IT/OT 융합 환경의 사이버 보안에 대한 Yokogawa의 접근

시오자키 테츠오 (Tetsuo Shiozaki)[*1]

많은 기업들이 자체적으로 사이버 보안 관제 센터(security operation center: SOC)를 구축하는 것을 기술 및 운영 상의 어려움으로 인해 주저하고 있습니다. Yokogawa는 고객의 시스템을 위한 SOC를 2019년에 개소하여 운영 중에 있습니다. 또한 Yokogawa는 사물 인터넷(IoT) 서비스를 위한 보안 모니터링 시스템도 개발하고 있습니다. 이 백서(white paper)에서는 Yokogawa의 SOC와 핵심 기술 및 자체 개발한 운영 방안과 사이버 보안에 대한 궁극적인 접근 방식에 대해 설명합니다.

도입

디지털 전환(DX)이 가속화되면서 클라우드 서비스의 활용도가 높아지고, 운영기술(OT)과 정보기술(IT)융합은 더욱 가속화되고 있습니다. 이러한 추세에 따라 보안 모니터링의 중요성이 증가하고 있습니다. IDC Japan의 설문 조사에 따르면 일본의 제조 회사 중 30% 이상이 IIoT(산업용 사물 인터넷) 시스템 및 OT 시스템에서 보안 사고를 경험했다고 응답했습니다(1). 그림1은 Yokogawa의 DX 인프라 아키텍처를 보여줍니다. 이 문서에서는 보안관리 서비스에 대해 설명합니다.

보안관제센터의 설립 배경

DX를 추진하기 위해서는 보안을 강화하는 것이 필수적이지만 Yokogawa는 보안 관제 센터를 설치하기 전에 다음과 같은 이슈를 해결해야 했습니다.

- 그동안 침입탐지시스템(intrusion detection system: IDS)을 이용한 보안 관제 서비스를 외부 IT업체를 통해 아웃소싱을 해 오고 있었습니다. 그러나 IDS 모니터링만으로는 사이버 공격을 식별하고 신속하게 탐지하고 그 영향 범위를 파악하기가 어려웠습니다. 다양한 로그(logs) 간의 상관관계 분석도 필요했습니다.
- Yokogawa의 IT 시스템은 전 세계적으로 사용되며 각 거점(Base)

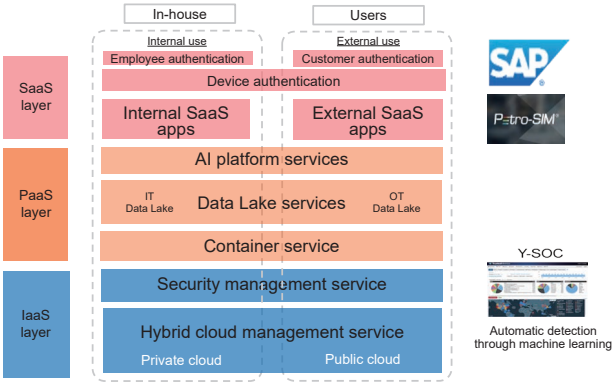

그림1 Yokogawa의 DX 인프라 아키텍처

에는 자체 IT 부서가 있습니다. 이들 거점(Base)은 자율적으로 각종 보안 제품을 설치했고, IT 거버넌스가 확립되지 않아 일원화된 모니터링 체계가 없는 상태였습니다

- 그 결과 지역별로 보안 수준이 서로 달랐고 취약한 지역에서 촉발된 사이버 공격은 글로벌 시스템을 위협했습니다.
- 다양한 로그(logs)를 분석하기 위해서는 Yokogawa의 자체 SIEM(Security Information and Event Management: 보안 정보 및 이벤트 관리) 인프라를 개발 및 운영해야 했지 이 작업을 수행할 IT보안 인력이 충분하지 않았습니다.

이러한 배경에서 Yokogawa는 SOC(보안관제센터)를 설립하기로 결정했습니다. 그러나 다양한 IT 및 OT 데이터 소스의 로그와 이

*1 디지털전략본부 산하 글로벌인프라보안센터

벤트를 수집, 처리 및 분석하고 신속하게 대응할 수 있는 솔루션이 필요했습니다. 회사는 향후 이러한 서비스를 고객에게 제공할 계획이었기 때문에 특정 제품에 종속적이 아닌 개방형 모니터링 솔루션이 필요 했습니다. 또한 Microsoft Azure 및 Amazon AWS와 같은 퍼블릭 클라우드도 지원해야 했습니다. 이에 구축해 개발에 필요한 인력투입을 줄이고 조기에 런칭할 수 있도록 클라우드를 통한 SaaS(Software as a Service: 서비스로서의 소프트웨어) 방식의 SIEM을 구축하기로 했습니다.

개발 이력 및 SOC 개요

모니터링 방식은 지역별로 모니터링을 수행하는 분산형 SOC와 한 곳에서 집중적으로 모니터링을 수행하는 중앙집중식 SOC의 두 가지 방식이 있습니다. Yokogawa 시스템의 규모를 고려하여 중앙집중식 방식을 선택했습니다. 일본(도쿄)과 싱가폴에서 레퍼런스 모델을 구축한 후 해외로 확장했습니다. 이 프로젝트의 진행 상황은 다음과 같습니다.

■ 2019년 1월부터 3월까지

도쿄 및 싱가포르 사무소에서 SaaS SIEM으로 일래스틱서치[Elasticsearch: 분산 처리 및 멀티 테넌시(multi-tenancy: 한 대의 서버에 작동하는 소프트웨어를 여러 테넌트가 공유하는 서비스)를 위한 오픈 소스 검색 엔진]의 PoC(proof-of-concept: PoC) Test를 수행했습니다. IDS와 AD(Active Directory: 액티브 디렉토리), DHCP(Dynamic Host Configuration Protocol: 동적 호스트 구성 프로토콜), DNS(Domain Name System: 도메인 네임 시스템) 서버의 로그를 수집했습니다. PoC에서는 로그 수집 방식, 전송 시간, 무단 접근 탐지, 분석 방식, 대시보드 디자인 등 SOC 구축에 필요한 요구 사항을 확인했습니다. 일래스틱클라우드(Elastic Cloud)의 효율성도 조사했습니다.

■ 2019년 4월 ~ 12월

인도(벵갈루루)에 SOC 개발팀을 조직하고 주요 6개 지역(일본, 유럽, 북미, 싱가포르, 중동, 인도)에서 보안 모니터링을 시작했습니다.

■ 2020년 1월 ~ 6월

15개 지역(중국, 러시아, 남미, 대만, 필리핀, 인도네시아 등)으로 모니터링을 확대했습니다. 우리는 CSIRT(Computer Security Incident Response Team: 컴퓨터 보안사건 대응팀)의 구조를 개선하기 위해 각 지역의 IT 부서와 협력했습니다.

■ 2020년 7월 ~ 12월

자체 모니터링 기능이 충분히 검증되어 아웃소싱을 중단하고 모니터링을 자체 시스템으로 전환하였습니다. 또한 Microsoft 365 관련 보안 기능(Defender ATP, MCAS)과 클라우드 기반 웹 애플리케이션 방화벽(web application firewall: WAF)을 사용하여 모니터링을 시작했습니다. 또한 IT 서비스를 위한 다양한 워크플로우를 제공하는 ServiceNow ITSM을 도입했습니다.

■ 2021년 1월부터

일본, 벵갈루루, 루마니아에서 24시간 삼극 모니터링 시스템(tripolar monitoring system)을 구축했습니다.

이 과정을 통해 현재 Yokogawa 보안운영센터(Yokogawa Security Operation Center: Y-SOC)는 다음과 같은 기능을 제공합니다.

(a) Yokogawa의 IT 인프라(PC, IDS, AD/DHCP/DNS, 메일 게이트웨이, 클라우드 서비스)에서 발생하는 보안 로그 및 이벤트를 수집합니다.

(b) Python 스크립트, Watcher(Elasticsearch용 경보 감지 플러그인) 및 Cyber Threat Intelligence(CTI: 사이버 공격 추적 및 감지 방법 모음)를 사용하여 의심스러운 통신 및 이벤트를 감지하고 자동으로 경보를 발행합니다.

(c) 각 지역의 보안 담당자와 협력하여 ServiceNow를 사용하고 사고 대응 워크플로를 자동화합니다.

그림2는 Y-SOC의 개요를 보여줍니다. 이 시스템은 전 세계적으로 약 3만대의 PC, 83개의 IDS, 111개의 AD 및 100개의 DNS를 모니터링합니다.

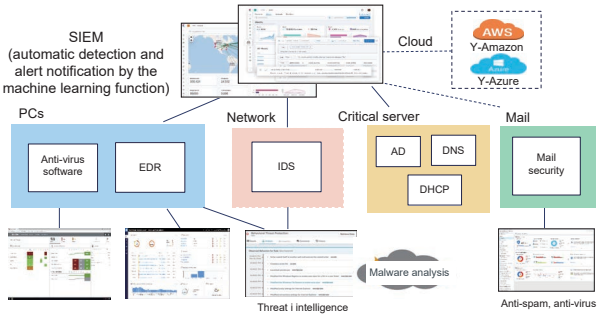

그림2 Y-SOC 개요

〈표1〉은 Y-SOC 시스템의 규모를 이벤트 수, 로그 용량, 저장 기간, 핫 노드 등으로 나타낸 것입니다.

매일 전 세계적으로 200~300GB의 로그와 5억 개의 이벤트가 수집됩니다. 분석 대상은 가장 최근 주(Week)의 데이터입니다. 유사한 사이버 공격 기법 및 관련 취약점의 존재를 조사하기 위해 3개월 동안의 데이터가 보관됩니다.

표1 Y-SOC 시스템 규모

항목	크기, 요금, 기간
데이터 수집 속도	5억-6억 로그/일
데이터 수집 크기	250-300GB/일
자주 액세스하는 데이터	지난 7일 간
자주 액세스하지 않음	지난 90일 간
가동시간 SLA	99.95%
데이터 복제	2(기본 및 복제)
핫 보유기간(Hot retention period)	30일 또는 40GB/인덱스(둘 중 더 이른 날짜)생산 혁신 창출
웜 보유기간(Warm retention period)개별 판단 및 재고 최적화	60일(연장 가능)

SOC 구축을 위한 기술

다양한 로그 수집 방법, 데이터 구조 설계, 효율적인 검색 인프

라 준비, 무단 접근 탐지 프로그램 개발, 대시보드 설계 등 SOC 구축을 위한 다양한 작업을 고려해야 합니다. 이 섹션에서는 각 단계의 기술적 특징에 대해 설명합니다.

모니터링 되어야 할 로그 검사

첫 번째 단계는 모니터링 되어야 할 로그 및 이벤트 정보를 선택하고 그 양을 추정하는 것입니다. 예를 들어, 인증 시스템은 기업에 중요하므로 AD 로그는 필수적입니다. IDS 및 DNS 로그는 해커가 무단 액세스를 얻기 위해 사용하는 명령 및 제어(command and control: C&C) 서버의 통신을 모니터링하는 데 필요합니다. 또한 각 터미널에 악성 코드가 있는지 모니터링해야 합니다. 따라서 로그 및 이벤트 정보를 모니터링하기 위해 표2에 표시된 장치를 선택했습니다.

표2 로그 및 이벤트 정보 수집 대상

카테고리	디바이스(장치)
네트워크	방화벽/IDS 및 IPS 프록시 서버 VPN 서버
사내 서버	DNS 및 DHCP 서버 등
사용자 인증	액티브 디렉토리(AD)
클라이언트 PC	엔드포인트 보호(Antivirus)
클라우드 서비스	웹 애플리케이션 방화벽 (WAF)

IEM 인프라의 설계

다음 단계는 위에서 설명한 로그를 처리하는 데 필요한 클러스터 구성 및 노드 유형을 설계하고 디스크 공간을 추정하는 것입니다. 이 경우 로그 및 시계열 메트릭(metrics) 데이터를 처리하는 데 널리 사용되는 핫 웜(Hot Warm) 아키텍처를 채택했습니다. 이 아키텍처에서는 전체 데이터는 변경할 수 없으며 시계열로 인덱싱될 수 있습니다. 따라서 각 인덱스가 특정 기간의 데이터를 보유하도록 함으로써 전체 인덱스의 수명 주기, 즉 유지 또는 삭제 여부를 관리할 수 있습니다. 이 아키텍처는 또한 클러스터의 모든 인덱스에 대한 스냅샷(snapshot)을 30분마다 생성하고 48시간 동안 유지하여 장애 및 실수로 삭제된 경우 복구를 위한 고가용성(high availability)을 보장합니다. 일래스틱서치(Elasticsearch)를 이용한 SIEM 인프라의 설계 항목은 다음과 같습니다.

- 클러스터 배치(cluster arrangement)
- 노드 유형(마스터, 데이터, 머신러닝 등)
- 노드 수 및 저장 용량
- 로그 저장 기간

로그 및 이벤트 수집

일래스틱서치(Elasticsearch)는 모니터링할 서버와 노드를 위한 다양한 로그 수집 에이전트(Beats)와 함께 제공됩니다. Y-SOC는 다음 에이전트를 사용합니다. SaaS형 서비스(Cisco WSA, Cloud WAF, Microsoft 365 등)에서는 API(Application Programming Interface: 응용프로그램 인터페이스)와 연동하거나 클라우드 스토리지(AWS S3 등)를 통해 로그를 수집합니다.

- 파일비트(Filebeat): 시스템에서 파일을 읽습니다.
- 윈로그비트(Winlogbeat): Windows 이벤트를 수집합니다.
- 메트릭비트(Metricbeat): 서버에서 메트릭 데이터를 수집합니다.
- 패킷비트(Packetbeat): 네트워크 대기 시간, 오류 및 응답 시간을 모니터링합니다.

공통 스키마 이름 정의

다양한 보안 제품 및 시스템에서 동일한 유형(예: 방화벽)이더라도 로그의 필드 이름과 형식이 동일하지 않습니다(예: 소스 주소 필드의 경우 src, client_ip, source_ip, src_ip). 그러나 SIEM은 다양한 로그 및 이벤트 정보를 연관시켜 검색하므로 모든 필드를 표준화하고 정규화해야 합니다.

Y-SOC의 경우 ECS(Elastic Common Schema)(2)를 기반으로 원본 인덱스 템플릿(yokogawa_ecs_template)을 개발하고 표준 ECS 명명 규칙에 따라 각 필드 이름을 정의하고 인덱싱했습니다. 이를 통해 서로 다른 데이터 소스 간 자동 상관관계를 만들 수 있었습니다.

동적 데이터 변환 및 보강

수집된 데이터는 저장되기 전에 분석에 적합하도록 동적으로 변환, 통합, 정규화 및 보강되어야 합니다. Y-SOC는 Logstash를 사용하여 데이터를 통합 데이터 형식으로 변환합니다. Logstash는 실시간 파이프라인 기능이 있는 오픈 소스 데이터 수집 엔진이며 입력, 필터 및 출력의 세 단계로 구성됩니다. Logstash는 다양한 기능의 플러그인을 사용할 수 있습니다(그림3).

각 플러그인의 구조와 기능은 다음과 같습니다. Y-SOC는 다중 파이프라인 처리를 사용하여 성능을 개선합니다.

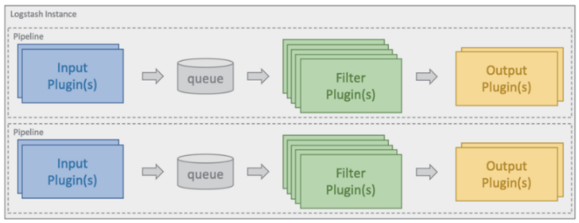

그림3 Logstash의 구성

- 입력 플러그인은 다양한 이벤트를 Logstash로 가져옵니다.
  - 파일: 파일에서 이벤트를 스트리밍합니다.
  - Beats: 다양한 Beats Agent로부터 로그를 수집합니다.
  - TCP: TCP 소켓을 통해 이벤트를 읽습니다.
  - JDBC: 트랜잭션을 Logstash 이벤트로 변환합니다.
- 필터 플러그인은 이벤트를 수정하고 조작합니다.
  - Grok: 비정형 데이터를 정형 형식으로 변환합니다.
  - Mutate: 이벤트 필드의 이름을 변경, 삭제, 교체 또는 수정합니다.
  - GEOIP: IP 주소를 검색하여 로그에 지리 정보를 추가합니다.
  - KV: 메시지를 자동으로 분석하고 키-값 쌍(key-value pairs)으로 나눕니다.
- 출력 플러그인은 이벤트 데이터를 특정 대상(destination)으로 보냅니다. 출력은 이벤트 파이프라인의 마지막 단계입니다.

표준화된 대시보드 디자인

Y-SOC의 경우 각 지역의 보안 상태를 집합적으로 보여주는 최상위 대시보드, 각 지역의 보안 상태를 보여주는 지역별 알림 대시보드, 각 장치에 대한 세 가지 레벨 정보를 보여주는 상세 대시보드의 3가지 대시보드를 개발했습니다(그림4).

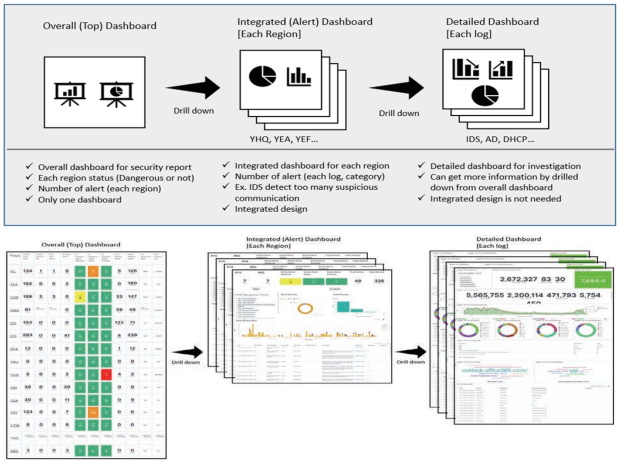

그림4 보안 대시보드

최상위 대시보드는 각 지역에서 얼마나 많은 무단 접근 및 악성 코드 IDS, AD, PC가 탐지되었는지와 그 해결 여부를 보여줍니다. 지역별 경보 대시보드는 IDS, AD, DNS 및 PC의 시계열 동작을 보여줍니다. YSOC 대시보드는 모든 데이터가 세분화된 레이어(layer) 구조로 설계되어 각 장치의 로그를 추가로 드릴다운하여 이상 원인을 식별할 수 있습니다.

SOC 사용자 규칙 작성

SOC를 운영하기 위해서는 다양한 역할을 가진 다양한 구성원이 필요합니다. 여기에는 각 지역의 총괄 책임자(general manager), SOC 개발자, 보안 분석가, 인프라 운영자 및 보안 담당자가 포함됩니다. SOC 시스템 및 대시보드 인증을 위해 PingFederate(클라우드 애플리케이션에 접근하기 위한 인증과 사내 시스템 접근을 위한 인증을 연결하는 SSO 제품)를 사용합니다. 각 사용자의 역할에 따라 접근 권한이 부여됩니다.

로그 및 이벤트 수집 및 탐지 논리(DETECTION LOGIC) 개발

사이버 보안 방어를 위해서는 침입 초기 단계에서 사이버 공격을 탐지할 수 있어야 합니다. 침입 후에는 피해가 확산되는 것을 방지하는 것이 중요합니다. 따라서 사이버 공격 추적 및 탐지 방법을 포함하는 다양한 유형의 사이버 위협 인텔리전스(cyber threat intelligence: CTI)를 사용합니다. 무단 접근에 사용되는 IP 주소, URL, 도메인을 탐지 로그와 자동 대조할 수 있는 시스템을 구축했습니다.

각 장치에 대한 무단 액세스 로그 데이터를 감지하기 위해 JPCERT/CC(3) 및 기타 기관의 자료를 참조하여 감지 규칙을 개발했습니다(표3).

표3 무단 접근 탐지 프로그램 예

PC	• mimikatz.exe 및 pwddump.exe와 같은 자격 증명 덤프 실행 파일을 탐지합니다. • 지원되지 않는 스크립트 등의 실행을 감지합니다.
IDS	• 취약점과 관련된 스파이웨어, 바이러스 및 위협 이벤트를 탐지합니다. • 의심스러운 DNS 쿼리 및 네트워크를 검색합니다.
DNS	• 악성 Tor(TCP/IP 연결 경로 익명화) 및 다크 웹에 대한 모든 액세스를 탐지합니다. • DNS 임계값을 초과하는 의심스러운 도메인 또는 호스트 이름 및 인코딩된 FQDN(정규화된 도메인 이름)을 탐지합니다

AD와 관련하여 JPCERT/CC(4) 및 Microsoft사에서 권장하는 이벤트를 모니터링합니다. 예를 들어 특정 권한(privileged righ)t으로 AD를 운용하는 경우 감사 로그(audit log)를 운용 이력과 비교합니다. 짧은 시간에 많은 수의 로그인 성공 또는 실패가 발생하면 시스템은 이를 의심스러운 동작으로 보고 경고를 발행하고 사용자에게 확인을 요청합니다.

이벤트를 감지하기 위해 일래스틱서치(Elasticsearch)의 머신러닝(ML) 기능을 활용합니다. 분석 애플리케이션은 주로 Python으로 개발되며 Jenkins으로 주기적으로 실행하여 다양한 CTI의 침해 지표(indicator of compromise: IOC) 정보와 분석을 매칭합니다(그림5). 비지도(unsupervised) 머신러닝 기능은 시계열 모델링을 기반으로 임계값(thresholds)과 이상(anomaly) 값을 자동으로 설정할 수 있습니다. 이 기능은 사고로 이어질 수 있는 행동을 감지하는 목적으로도 사용됩니다. 이는 통신 대상, 로그인 횟수, 데이터 업로드, 의심스러운 DNS 쿼리와 같은 행동 특성에서 식별할 수 있습니다. 분석 결과는 Alert Index(경고 인덱스)에 저장되어 Y-SOC의 보안 분석가에게 통보됩니다. 이러한 탐지 프로그램은 새로운 위협이 보고될 때마다 지속적으로 수정됩니다.

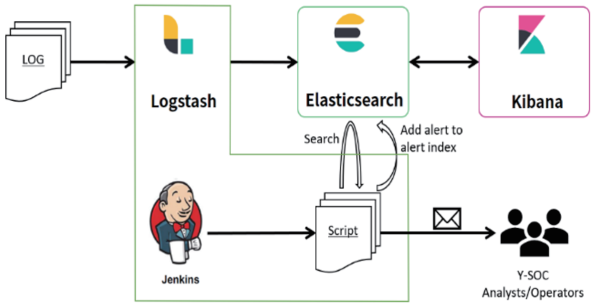

그림5 Python 스크립트의 실행 환경

CSIRT에 의한 사고 대응 관리

SOC가 경보를 발령한 후에는 즉시 상황을 조사하고 조치를 취해야 합니다. 따라서 각 지역의 보안 담당자와 원활하게 협력할 수 있도록 사고 대응 워크플로를 구축했습니다. 워크플로는 다음과 같습니다(그림6).

(1) 분석 엔진은 자동으로 이상을 감지하고 '카테고리/레벨 위협 매트릭스(threat matrix)'를 기반으로 각 경고(alert)의 중요성을 결정합니다.

(2) Alert Index(경고 인덱스)에 경보 정보가 수집되어 Y-SOC 팀에 자동으로 통보됩니다(일 평균 50~70개 정도).

(3) Y-SOC 팀의 보안 분석가는 각 경보가 true-positive(실제공격)인지 false-positive(오 탐지)인지를 판단합니다. 이 결정은 아래 단계를 따릅니다.

- 다양한 로그 소스를 분석하고 상관 관계를 분석하여 사실 여부를 판단합니다.
- 내부 통신 트래픽을 검사합니다.
- 다양한 CTI(Virus Total, MineMeld, 온라인 위협 인텔리전스 플랫폼, 온라인 샌드박스)를 이용하여 외부 통신 및 파일을 분석합니다.

(4) 보고해야 할 사고(incident)을 파악한 후 사건 내용, 현장 조사 방법, IoC, 완화를 위한 조치(mitigation measures) 등을 지역별 담당자에게 통보합니다.

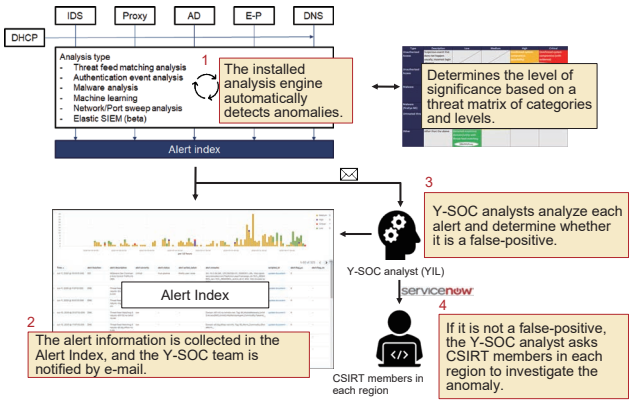

그림6 사고 워크플로

사이버 공격(cyberattacks)을 분석하기 위해 사이버 공격 전술과 기법을 공격(attack) 라이프사이클별로 체계화한 프레임워크인 MITRE ATT&CK(5)를 사용합니다. 이 프레임워크를 통해 사용된 공격 방법과 소프트웨어를 분석하고 공격 그룹을 추정하고 탐지 방법을 수정하고 완화를 위한 대응 조치(mitigation measures)를 작성합니다. 또한 MITRE ATT&CK Navigator 및 기타 도구를 사용하여 사이버 공격 전술을 예측합니다.

각 사건(incident)은 ServiceNow ITSM을 사용하여 티켓팅되며 사고(incident)의 상태(발생 횟수, 취한 조치 수, 취하지 않은 조치 수, 응답 시간)가 관리됩니다. 또한 분기별로 지역별 사고(incident) 건수 변화 및 공격 벡터(Attack Vector: 무단 접근 경로 및 방법)를 분석하여 탐지 규칙 및 IT 인프라의 보안성을 향상시킵니다(그림7).

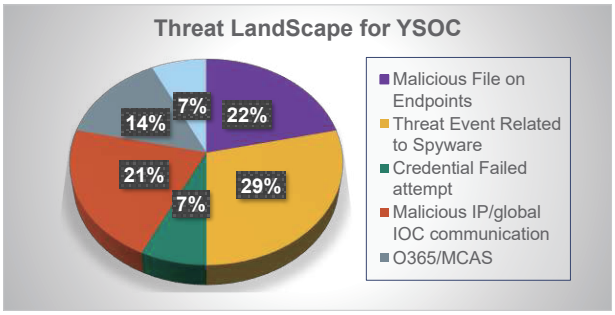

그림7 Y-SOC 위협 환경

클라우드 서비스 보안 모니터링

Yokogawa는 Amazon AWS 및 Microsoft Azure와 같은 퍼블릭 클라우드 서비스를 적극적으로 사용하여 내부 시스템 및 외부 서비스에서 DX를 추진합니다. 외부 공용 서버의 경우 웹 애플리케이션 보안을 위한 개방형 커뮤니티인 OWASP의 핵심규칙집합(core rule set: CRS)에 따라 WAF 로그를 수집하고 WAF 정책을 사용자에 맞게 설정합니다. 이는 과탐지(over-detection)로 인한 통신 차단(communication blocking)을 방지합니다.

또한 Yokogawa의 Sushi Sensor(스시 센서)와 클라우드 IoT 허브를 '외부 DX' 서비스로 활용하여 컨테이너 애플리케이션(container application)을 개발하고 클라우드 네이티브 IoT 서비스를 시작했습니다. 서비스의 보안성을 확보하기 위해 'Azure Security Center(Azure 보안센터)'를 사용하고 있으며, 75% 이상의 보안 점수를 유지하고 있습니다.

미래 전망(FUTURE DEVELOPMENTS)

우리는 사고 관리(incident management), 취약성 대응(vulnerability response) 및 위협 정보(threat information)에서 ServiceNow SecOps와 협력할 계획입니다(그림8).

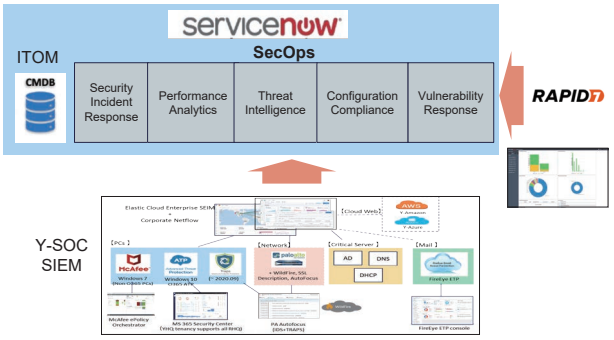

그림8 ServiceNow와의 협업

사고 관리(incident management)와 관련하여 SIEM을 각 보안 제품과 통합하여 사고(incident)의 발견, 조사, 영향 범위 식별, 억제

및 복구(SOAR: 보안 오케스트레이션, 자동화 및 대응)와 같은 워크플로를 자동화할 수 있습니다.

취약성 평가를 위해 ServiceNow는 'Rapid 7 Insight VM' 취약성 평가 소프트웨어로부터 취약성 보고서를 수신하고 이를 ServiceNow의 CMDB(Configuration Management Database: 구성 관리 데이터베이스)와 교차 점검하여 패치 대응(patch response) 담당자를 지정하고 대응 상태를 관리하며 사이버 공격에 대한 취약성의 존재 여부를 확인합니다.

위협 인텔리전스를 위해 시스템이 자동으로 사이버 위협 인텔리전스 정보를 참조하도록 하고 있습니다.

외부용 IoT 클라우드 서비스의 경우 Azure Security Center 및 ServiceNow와 연계하여 사고 대응 워크플로를 개선하고 보안 상황을 파악할 예정입니다. 또한 e-RT3(PLC) 등의 제어 장치에서 로그를 수집할 계획입니다.

결론

본 백서(paper)에서는 SIEM과 ML을 활용하고 CTI와 연계하여 SOC를 효율적으로 개발 및 운영할 수 있음을 설명하였습니다. Yokogawa는 고객 사이트의 엣지 서버(edge server)와 클라우드 서비스를 연결하여 IT와 OT의 통합을 강화하고 시스템을 외부 OT SOC 서비스로 확장할 계획입니다.

이를 위해 모니터링 기술을 강화할 것입니다. 또한, 미국 국토안보부의 사이버보안 및 기반시설 보안국(CISA)(7) 및 위협 및 탐지 정보 교환 협약(STIX/TAXII)(6)에 따른 기타 정부 조직 및 전문 조직들과 사이버 위협 정보를 공유하는 시스템을 구축할 것입니다. 우리는 또한 'ATT&CK for ICS'와 같은 제어 시스템에 대한 위협에 관한 지식을 확장하는 데 기여할 것입니다.

참고문헌

(1) IDC Japan, "Announcement of the 2020 IIoT/OT security measures survey on Japanese enterprises," 2020, https://www.idc.com/getdoc.jsp?containerId=prJPJ46173120 (in Japanese) (accessed on April 30, 2021)
(2) Elastic Common Schema (ECS), https://github.com/elastic/ecs (accessed on April 30, 2021)
(3) JPCERT/CC, "How to use and analyze logs in dealing with advanced cyberattacks," 2016, https://www.jpcert.or.jp/research/aptloganalysis.html (in Japanese) (accessed on April 30, 2021)
(4) JPCERT/CC, "How to use logs to detect and counteract attacks on active directory," 2017, https://www.jpcert.or.jp/research/AD.html (in Japanese) (accessed on April 30, 2021)
(5) MITRE ATT&CK, https://attack.mitre.org/ (accessed on April 30, 2021)
(6) STIX/TAXII, https://oasis-open.github.io/cti-documentation/ (accessed on April 30, 2021)
(7) CISA, Automated Indicator Sharing, https://www.cisa.gov/ais (accessed on April 30, 2021)