De integratie van SIEM met PSIM levert efficiency voordelen op. Immers, incidenten en events kunnen door hetzelfde proces worden afgehandeld en er ontstaat vanuit één centraal punt een overzicht van alle ICT en non-ICT security incidenten. Ronald Eygendaal schetst de nieuwste ontwikkelingen.

tekst Ronald Eygendaal

SIEM: de volgende fase

In november 2013 startte het project Situation AWare Security Operation Center (SAWSOC). Doel van Sawsoc is vaststellen en implementeren van technieken die nodig zijn voor de convergentie tussen physical en cybersecurity. Sawsoc is een samenwerkingsproject tussen een aantal onderzoeksinstellingen, universiteiten en IT-bedrijven uit Ierland, Engeland, Israël, 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 erachter is dat door de holistische benadering en verbeterde technieken bewuster en betrouwbare (lees: juist, tijdig en betrouwbaar) detectie en analyse van aanvallen kan plaatsvinden. Dit dient uiteindelijk te leiden tot het verwezenlijken van de twee belangrijkste doelstellingen van Sawsoc:

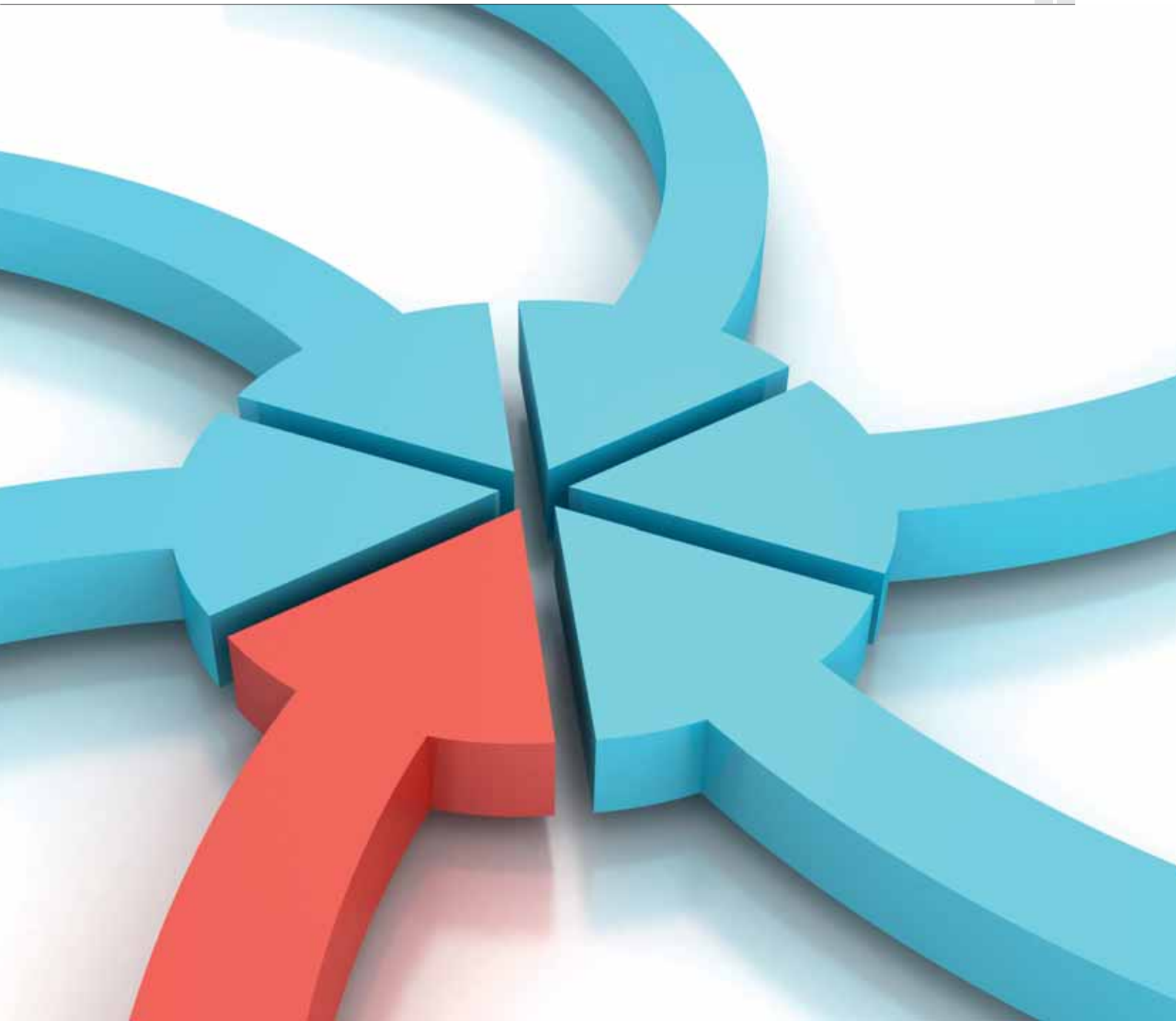
1. De belofte voor bescherming/beveiliging van burgers en goederen.
2. Verbeteren van de perceptie van veiligheid door burgers.

Het totale project duurt 30 maanden en kent een budget van ongeveer vijf miljoen euro, waarvan 3,4 miljoen wordt bijgedragen door de Europese Commissie. Het project kent elf partners uit zeven landen en dient in mei 2016 een platform op te leveren op basis waarvan systemen kunnen worden ontworpen, dat echte convergentie van physical en cybersecurity technologieën bewerkstelligt en dat verdere versnippering voorkomt.

WASDOM

Willen we Sawsoc tot een succes maken, dan is het van belang dat de volgende drie elementen ervan tot wasdom komen:

1. Security Information & Event Monitoring (SIEM).



2. Physical Security Information Management (PSIM).
3. Identity Management (IM).

SIEM

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

PSIM

Wat een SIEM doet in de ICT security wereld, doet Physical Security Information Management voor de physical security wereld. 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 camera-, toegangscontrole-, inbraakdetectie- en soortgelijke systemen samengebracht in PSIM. In de basis hebben SIEM en PSIM vijf identieke hoofdfuncties:

1. Collectie: via onafhankelijke device management software kan het systeem gegevens verzamelen van een willekeurig aantal uiteenlopende beveiligingssystemen en apparaten.
2. Analyse: het systeem kan gecollecteerde informatie zoals data, gebeurtenissen, alarmen en andere belangrijke gegevens analyseren en correleren.
3. Verificatie: de gegevens uit de analysefase worden gefilterd, geïdentificeerd en geperiodiseerd op zodanige wijze dat ze inzichtelijk worden voor de security operators.
4. Resolutie (incident response): het systeem voorziet in een unieke set van standaard operationele procedures (SOP's) welke afgeleid zijn van beleid en best practices afspraken van de organisatie. Door deze stap-voor-stap instructies zijn security operators in staat de gebeurtenissen af te handelen in geval van een noodsituatie.
5. Rapportage: het systeem verzamelt niet alleen informatie aan het begin, maar regisseert ook alle informatie en overzicht van genomen acties en maatregelen. Dit kan achteraf worden gebruikt voor rapportagedoeleinden.

In Sawsoc komen SIEM en PSIM echt samen.

IDENTITY MANAGEMENT

Voor de convergentie tussen SIEM en PSIM is het hebben van één identiteit in zowel de fysieke als de cyberwereld noodzakelijk. Immers, hoe kan je anders relaties leggen tussen de virtuele en fysieke persoon. Sinds 2009 is er een trend gaande 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 naast de drie klassieke authenticatie-elementen - wat je weet, wat je hebt, wie je bent - nu ook een vierde element - 'waar je bent' - in het authenticatieproces worden gebruikt.

Een ander voordeel van convergentie naar één identiteit is kostenreductie. Geïsoleerde oplossingen bieden onvoldoende garantie: gaten in het proces van uitgifte en inname van rechten kunnen gemakkelijk ontstaan. Door convergentie tussen de fysieke en de cyberwerelden kunnen de processen rond rechtenbeheer worden vereenvoudigd en verbeterd en worden kosten bespaard. Kortom, convergentie betekent meer veiligheid tegen minder kosten.

CONCLUSIE

Sawsoc zal een geavanceerd Security Operations Center (SOC) platform opleveren. Hierdoor kunnen accurate, tijdige en betrouwbare detectie en diagnose van aanvallen worden ondersteund. Daarnaast kan met correleren van gebeurtenissen uit een breed scala van fysieke en logische beveiligingsbronnen een verbeterde situational awareness worden ontwikkeld. Echter, in de dagelijkse praktijk zien we nog een stringente scheiding tussen de fysieke en cyberdomeinen. Zo worden PSIM-systemen geleverd door de elektrotechnische beveiligingsinstallateurs, SIEM wordt veelal geleverd voor de IT security-bedrijven. Bedrijven die in beide werelden succesvol actief zijn, kan men op de vingers van één hand tellen en succesvolle samenwerkingen tussen deze bedrijven zijn gering. Gezien de huidige legacy (de vervangingscyclus van tien jaar) en de wet- en regelgeving ten aan van fysieke beveiliging zal convergentie tussen PSIM en SIEM zeker nog een aantal jaren op zich laten wachten.

De benodigde convergentie naar één identiteit kent ook nog de nodige obstakels. Ook hier speelt de stringente scheiding tussen de domeinen een belangrijke rol. Dit wordt nog versterkt doordat we qua organisatorische bedrijfsindelingen de twee domeinen vaak nog geschieden houden. Zo is veelal Facilities verantwoordelijk voor physical security en IT voor ICT security. Pas als al deze hobbels genomen zijn, kan Sawsoc tot wasdom komen.

VOLGENDE FASE?

Tenslotte, binnen het Sawsoc project ontbreken vooralsnog de grote leveranciers uit zowel de PSIM- als de SIEM-werelden. Vraag blijft daarom of Sawsoc echt gaat zorgen voor de volgende fase van SIEM? Of verbranden we 3,4 miljoen euro Europees geld voor niets? ■

Ronald Eygendaal is freelance verslaggever en schrijft regelmatig over informatiebeveiliging, elektronische & technische beveiliging, fraudedetectie & -bestrijding, en bewaking & beveiliging.