http://salvio.montm.art:796 | salvio@montm.art

Salvio NC SensiOS

TINKLO IR INFORMACINIŲ SISTEMŲ (TIS) KIBERNETINIO SAUGUMO SENSORIŲ SISTEMA

Salvio NC SensiOS apjungia pažangiausias atvirojo kodo programas, komercines technologijas ir naujausias tinklų ir informacinių sistemų įsilaužimų stebėjimo, aptikimo ir reagavimo į kibernetinius įsilaužimus ir grėsmes saugumo sistemas į vieną sprendimą, kuris sumažina rimtų grėsmių galimybes ir padeda greitai į jas reaguoti. Lengvai įdiegiamas, suderinamas su populiariausiomis operacinėmis sistemomis, pagrįstas plačiai pripažintais standartais ir protokolais, nereikalauja jokių išankstinių išlaidų ar gamintojų licencijų.

Salvio NC SensiOS yra puikus sprendimas tiek mažoms / vidutinėms įmonėms, tiek didelėms įmonėms, ieškančioms kibernetinio saugumo rizikos ir incidentų valdymo, IT infrastruktūros saugumo ir stebėjimo sprendimų.

TINKLO IR INFORMACINIŲ SISTEMŲ (TIS) KIBERNETINIO SAUGUMO SENSORIŲ SISTEMA

Salvio NC SensiOS

NEPAKEIČIAMAS IT SISTEMŲ ADMINISTRATORIAUS ĮRANKIS

KIBERNETINIO SAUGUMO RIZIKOS IR INCIDENTŲ VALDYMAS

- Sustiprina verslo aplinkos kibernetinio saugumo atsparumą išorės ir vidaus įtakai
- Techninė priemonė IT infrastruktūros saugumo užtikrinimui pagal TIS2 direktyvos reikalavimus
- Užtikrina kibernetinio saugumo incidentų valdymo ir tyrimo veiksmingumą
- Pagerina IT sistemų administratoriaus darbo efektyvumą ir produktyvumą
- Pilnas sistemos diegimas, konfigūracijos ir eksplotacijos palaikymas
- Naujos kartos kibernetinio saugumo technologijos

IT INFRASTRUKTŪROS SAUGUMO UŽTIKRINIMAS

- Tinklo infrastruktūros įrenginių būklės stebėjimas
- Pilnas lokalaus tinklo duomenų perdavimo stebėjimas ir registras
- Apsauga nuo kenkėjiškų programų ir virusų
- Kenkėjiškų veiksmų aptikimas vidiniame tinkle
- IT sistemų žurnalo įrašų agregavimas, archyvavimas ir tyrimas
- Saugumo incidentų valdymas
- Pranešimai, ataskaitų teikimas ir įspėjimai apie aptiktus grėsmių požymius

FUNKCIONALUMAS

- Vietinio ir išorės tinklo pralaidumo (paslaugų kokybės) stebėjimas
- Duomenų srauto antivirusinis skenavimas realiu laiku vidiniame tinkle
- Tinklo duomenų paketų, sistemų registro įrašų, tinklapio kreipinių, perduotų failų registras
- Lokalus apgaulės tinklas HoneyNET, skirtas ankstyvam grėsmių aptikimui
- Tinklo įsilaužimo aptikimo sistema NIDS
- Kompiuterių įsilaužimo aptikimo sistema HIDS
- Tinklo protokolų anomalijų stebėjimo sistema BRO/ZEEK
- Kompiuterių ir tinklo įrenginių būsenos ir veiklos parametrų registravimas ir stebėjimas
- Pranešimų ir įvykių valdymo konsolė
- Visų tinklo sistemų registrų įrašų tyrimo ir analizės konsolė
- Tinklo anomalijų registro įrašų tyrimo ir analizės konsolė
- Pranešimų tvarkyklė panaudojant įvykių vertinimo taisykles

Salvio NC SensiOS
TECHNOLOGIJŲ APŽVALGA

Lokalus apgaulės tinklas HoneyNET, skirtas ankstyvam grėsmių aptikimui

Pilnas komplektas apgaulės aplikacijų, skirtų tinklo duomenų srauto stebėjimui, botų veiklos aptikimui ir bandymų atspėti vartotojų vardus bei slaptažodžius registravimui. Šis python aplikacijų komplektas imituoja ir registruoja bandymus naudoti pagrindinius tinklo protokolus, tokius kaip : dhcp, dns, elastic, ftp, http proxy, https proxy, http, https, imap, ipp, irc, ldap, memcache, mssql, mysql, ntp, oracle, pjl, pop3, postgres, rdp, redis, sip, smb, smtp, snmp, socks5, ssh, telnet, vnc.

Tinklo įsilaužimo aptikimo sistema (NIDS) – SURICATA

Suricata – tai naujos kartos didelio našumo tinklo analizės ir grėsmių aptikimo programinė įranga, kurią sukūrė ir prižiūri Open Information Security Foundation (Boston, Massachusetts JAV). Ši programinė įranga ne tik pakeičia ar dubliuoja tradicinius grėsmių diagnostikos įrankius, bet ir praktikoje realizuoja naujomis idėjomis pagrįstas modernias technologijas. Suricata palaiko procesorių daugiagijį režimą, automatinį protokolų aptikimą (IP, TCP, UDP, ICMP, HTTP, TLS, FTP ir SMB), Gzip archyvų išskleidimo ir greito IP paketų aptikimo funkcijas. Suricata taip pat naudojama tinklo paketų (PCAP) kopijų archyvavimui, tinkle perduodamų failų dekodavimui ir archyvavimui realiu laiku, o taip pat ir interneto naršyklių HTTP seansų registrui.

Kompiuterių įsilaužimo aptikimo sistema (HIDS) – SAGAN/LOKI

Sagan yra procesorių daugiagijį režimą naudojanti, didelio našumo sistemų registro įrašų analizės ir koreliacijos programinė įranga, sukurta Quadrant Information Security (Jacksonville, Florida JAV), veikianti Unix tipo operacinėse sistemose. Sagan parašyta C kalba ir naudoja kelių gijų procesoriaus architektūrą, kad pasiektų didelio našumo registro įrašų ir įvykių analizę. Sagan struktūra ir taisyklės veikia panašiai kaip klasikinės Sourcefire Snort IDS/IPS sistemos priemonės. Tai leidžia Sagan būti suderinama su Snort arba Suricata taisyklių valdymo programine įranga ir suteikia Sagan galimybę koreliuoti su Snort IDS/IPS duomenimis. Sagan palaiko skirtingus išvesties formatus, skirtus ataskaitoms teikti ir analizuoti, įrašų normalizavimą ir programų paleidimą aptikus rizikos požymius, GeoIP technologiją aptikimui/pranešimams ir vertina įvykių laiko faktorių. Įrašų agregavimą iš tinklo įrenginių atlieka rsyslog programa, kurią 2004 m. sukūrė Rainer Gerhards, Adiscon GmbH (Großrinderfeld, Vokietija) ir yra naudojama Unix tipo kompiuterių sistemose registro įrašų konsolidavimui IP tinklo protokolų pagalba. Tolesnei registro įrašų analizei įrašai yra įkeliami į Loki programinę įrangą, kuri yra lengvai išplečiama klonuojant, gali būti dubliuojama (high – availability) ir palaiko sistemos vartotojų teisių ir atsakomybių hierarchiją (multi-tenant).

Tinklo anomalijų stebėjimas – BRO/ZEEK

Zeek yra tinklo monitoringo programa, kurios paskirtis yra inspektuoti informacijos srautą tinkle ir generuoti registro įrašus, aprašančius stebimo tinklo duomenų perdavimo būdus. Zeek buvo sukurta 1996 m. Lawrence Berkeley National Laboratory Kalifornijos universitete (JAV). Pagrindinė Zeek naudojimo paskirtis - kibernetinių grėsmių paieška realiuoju laiku. Tinklo protokolų identifikavimui Zeek naudoja įprastų tinklo prievadų (portų) registrą ir dinaminį duomenų perdavimo būdų aptikimą (įskaitant požymių ir elgesenos analizę). Zeek monitoringo programa atlieka aplikacijų (protokolų) dekodavimą ir registravimą, aptinka anomalijas, požymių (signature) sutapimą ir registruoja kiekvieną IP sesiją vietiniame tinkle.

Tinklo srauto antivirusinis skenavimas realiuoju laiku – ClamAV

ClamAV antivirusinė programa yra naudojama tinkle perduodamų failų, kuriuos užregistravo ir suarchyvavo Suricata IDS sistema, nuskaitymui realiuoju laiku. ClamAV yra kelių apsaugos nuo kenkėjiškų programų įrankių platformų rinkinys, galintis aptikti daugelio tipų kenkėjiškas programas, įskaitant virusus. ClamAV virusų duomenų bazė yra atnaujinama ne rečiau kaip kas keturias valandas ir 2023 metų birželio duomenimis joje yra daugiau nei 6 mln. virusų kodų. 2007 m. ClamAV susijungė su Sourcefire Vulnerability Research Team (VRT). 2013m. Cisco įsigijo Sourcefire, ir Sourcefire VRT (kartu su ClamAV) tapo Cisco Talos.

Duomenų apdorojimo ir įvykių valdymo sistema – EveBOX, PROMETHEUS, GRAFANA

EveBox yra web-konsolės pagrindu veikianti įspėjimų ir įvykių valdymo įrankis, skirtas Sagan ir Suricata IDS/IPS sistemų pranešimams administruoti, kuris suteikia vartotojui "inbox" stiliaus metodą pranešimų valdymui. EveBox konsolę SOC operatorius gali pasirinkti papildomai prie klasikinių įvykių paieškos / analzės įrankių, tokių kaip Grafana Loki arba Unix lnav. Prometheus yra daugelyje populiarių platformų veikianti programa, naudojama įvykių stebėjimui ir pranešimams. Prometheus duomenis registruoja specializuotoje laiko parametrų (time series) duomenų bazėje (užtikrinančioje daugiamatį duomenų kaupimą), naudoja duomenų surinkimą HTTP protokolu, įvairialypes užklausas ir pranešimus realiuoju laiku. Grafana yra daugelyje populiarių platformų veikianti analizės ir interaktyvios vizualizacijos web-interfeiso programa. Grafanoje yra pateikiamos diagramos, grafikai ir pranešimai iš Prometheus laiko parametrų duomenų bazės. Ši programa veikia kaip Loki registro įrašų agregavimo platformos konsolė ir yra sukurta bei prižiūrima Grafana Labs, turinčioa biurus Niujorke ir Stokholme. 2021 m. Grafana Labs užsitikrino apie 220 mln. USD C serijos finansavimą.

Fizinis (x86-64) / virtualus įrenginys – Unix tipo GNU/Linux Debian OS

Sistemos diegimui gali būti naudojami nedidelių gabaritų Lanner, SuperMicro, HP, Dell, Lenovo kompiuteriai, o taip pat sistema gali būti realizuota kaip viena arba kelios virtualios mašinos x86-64 tipo procesoriaus didelio našumo serveriuose. Visos kibernetinio saugumo taikomosios programos yra instaliuojamos naudojant stabilią Debian GNU/Linux OS versiją. Debian operacinę sistemą 1993m. sukūrė ir palaiko ne pelno siekianti Debian Project organizacija. Taikomųjų ptogramų agentai / sensoriai gali būti įdiegti Linux / Windows / Apple darbo vietose ir serveriuose, registro įrašai, konfigūracijos ir tinklo srautai / statistika gali būti surenkami iš visų pagrindinių tinklo įrangos gamintojų įrenginių. Debian projektas yra asmenų, kurie bendrai siekė sukurti nemokamą operacinę sistemą, asociacija. Debian būstinė yra Hauppauge (Niujorkas, JAV). Naudojant metodą, pagrįstą COCOMO modeliu, apskaičiuota, kad visų paketų, įtrauktų į Debian 5.0 Lenny (323 milijonai eilučių kodo), kūrimo kaina yra apie 8 mlrd.USD.

Salvio NC SensiOS
GALIMOS PAPILDOMOS FUNKCIJOS

Tinklo infrastruktūros stebėjimas ir pranešimai – SNMP/IPMI/TCP (HTTP protokolu)

Papildoma web-interfeiso pagrindu veikianti monitoringo ir pranešimų sistema indikuoja visus sistemos parametrus ir yra pasiekiama iš išorės per openvpn arba ssh tunelį. Visi stebimi duomenys archivuojami Prometheus laiko parametrų duomenų bazėje. Operacinės sistemos ir taikomųjų programų parametrus registruoja taikomoji programa Netdata. Registro įrašų surinkimą atlieka rsyslog ir grok taikomosios programos, aparatinės įrangos būsenos duomenis ir tinklo įrenginių parametrus registruoja Prometheus SNMP plėtinys tiesiai iš tinklo įrenginių SNMP agentų. Pranešimai ir įspėjimai gali būti sukonfigūruoti bet kuriam grafikui ir metrikai, kad būtų galima greitai reaguoti į jautrius stebimos sistemos būsenos pokyčius. Kiekvienas grafikas arba visa web-interfeiso panelė gali būti automatiškai konvertuojama į PDF dokumentą ir išsiųsta iš anksto sukonfigūruotiems gavėjams pagal iš anksto nustatytą tvarkaraštį. Tai leidžia sistemos administratoriams automatizuotu būdu teikti periodines ataskaitas įmonės vadovybei ir partneriams / kibernetinio saugumo konsultantams.

Paskirstyta tinklo atsarginių kopijų sistema– BAREOS

Bareos yra programų rinkinys, skirtas kompiuterio duomenų atsarginių kopijų įrašymui, atkūrimui ir tikrinimui tinkle – tai atsarginių kopijų sistema mišrių operacių sistemų IT infrastruktūroms. Bareos yra korporatyvinio lygio kompiuterinių tinklų atsarginių kopijų kūrimo sistema, skirta heterogeniniams tinklams. Bareos komponentai, (Bareos Director, Storage Daemons ir File Daemons) naudoja šifravimą duomenų perdavimui vietiniame tinkle, o autentifikavimas yra šifruotas TLS/SSL protokolais – panaudojant sertifikatus arba iš anksto bendrinamus raktus. Bareos užšifruoja tiek pačias atsargines kopijas (per periferines taikomasias programas / agentus), tiek ryšį tarp individualių kompiuterių.

SSL/TLS šifruoto srauto monitoringas – HTTP/ SMTP/IMAP tarpiniai serveriai (proxy)

SSL/TLS būdu užšifruoto HTTP, SNMP ir IMAP srauto tikrinimas panaudojant tarpinius (proxy) serverius leidžia identifikuoti kenkėjišką veiklą, vykstančią šifruotais ryšio kanalais. Šiuo atveju monitoringas veikia kaip autorizuoto tarpininko (angl. man-in-the-middle) procesas, kai yra iššifruojamas, inspektuojamas, o po to vėl užšifruojamas duomenų srautas tarp kliento ir serverio. Tai leidžia užkirsti kelią duomenų pažeidimams identifikuojant užkoduotas kenkėjiškas programas ir neleidžiant įsilaužėliams prasiskverbti per kibernetinio saugumo užkardas, matyti ir suprasti, ką darbuotojai siunčia už organizacijos ribų, užtikrinti, kad darbuotojai tinkamai elgtųsi su konfidencialiais duomenims. Šifruoto srauto monitoringas užtikrina daugiasluoksnės apsaugos strategijos efektyvumą ir visos organizacijos kibernetinį saugumą.

DĖL PAPILDOMOS INFORMACIJOS PRAŠOME SUSISIEKTI SU MUMIS

e-mail: salvio@montm.art
Tel: +370 698 36598
Internetinis puslapis : http://salvio.montm.art:796
Demo versija : http://snc-sensios.montm.art:3000