Integratie van PSIM en SIEM in Situation AWare Security Operation Center

De convergentieslag

De bekende security industrie-analist en visionair Steve Hunt schreef er in 2005 al over: convergentie tussen SIEM en PSIM. In de visie van Hunt levert integratie van SIEM met PSIM veel efficiency voordelen op. Incidenten en events kunnen immers grotendeels door hetzelfde proces worden afgehandeld. Er ontstaat vanuit één centraal punt een overzicht over alle ICT en non-ICT security incidenten. Door het voortdurend monitoren en analyseren van systemen en logging kan men veel pro-actiever handelen op mogelijke security issues. Technologie providers zoals NICE en Proximex (onderdeel van TYCO security) volgden in 2011 met de eerste commercieel verkrijgbare SIEM/PSIM oplossingen gedreven vanuit de NERC-CIP regelgeving.

In november 2013 startte project Situation AWare Security Operation Center (SAWSOC). Doel is het vaststellen en implementeren van technieken die nodig zijn voor de convergentie tussen physical en cyber security. SAWSOC is een samenwerkingsproject tussen een aantal onderzoeksinstellingen, universiteiten en IT-bedrijven uit Ierland, Engeland, Israel, Finland, Duitsland en Polen. Dit project wordt gesponsord door de Europese Commissie vanuit het FP7-SECURITY Programma (SEC-2012.2.5-1 Convergence of physical and cyber security – Capability Project). De gedachte achter SAWSOC is dat door de holistische benadering en verbeterde technieken bewuste en betrouwbare detectie en analyse van aanvallen kan plaatsvinden. Dit dient uiteindelijk te leiden tot het verwezenlijken van de twee grote belangrijke doelstellingen van SAWSOC: bescherming/beveiliging van burgers en goederen, en het verbeteren van de perceptie van veiligheid door burgers.

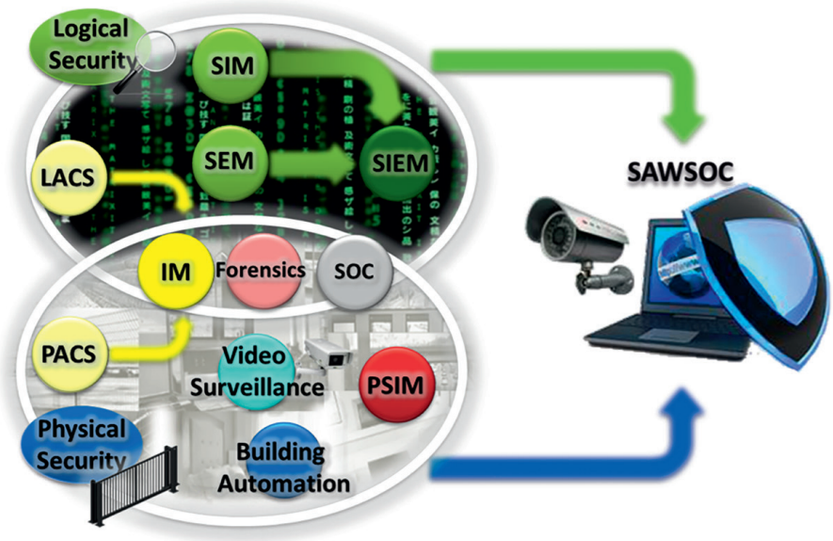
Het SAWSOC-project duurt 30 maanden en beschikt over een budget van ongeveer 5 miljoen euro, waarvan 3,4 miljoen wordt bijgedragen door de Europese commissie. Het project bestaat uit 11 partners uit 7 landen. Het dient in mei 2016 een platform op te leveren op basis waarvan systemen kunnen worden ontworpen, wat echte convergentie van physical en cyber security technologieën bewerkstelligt en verdere versnippering voorkomt.

> **“Convergentie betekent kortweg meer veiligheid tegen minder kosten.**

Sleutelelementen

Opdat het project zou slagen is het van belang dat de drie belangrijkste elementen binnen SAWSOC tot ontwikkeling komen: Security Information & Event Monitoring (SIEM), Physical Security Information Management (PSIM) en Identity Management (IM).

Security Information & Event Monitoring (SIEM) is binnen de ICT security ondertussen een begrip. Een SIEM geeft grip op en inzicht in alle mogelijke netwerkbeveiliging, risico's en bedreigingen. SIEM maakt het geautomatiseerd monitoren en controleren van het beveiligingsbeleid van een organisatie mogelijk. Een SIEM doet dit door realtime informatie te verzamelen uit logfiles van netwerkcomponenten, tools, securitycomponenten, servers, laptops, desktops, applicaties en databases en deze vervolgens te correleren, analyseren, presenteren en om security threats te detecteren. Een belangrijk aspect hierbij is de correlatie, waarbij verbanden tussen logs gezocht worden. Hierdoor geeft een SIEM een overzichtelijk beeld van de actuele status van de ICT security. Wat een SIEM doe in de



ICT security wereld, doet een PSIM (Physical Security Information Management) voor de physical security wereld. Een PSIM is een software platform dat verschillende losse (beveiliging)systemen integreert die beheerd worden via een uitgebreide meestal grafische gebruikersinterface. Hierdoor kan men dagelijkse operationele handelingen, incident management en crisisbeheersing op een duidelijke, gestructureerde en controleerbare wijze uitvoeren. Zo worden camerasystemen, toegangscontrole, inbraakdetectie en andere soortgelijke systemen samengebracht in PSIM. Een SIEM en een PSIM hebben een vijftal identieke hoofdfuncties:

- Collection: via onafhankelijke device management software kan het systeem gegevens verzamelen van een willekeurig aantal uiteenlopende beveiligingssystemen en apparaten.

- Analyse: het systeem kan gecollecteerde informatie zoals data, gebeurtenissen, alarmen en andere belangrijke gegevens, analyseren en correleren.
- Verificatie: de gegevens uit de analysefase worden gefilterd, geïdentificeerd en geperiodiseerd op een dergelijke wijze dat ze inzichtelijk worden voor de security operators.

- Resolutie (incident response): het systeem voorziet in een unieke set van standaard operationele procedures (SOP's) die afgeleid zijn uit het beleid en de best practices afspraken van de organisatie. Door deze stap-voor-stap instructies zijn security operators in staat de gebeurtenissen af te handelen in het geval van een noodsituatie.

- Rapportage: het systeem verzamelt niet alleen informatie in het begin, maar registreert ook alle informatie en maakt een overzicht van genomen acties en maatregelen. Dit kan achteraf worden gebruikt voor rapportage doeleinden.

In SAWSOC komen SIEM en PSIM echt samen.

Identity Management

Voor de convergentie tussen SIEM en een PSIM is het beschikken over één identiteit in zowel de physical en cyberwereld noodzakelijk. Hoe kan anders immers een relatie gelegd worden tussen de virtuele en fysieke persoon. Sinds 2009 bestaat er een trend om Logical Access Control Systems (LACS) en Physical Access Control Systems (PACS) samen te voegen tot Identity Management. Convergentie naar één identiteit brengt onder meer authenticatie naar een hoger model. Zo kan er naast de drie klassieke authenticatie-elementen (wat je weet, wat je hebt, wie je bent) nu ook een vierde element, namelijk 'waar je bent', in het authenticatieproces worden gebruikt.

> **Gezien de huidige legacy, de vervangingscyclus (10 jaar) en de wet en regelgeving ten opzichte van fysieke beveiliging zal het zeker nog een aantal jaren duren voordat convergentie tussen PSIM en SIEM zal plaatsvinden.**

Een ander groot voordeel van convergentie naar één identiteit is kostenreductie. Geïsoleerde oplossingen bieden onvoldoende garantie: er kunnen gemakkelijk gaten ontstaan in het proces van uitgifte en inname van rechten. Door convergentie tussen de physical en cyber security werelden kunnen de processen rond rechtenbeheer worden vereenvoudigd en verbeterd en worden kosten bespaard. Convergentie betekent kortweg meer veiligheid tegen minder kosten.

Conclusie

SAWSOC zal een geavanceerd Security Operations Center (SOC) platform opleveren. Hierdoor kan een accurate, tijdige en betrouwbare detectie en diagnose van aanvallen worden ondersteund. Daarnaast kan met het correleren van gebeurtenissen uit een breed scala van fysieke en logische beveiligingsbronnen een verbeterde situational awareness worden ontwikkeld. In de

dagelijkse praktijk zien we echter nog een stringente scheiding tussen de physical en cyber domeinen. Zo worden PSIM systemen geleverd door de elektrotechnische beveiligingsinstallateurs en SIEM wordt veelal geleverd door de IT security bedrijven. Bedrijven die in beide werelden succesvol actief zijn, kunnen op één hand geteld worden en succesvolle samenwerkingen tussen deze bedrijven zijn gering. Gezien de huidige legacy, de vervangingscyclus (10 jaar) en de wet en regelgeving ten opzichte van fysieke beveiliging zal het zeker nog een aantal jaren duren voordat convergentie tussen PSIM en SIEM zal plaatsvinden.

Ook de benodigde convergentie naar één identiteit kent nog de nodige obstakels. Ook bij deze convergentie is de stringente scheiding tussen de domeinen één van de grootste obstakels. Dit wordt nog verstrekt doordat de twee domeinen op het vlak van organisatorische bedrijfsindeling vaak gescheiden gehouden worden. Zo is de facility afdeling vaak verantwoordelijk voor physical Security en IT voor ICT security. Pas als deze hindernissen genomen zijn, kan SAWSOC tot volle ontwikkeling komen. Tot slot ontbreken binnen het SAWSOC-project de grote leveranciers uit zowel de PSIM en SIEM securitywereld. De vraag blijft dan ook: zal SAWSOC echt zorgen voor de volgende fase van SIEM? Of verbranden we 3,4 miljoen Europees geld voor niets?

(Door Ronald Eygendaal)

Bronnen:
http://www.sawsoc.eu/
http://www.surveillance-magazine.com/2014/01/05/the-converging-roles-of-physical-and-it-security-and-the-rise-of-psim
http://www.nice.com/news/newsletter/more2.php?page_id=467&edition=11_9s
http://www.securitysquared.com/2010/03/psim-and-siem-proximex-arcsight.html