tik apie jo administruojamų įrenginių atsiųstus įrašus.

Paslaugos užsakymo elektroninę formą galima rasti adresu https://info.tinklas.vu.lt/zurnalai/ .

Sisteminių žurnalų terminuoto saugojimo paslaugos naudotojo instrukcija pateikta 4 priede.

Literatūra ir šaltiniai

1. LITNET tinkle vykstančių saugumo incidentų statistika. Nuoroda: https://cert.litnet.lt/statistika-2/
2. Cyber Threats Are ‘Mind Blowing,’ Crooks Getting Smarter: Report. Nuoroda: http://www.nbcnews.com/mach/features/cyber-threats-are-mind-blowing-crooks-getting-smarter-report-n554176
3. CRITICAL SECURITY CONTROLS. Nuoroda: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf
4. Guide to Computer Security Log Management. Nuoroda: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
5. Lietuvos Respublikos elektroninių ryšių įstatymas

Priedai

1. Paslaugos architektūrinė schema
2. Sistemos sandaros aprašymas
3. Techniniai reikalavimai
4. Instrukcijos paslaugos naudotojui