

Cisco Security Intelligence Operations

Hva er Cisco Security Intelligence Operations?

Cisco Security Intelligence Operations (SIO) er en avansert sikkerhetsinfrastruktur som benyttes til å identifisere, analysere og forhindre trusler innen IT sikkerhet. Cisco SIO sitt globale forskningsteam analyserer store mengder sikkerhetsrelatert data som blir samlet inn fra hele verden. Med avanserte sikkerhetsanalyser tilbyr SIO rask og effektiv beskyttelse mot nye trusler innen IT.

Hvilke problemer kan dette løse?

Dagens samarbeidsorienterte infrastruktur og den raske utviklingen av sikkerhetstrusler gjør at trusselbildet er blitt mer omfattende enn noen sinne. Nye applikasjoner og tjenester, ofte utestet og sårbare, kan bli utnyttet av cyberkriminelle for sabotasje eller økonomisk gevinst. De nyeste truslene er ofte rettet mot personlig data og har en variert natur. Med angrepsvektorer som web, e-post og USB nøkler klarer ikke alltid tradisjonelle sikkerhets verktøy å beskytte infrastrukturen. Selv store anerkjente teknologier klarer ikke å holde takt med utviklingen innen dagens spesialiserte og målrettede angrep. Konsekvensen av å bli utsatt for angrep kan medføre svekket rykte, tyveri av identitetsinformasjon, systemnedetid, samt kostnader for opprydding og gjenoppretting av systemer. Følgende statistikker illustrerer dagens risikoklima:

- Det sendes mer enn 100 milliarder spam e-postmeldinger hver dag, dette er ca. 85 % av all e-post på verdensbasis. 80 % av all spam blir sent fra infiserte klienter.
- Antall trusselvarsler fra produsenter økte fra 6.77 % fra 2007 til 2008.
- Sårbarheter i virtualiseringsprodukter tredoblet til 103 i 2008 fra 35 i 2007.
- Omtrent 50 % av angrep er fra kilder som tidligere har vært brukt til angrep. Ca. 70 % av botnet bruker dynamiske IP adresser for å unngå svartelister.
- I løpet av 2008 var det en 90 % økning i vekst på trusler som stammer fra legitime domener, en dobling av antallet i 2007.¹
- Bedrifter som ble utsatt for angrep i 2008 betalte i snitt \$6.6 millioner i fjor for å gjenopprette tillit til deres varemerker og for å unngå å miste kunder.²

Med begrensede ressurser til å ta i bruk og vedlikeholde IT systemer trenger organisasjoner en løsning som kan beskytte mot økende sikkerhetstrusler samt senke kostnader. Cisco SIO infrastrukturen hjelper organisasjoner med å takle dagens utfordringer innen IT sikkerhet.

¹ Cisco 2008 Annual Security Report:

https://tools.cisco.com/gdrp/coiga/showsurvey.do?surveyCode=4026&keyCode=171020_1

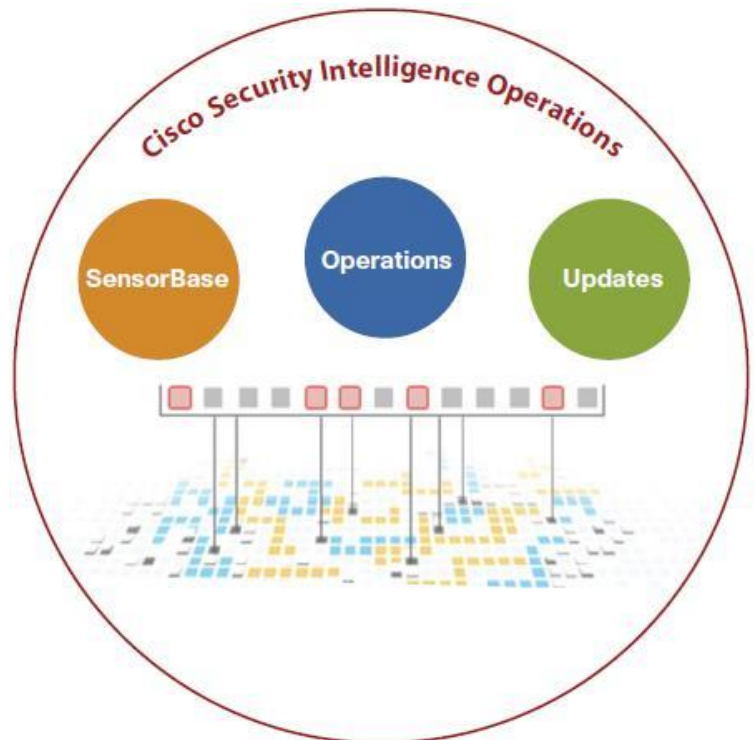
² Poneman Institute Study 2008:

<http://www.washingtonpost.com/wp-dyn/content/article/2009/02/02/AR2009020203064.html?hpid=sec-tech>

Cisco Security Intelligence Operations

Cisco Security Intelligence Operations er ett sofistikert sikkerhets økosystem som inneholder tre komponenter:

1. Cisco SensorBase: Verdens største overvåkningsnettverk som samler data på en global skala fra Cisco enheter og tjenester
2. Cisco Threat Operations Center: Ett globalt team som består av sikkerhetsingeniører og automatiserte systemer som analyserer trusselbildet og utvikler løsninger basert på omfattende etterretning.
3. Dynamiske oppdateringer: Sanntidsoppdateringer automatsikt dyttet ut til sikkerhetsenheter, samt "best practice" anbefalinger for å hjelpe kunder å følge med på trusselutviklingen, analysere situasjoner og forbedre den overordnede sikkerhetsberedskapen innen organisasjonen.



Cisco SensorBase

Etterretningsavdelingen av Cisco SIO inneholder verdens største sanntidsovervåkning nettverk: Cisco SensorBase. SensorBase kilder inneholder:

- Mer enn 700,000 Cisco sikkerhetsenheter fra alle verdensdeler som samler data om sikkerhetstrusler.
- Cisco IntelliShield, en trusseldatabase over 40,000 sårbarheter og 3300 IPS signaturer.
- Mer enn 600 tredjepartskilder som overvåker over 500 tredjeparts datastrømmer og 100 sikkerhetsrelaterte nyhetsstrømmer døgnet rundt.

Mer enn 1000 servere er brukt for å samle og behandle informasjon om trusler. Over 500 GB data blir behandlet hver dag. Cisco Threat Operations Center behandler denne globale sanntidsinformasjonen og bruker dette til å utvikle sikkerhetstjenester i Cisco enheter.

Threat Operations Center

Den operasjonelle avdelingen av Cisco SIO er en kombinasjon av mennesker og automatiserte algoritmer som:

- Behandler Cisco SensorBase data i sanntid.
- Lager maskingenererte og manuelt genererte regler.
- Utvikler løsninger for å beskytte mot nye og dynamiske trusler.



Threat Operation Center teamene består av mer enn 500 mennesker dedikert til 24x7x365 forskning, analyse og QA spredt over fem globale lokasjoner. Threat Operations samarbeider også med andre Cisco avdelinger for å bedre kunne kjempe cyberkriminalitet:

- Cisco IronPort E-mail and Web Threat Research Team: Tilbyr beskyttelse mot SMTP og Web baserte angrep.
- Cisco Malware Research Lab: En sentralisert lab som fokuserer på forskning på de nyeste malware og ondsinnede nettaktiviteter.
- Intrusion Protection Signature Team: Forsker og utvikler spesifikke signaturer til Cisco IPS produkter. Disse beskytter mot kjente sårbarheter.
- Cisco Produkt Security Incident Response Team (PSIRT): Evaluerer og arbeider på tvers av Cisco for å motvirke sårbarheter rapportert i Cisco produkter.
- Strategic Assessment Technology Team (STAT): Avansert lokasjonsspesifikk sikkerhetsforskning og produktsårbarhets testing.
- Infrastructure Security Research & Development (ISRD): Forskningsorientert gruppe som spesialiserer på IT sikkerhet og utvikler løsninger for kunders infrastruktur.
- Remote Management Servies (RMS): Tilbyr 24x7x365 fjernovervåkning og drift av Cisco sikkerhetsenheter som er i kunders nettverk.
- Intellishield Security Analysts: Ett team som analyserer og forsker på sikkerhetsrelaterte begivenheter som kan påvirke kundenettverk, applikasjoner og enheter.

- Applied Intelligence: Ett team som utvikler løsninger for å rette på sikkerhetshull annonsert fra "Cisco Security Advisories and Responses", "Microsoft Security bulletins", og andre produsenter.

Global Correlation

Cisco Global Correlation er ett sofistikert og automatisert sikkerhetssystem som gjør IPS mer effektiv enn noen gang. Global Correlation korrelerer automatisk trusselinformasjon fra SensorBase som rykte, kjente applikasjonssårbarheter, uvanlige trafikkmønstre og andre sårbarheter for å fange opp varierte, utsprede og målrettede angrep.

Global Correlation er basert på den komplette oversikten over alle trusselvektorene som SensorBase gir innsikt i.

Der tradisjonelle nettverks IPS undersøker kun pakkeinnhold, gjør Global Correlation en analyse av den overordnede sammenhengen for å bedre forstå om trafikken inneholder mistenksom aktivitet. Nå er det ikke lenger bare innholdet som er inspisert, men også hvem som sendte det, hva det inneholder, hvor det kom fra, og hvordan det utviklet seg. Følgende parametre er vurdert i Global Correlation motoren:

- Hvem: Rykte til avsenderen. Ryktefiltret sperrer trafikk fra de verste angriperne, stopper 10 % til 15 % av angrep, og gir en tilpasset ryktescore til mistenkte angrep.
- Hva: Pakkeinnhold som matcher utnyttelse av sikkerhetshull eller en kjent signatur. Cisco har mer enn 3300 signaturer og team som stadig forbedrer og utvikler signaturer.
- Hvor: Analyse av geografisk opprinnelse av pakkene og korrelering med eksisterende trender.
- Hvordan: Sprednings og muterings metoder blir analysert. IPS korrelerer informasjon fra ryktescore, signaturanalyse og trafikkmønstre.

Global Correlation bruker disse parametrene for stadig å forbedre nye oppdateringer, tester og nye regler. Dette fører til en raskere, mer effektiv, og nøyaktig hindring av angrep gjennom IPS sensorer. Resultatene innebærer:

- Dobling av effektiviteten i forhold til IPS som kun baserer seg på signaturer.
- Mer nøyaktig identifisering av angrep og færre "false positives" pga. rykteanalyse.
- Oppdateringer som er 100 ganger raskere enn tradisjonelle metoder som baserer seg kun på signaturer.

Dynamiske Oppdateringer



Cisco SIO sine dynamiske oppdateringer leverer nøyaktig og komplett sikkerhetsinformasjon til Cisco kunder og enheter. Trusselbekjempende data er levert gjennom:

- Automatiske regel oppdateringer for alle Cisco produkter, som brannmur, web, IPS eller e-post enheter.
- Intellishield sårbarhetsanalyse og varsel tjenester.
- Sikkerhets "best practice" anbefalinger og deltagelse i nettsamfunn.

Enkelte sikkerhetsoppdateringer er tilgjengelige i sanntid, for eksempel ryktebasert data som er brukt av Cisco sikkerhetsenheter for å blokke trafikk fra kjente ondsinnede sendere. Andre systemer, som Cisco IPS med Global Correlation, søker etter nye regler hvert 5 minutt.

I tillegg til dynamiske oppdateringer, er Cisco sin sikkerhetsetterretning offentliggjort i mange andre former for at sluttbrukere, bedrifter, og til og med regjeringer skal kunne dra nytte av den. Eksempler av dette er:

- Cisco IntelliShield Alerts, including Malicious Code Alerts, Security Activity Bulletins, Security Issue Alerts, Threat Outbreak Alerts, and Geopolitical Security Reports
- Cisco Annual Security Reports
- Cisco PSIRT Security Advisories and Security Responses
- Applied Mitigation Bulletins
- Cyber Risk Reports
- Security Intelligence Best Practices
- Service Provider Security Best Practices
- Cisco IPS Active Update Bulletins
- IntelliShield Event Responses
- Annual Security Report
- Cisco IronPort Virus Outbreak Reports

Gjennom denne omfattende sikkerhetssyklus tankegangen for å forstå og bekjempe trusler, får du kunnskapen som trengs til å ta reflekterte beslutninger. Du får forbedret sikkerhetsholdningen i din bedrift mens nettverket ditt blir automatisk beskyttet av de nyeste angrep.

Hva er fordelene med Cisco Security Intelligence Operations?

Forretningsfordelene av Cisco SIO er som følger:

- Unngå unødvendige kostnader for å rydde opp etter ett IT angrep.
- Beskytt rykte på din merkevare og din bedrift.
- Øk oppetid.
- Øk vekst ved å ta i bruk nye teknologier.
- Optimaliser effektivitet av drift.
- Forbedre samsvar med offentlige krav.
- Få innsikt i det nyeste i trussellandskapet.

- Forbedre beskyttelse mot nye trusler med økt effektivitet av sikkerhetsenheter, som Cisco IronPort Email and Web Security, Cisco IPS, og Cisco Adaptive Security Appliances.
- Øk beskyttelse mot spam og trusler med høyere nøyaktighet på trusselidentifisering.

Hvorfor Cisco?

Med økningen i varierte, protokolluavhengige, og produsentuavhengige sårbarhetstrusler har sikkerhetsindustrien måttet innse at punktbasert forsvar som beskytter mot individuelle trusler eller som beskytter individuelle produkter ikke lenger er tilstrekkelige. Integrert sikkerhetsadministrasjon, sanntids ryktebasert analyse og en flerpunkts lagbasert struktur er nødvendig.

Etter hvert som infrastrukturløsninger blir mer samarbeidsorienterte, er økt risiko uunngåelig. Cisco Security Intelligence Operations forbedrer evnen til å identifisere, analysere og forhindre dagens trusler. Cisco har forpliktet seg til å tilby komplette sikkerhetsløsninger som er integrert, raske, og effektive. Dette gir uslåelig sikkerhet for organisasjoner for å kunne trygt benytte seg av samhandlingsteknologier.