IIoT SOC 서비스

코이즈미 세이이치 (Seiichi Koizumi)[*1]　　*시오자키 테츠오 (Tetsuo Shiozaki)*[*1]

고객이 디지털 전환(DX)을 촉진할 수 있도록 돕기 위해, Yokogawa는 사물 인터넷 (Internet of Things, IoT) 클라우드 서비스인 Yokogawa Cloud를 제공해 오고 있습니다. 우리는 또한 DX 서비스를 안전하게 만들기 위해 노력하고 있습니다. Yokogawa 사내 보안 시스템(Yokogawa 보안 모니터링 센터: Y-SOC)의 운영을 통해 습득한 노하우를 활용하여 IT/OT 보안 모니터링 서비스를 개발했습니다. 본 글에서는 IT/OT 융합의 기술적 동향을 설명하고, Yokogawa의 IT/OT 통합 SOC 서비스의 적용 사례를 소개합니다.

도입

디지털 전환(DX)을 향하여 클라우드 서비스가 확대되고 운영 기술(OT)과 정보 기술(IT)이 통합되고 있습니다(IT/OT 융합). IT와 OT의 영역은 전통적으로 별도로 관리되었으나, OT데이터를 관리 정보 리소스로 효과적으로 사용하기 위해 네트워크가 점점 상호 연결되고 있습니다. 그림 1은 통합된 IT/OT 네트워크의 아키텍처를 보여줍니다[(1)].

아울러, 방대한 양의 OT 데이터를 효율적으로 관리하고 분석하기 위해 클라우드 서비스의 확장성, 데이터 레이크 및 머신 러닝기능이 필요합니다. 이에 따라 이제는 IT 네트워크를 건너뛰어 클라우드 시스템에 직접 연결되는 OT 네트워크의 수가 점점 늘고 있습니다.

IoT 클라우드 서비스인 Yokogawa Cloud는 로그 및 이벤트 모니터링, 취약성 진단, 액세스 제어, 데이터 암호화 등 다양한 보안 조치가 수반되어 있습니다. 한편 사내 OT 네트워크는 보안 위협에 직면해 있는데, 이는 인터넷에 접속하여 범용 OS 제품을 사용하기 때문이며, 인터넷과 범용 OS 제품 둘 다 보안에 취약합니다.

IDC Japan의 "2021년 일본 내 기업을 대상으로 한 IoT/OT 보안 조치에 대한 조사"[(2)]에 따르면, 36.4%의 기업이 자사의 플랜트 및 시스템과 관련하여 보안 사건이나 사고를 경험했습니다(전년도에는 34.4%). 거의 절반에 가까운 기업(47.7%)이 자사의 IIoT/OT 보안 조치가 충분하지 않다고 생각하고 있습니다. 본 글에서는 IT/OT 융합의 동향에 대해 설명하고, Yokogawa의 OT 보안 운영 센터(OT SOC)와 센터의 서비스 사례를 소개합니다.

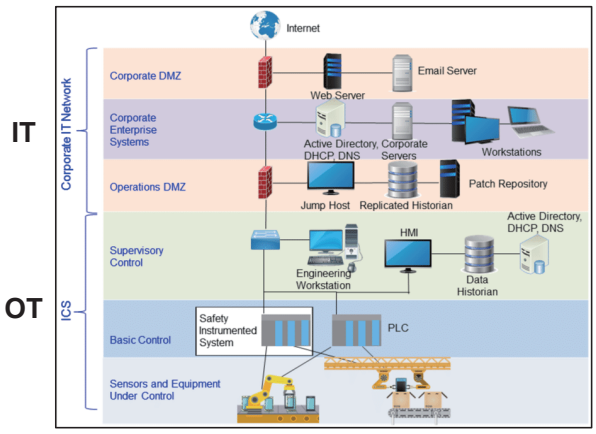

그림1 통합 IT/OT 네트워크의 아키텍처

*1 디지털 솔루션 본부 산하 DX 플랫폼 센터
DXP 기획부

IT/OT 융합의 동향

배경

지속 가능한 개발 목표(SDGs)의 추진 필요성으로 인해, 프로세스 산업의 비즈니스 환경은 녹색 에너지로의 전환과 탄소 배출권의 도입 등 큰 변화를 겪고 있습니다. 단순히 IT 도메인이나 OT 도메인을 개선하는 것만으로는 이러한 변화에 대한 대응으로 충분하지 않습니다. 따라서 두 도메인의 경계를 초월하는 IT/OT의 융합이 확산되고 있습니다. 이전에는 플랜트 제어 장비 계층과 전사적 자원 관리(enterprise resource planning, ERP) 및 고객 관계 관리(customer relationship management, CRM)와 같은 IT 시스템의 계층이 서로 분리되어 있었습니다. 클라우드 컴퓨팅 및 엣지 컴퓨팅과 같은 유연한 IT 기술을 사용하여 IT 데이터와 OT 데이터를 데이터 레이크에 저장함으로써 IT 또는 OT 제어만으로는 처리하기 어려운 플랜트 운영 작업을 최적화할 수 있습니다. 이를 통해 플랜트들은 CO_2 배출 제한에 따른 제조 일정 조정과 에너지 소비 모델을 활용한 디지털 트윈 기술을 갖춘 유틸리티 제어의 최적화 등 비즈니스 환경의 변화에 자동적으로 적응할 수 있습니다.

IT/OT 융합에도 불구하고, 원자재에서 중간재 및 최종 제품에 이르기까지 가치 사슬 전체에서 탄소 배출권 및 CO_2 배출량 감소 등의 일부 문제는 단일 기업의 역량을 넘어섭니다. 하나의 해결책으로 관심을 끄는 접근 방식은 기업의 경계를 넘어선 복합 시스템(system of systems, SoS)협업을 통해 새로운 비즈니스 가치를 유연하게 창출하는 것입니다[3]. 따라서 IT/OT 융합의 적용 분야는 더욱 확대될 것으로 예상됩니다. 그림 2는 Yokogawa의 SoS 개념입니다[4].

IT/OT 융합을 지원하는 기술 및 관련 쟁점

ISA-95[5] 및 Purdue Model[6]은 OT 제어 장치와 IT 시스템을 연결하는 데 사용되는 경우가 많습니다. OT 제어 장치로는 분산 제어 시스템(distributed control systems, DCS)과 프로그래머블 로직 컨트롤러(Programmable Logic Controller, PLC)등이 있으며, IT 시스템에는 ERP, 공급망 관리(supply chain management, SCM) 및 제조 실행 시스템(manufacturing execution systems, MES) 등이 있습니다. 이러한 모델은 산업용 데이터, 실시간 성능, 고가용성(high availability), 안전성(safety) 및 안정성(stability)에 대한 표준 지원과 같은 OT 도메인 내 기능(functional) 및 비 기능(non-functional) 요구 사항을 충족합니다. 이러한 모델들이 온프레미스(on-premises) IT 시스템을 맡기는 하지만, 클라우드 컴퓨팅과 엣지 컴퓨팅[7]을 통합하는 새로운 IT/OT 융합 모델도 확산되고 있습니다.

이 새로운 IT/OT 융합 접근 방식은 고객에게 다양한 이점을 제공하는데, 즉 프로세스 산업 전반적 운영의 시각화와 산업용 IoT(IIoT), AI, 디지털 트윈 기술을 이용한 개선 대책의 개발, 소프트웨어 정의 기술(software defined everything, SDx)과 가상 컨테이너를 활용한 유연한 자동 제어, IT 서비스 관리(ITSM)와 운영 지원 시스템/비즈니스 지원 시스템(OSS/BSS)의 통합을 통해 제조 제어를 위한 반복 서비스(recurring services)의 제공 등이 있습니다. IT/OT 융합은 제조업의 DX를 위한 추진력이 되었습니다.

부정적인 측면에서는, 기존의 IT 또는 OT 전용 취약성 대책으로는 다룰 수 없는 위협이 부상하고 있습니다[8]. 해결해야 할 구체적인 기술 문제로는, 클라우드 연결로 인한 대응책이 필요한 항목의 증가, 일관성 없는 IT 및 OT 관리 시스템과 서로 다른 보안 정책의 공존, 계층적 네트워크 보안의 제한된 성능, 다양한 장치 및 프로토콜 관리의 어려움 등이 있습니다.

IT 보안과 OT 보안의 차이

IT 보안과 OT 보안 사이에는 몇 가지 차이가 있습니다. OT SOC 설계 시 이러한 차이를 반드시 고려해야 합니다.

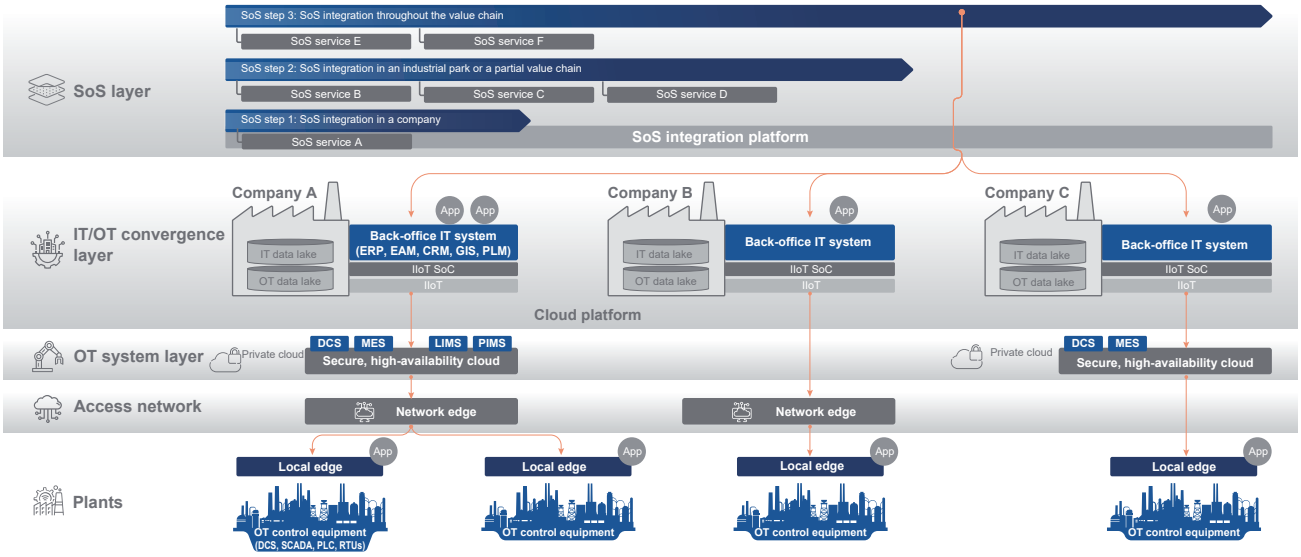

그림2 IT/OT 융합 및 복합 시스템 (system of systems)

첫째, IT와 OT는 세 가지 보안 요소인 기밀성(confidentiality), 무결성(integrity) 및 가용성(availability)의 우선순위가 다릅니다.

IT 도메인에서는 인터넷을 통한 악성 소프트웨어(malware), 피싱(phishing), 데이터 유출(Data Loss), 무단 액세스(unauthorized access) 및 그 밖의 다양한 위협으로부터 시스템을 보호해야 하기 때문에 기밀성이 우선됩니다. OT 도메인에서 주요 위협은 핵심 프로세스 제어 장비, 안전 시스템, 생산 라인의 탈취(takeover)입니다. 그래서 OT 도메인의 최우선 순위는 가용성(availability)이며, 모니터링은 안전, 안정성 및 생산성에 초점을 둡니다. OT 자산, 로그 및 이벤트 정보를 완벽하게 시각화하고 관련 이벤트에 대한 조사 및 추적이 가능한 모니터링 인프라가 필요합니다.

전력, 정유 및 수 처리를 위한 산업 제어 시스템에서 복잡한 물리적 프로세스는 오랜 세월 동안 축적된 경험을 바탕으로 운영됩니다. 따라서 악의적인 제삼자에 의해 초래된 것이 아니라 할지라도 약간의 결함이나 비정상적 패턴으로 인해 계획되지 않은 가동 중단(shutdowns)이 발생할 가능성이 높습니다. 위험을 식별하고 분석하며, 사고를 예방하기 위해서는 프로세스 상의 편차를 점검하고, 잠복된 요인으로 인한 비정상적 장치 거동을 억제하며, 기존 시스템과 호환되지 않을 수 있는 새로운 장치에 대한 모니터링이 중요합니다[9].

OT SOC는 다양한 장치의 작동 상태를 모니터링하고 이상 징후를 감지하여 안전을 보장해야 함은 물론, 이벤트 발생으로부터 통지까지의 시간 그리고 그 내용의 측면에서 높은 서비스 수준 협약(service level agreement, SLA)을 충족해야 합니다.

둘째, 준수해야 할 보안 표준이 다릅니다. ISO27001, NIST, PCI-DSS는 IT 시스템에 대한 것이며, 제어 시스템에 몇 가지 다른 표준이 적용됩니다(그림 3). North American Electric Reliability Corporation critical infrastructure protection(NERC CIP)는 자세한 OT 데이터를 요구합니다. 산업 제어 시스템용 사이버 보안 조치에 대한 국제 표준인 ISA/IEC 62443은 다른 많은 표준에서 언급되고 있습니다. OT 보안에 대해 모니터링 할 때에는 이러한 표준과 일관성을 보장해야 합니다. 그림 4는 IEC 62443 시리즈의 구조를 보여줍니다.

그림3 OT 보안에 대한 표준

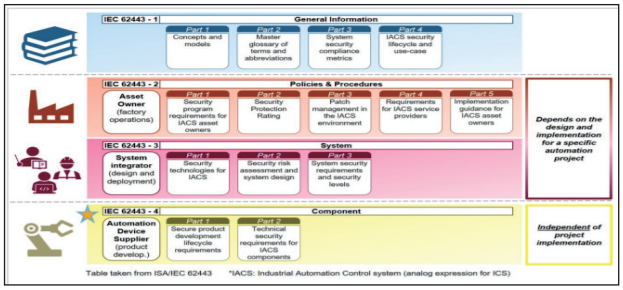

그림4 IEC 62443 series[10]의 구조

셋째, 통신 프로토콜이 다릅니다. OT 시스템은 장비의 유형에 따라 다양한 프로토콜(Modbus, MQTT, OPC UA)과 산업용 이더넷(PROFINET Ethernet/IP)를 사용하며, 일부 로그 형식은 공개되지 않습니다. 따라서 OT SOC에는 다양한 데이터 세트를 수집, 분석, 시각화하기 위한 다양한 렌즈 세트(로그, 이벤트, 네트워크 및 이벤트 시퀀스를 모니터링하기 위한 메커니즘)가 딸려 있습니다. 경우에 따라서는 이벤트 데이터 및 로그를 수집하고 해석하는 방법에 대해 제어 장치 제조업체와 협상할 필요가 있습니다.

넷째, 고객 지원도 다릅니다. IT 시스템은 정보 시스템 부서에서 관리하는 경우가 많으며 단일 창구가 있습니다. 반면에 OT SOC는 OT 시스템이 데이터에 직접 액세스하여 분석하고 문제의 원인을 파악하는 현지 OT 엔지니어에 의해 작동되기 때문에 특수 프로세스 제어 장비, 안전 시스템 및 생산 라인에 익숙한 OT 엔지니어의 도움이 필요합니다. 이러한 이유로, OT SOC 보안 엔지니어는 현지 OT 엔지니어와 신뢰 관계를 구축해야 하고 현지 언어로 의사소통할 수 있어야 합니다.

IT/OT 보안에 대한 Yokogawa의 접근 방식

보안 모니터링 서비스에 있어서 Yokogawa의 노력

Yokogawa는 2019년에 Yokogawa 보안 운영 센터(Security Operation Center, Y-SOC)를 구성했으며, 이는 Yokogawa의 전 세계 16개 거점에 있는 다양한 IT 장비를 모니터링 합니다. 모니터링 대상에는 IDS, AD, PC, DHCP, DNS와 같은 내부 IT 장치뿐만 아니라 Amazon Web Services 및 Microsoft Azure의 웹 애플리케이션 방화벽(WAF)을 비롯한 클라우드 환경도 포함되며, 실시간 분석을 위해 하루 당 5~6억 개의 이벤트 로그를 수집합니다[11].

Y-SOC는 클라우드 기반 보안 정보 및 이벤트 관리(SIEM)시스템을 갖추고 있으며, 사이버 위협 인텔리전스(CTI) 및 머신 러닝을 기반으로 탐지 프로그램을 개발하고, ServiceNow SecOps와 SecOps 커넥터를 통합하며, 사고 감지부터 방어까지 작업을 자동화합니다(보안 오케스트레이션, 자동화 및 대응: SOAR). 모니터링 대상은 현재 IoT 게이트웨이, PLC, 협업 정보 서버 및 원격 FAT와 같은 OT 도메인을 포함하도록 확대되었습니다. 그림 5는 Y-SOC의 구조를 보여주며, 그림 6은 자동화된 사고 대응의 흐름을 보여줍니다. Y-SOC가 사고를 감지하면[1] ServiceNow SecOps는 자동으로 사이버 위협 정보를 참조하여[2] 공격을 차단하며[3], CSIRT에 임무 수행을 요청하고[4] 사고 내용을 검토합니다[5].

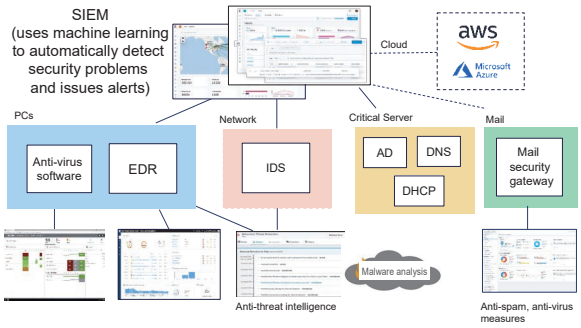

그림5 Y-SOC의 구조

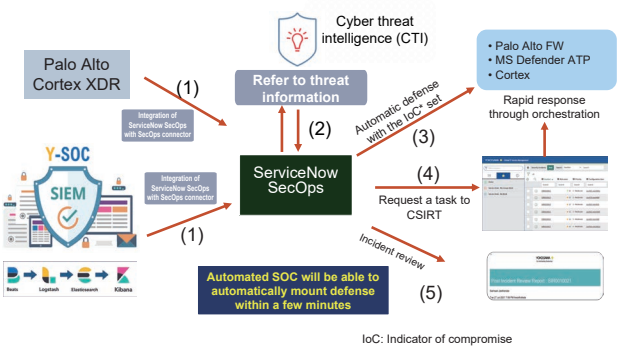

그림6 사고 대응 및 자동화된 보호 업무 흐름

또한 센터는 각 모니터링 센터에서 고객의 보안 상태를 모니터링하는 OT SOC/네트워크 운영 센터(network operations center, NOC)서비스를 제공합니다. 통합 위협 관리 장치(Unified threat management devices(예: FortiGate, NOZOMI Networks Guardian)) 및 통신 분석 전용 모니터링 서버가 플랜트 네트워크의 주요 위치에 설치됩니다. 사고 발생 시 센터는 탐지 내용 및 통신 상태를 보고하고 대응 방법에 대한 조언을 제시합니다.

IT/OT-통합 SOC

Yokogawa는 Y-SOC의 사이버 보안 전문 지식을 각 지역 사무소에서 OT SOC 운영과 통합한 SOC 서비스를 확대해 왔습니다.

이 서비스는 지역 SOC 엔지니어의 역량을 결집하여 Y-SOC의 역량으로 고객이 머신 러닝 기반 탐지 프로그램을 개발하고 보안성을 분석할 수 있도록 탁월한 지원을 제공함으로써 보안 위협을 보다 효율적으로 분석할 수 있도록 지원합니다.

Y-SOC의 클라우드는 고객 OT 시스템에서 다양한 이벤트 및 로그 정보를 수집하며, 그 대시보드에서는 해당 정보를 통합된 방식으로 보여줍니다. CTI 및 머신 러닝에 의해 경고가 감지되면 지역 SOC 엔지니어에게 자동으로 경보가 발령되고, 그런 다음 이 엔지니어는 다양한 제품 콘솔과 도구를 사용하여 경고 내용을 상세히 분석합니다. 고객용 대시보드 스크린뿐만 아니라 Y-SOC와 지역 SOC 간 사고 업무 흐름은 이슈 및 프로젝트 관리에 사용되는 오픈 소스 프로그램인 Jira로 개발됩니다.

지역 SOC 엔지니어는 Y-SOC의 사이버 보안 지식을 최대한 활용할 수 있으며, 지역 고객과의 긴밀한 협력 작업을 통해 그들에게 세심한 서비스를 제공할 수 있습니다. 그림 7은 Y-SOC와 지역 SOC 간 협업을 보여줍니다.

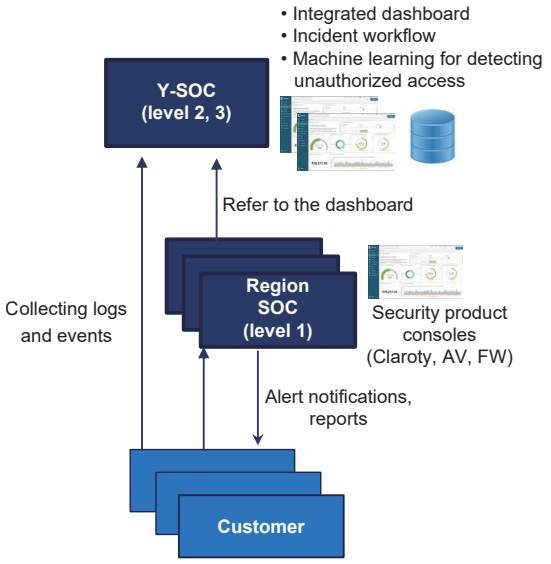

그림7 Y-SOC 와 지역 SOC 간 협업

OT SOC 모니터 링의 예

OT SOC 모니터링의 한 가지 예가 아래에 제시되어 있습니다. 그림 8은 OT SOC 모니터링 네트워크의 구성을 보여주며, 그림 9는 OT SOC의 아키텍처를 보여줍니다.

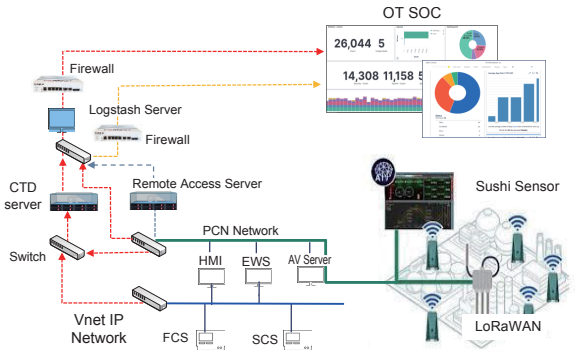

그림8 OT SOC 모니터링 네트워크의 구성

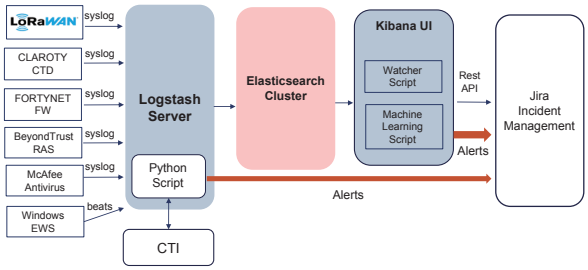

그림9 OT SOC의 아키텍처

표 1 OT SOC 사용 사례와 보안 표준 간 관계

No.	사용 사례	설명	ICS / ISO 표준	보안 항목
1	IoT 장치 (Sushi sensor 등) 모니터링	Modbus 및 기타 통신을 모니터링하여 인가/승인되지 않은 장치를 탐지합니다. LoRaWAN 게이트웨이 로그를 수집하고, 센서의 배터리 수준을 모니터링합니다.	ISO/IEC 19770-1, IEC 62443	자산 관리
2	방화벽 정책 모니터링	인바운드/아웃 바운드 패킷, 방화벽 정책 변경 사항 및 그 유효성, 그리고 결과 구성을 모니터링합니다.	ISO/IEC 19770-1, IEC 62443	규정 준수 관리
3	다운로드 및 구성 변경 모니터링	모든 노드 (EWS/FCS)의 변경 사항을 추적하고 경보를 발령합니다.	ISO/IEC 19770-1, IEC 62443	자산 관리
4	바이러스 탐지	바이러스 감염에 대한 경보 정보를 모니터링합니다. USB 플래시 드라이브의 무단 연결을 모니터링합니다	IEC 80001-2-8: 2016, ISO/IEC 27035, ISO 27039	위험 관리
5	원격 액세스 서버 모니터링	유지 보수를 위해 수행되는 원격 액세스를 모니터링합니다. 유지 보수 데이터의 다운로드 및 업로드를 모니터링합니다.	IEC 62827-3: 2016, ISO/IEC 18028-4:2005	원격 액세스 보안
6	OT 프로토콜 모니터링	OT 장비 모니터링을 위한 지속 위협 탐지 (CTD)를 실행합니다. OT 네트워크에서의 지도 생성 및 OT 프로토콜 상태를 모니터링 합니다.	ISO/IEC 19770-1, IEC 62443	자산 관리

다양한 장치로부터의 시스템 로그는 Logstash 서버(로그 수집 및 관리를 위한 Elastic NV의 tool)로 전송됩니다. Windows 이벤트는 Level 2 프로세스 네트워크 서버(예: EWS)에서도 수집됩니다. 사이버 위협 정보(CTI)를 참조하여, Python 스크립트는 무단 액세스 및 비정상적 통신을 자동으로 감지합니다. 그런 다음 Hot-Warm 아키텍처가 있는 Elasticsearch Cluster에 의해 데이터가 관리되기 때문에 시계열(time series)데이터의 손쉬운 액세스와 축적이 모두 충족됩니다. Watcher 스크립트와 머신 러닝 스크립트는 누적된 데이터를 처리한 다음 Kibana(시각화 도구)가 대시보드에 이를 표시합니다. 사고가 감지되면 Jira가 API를 통해 자동으로 티켓을 생성하여 SOC 레벨 1에 있는 SOC 엔지니어에게 전달합니다. 이 경우에 우리는 OT 시스템의 가용성에 우선순위를 두고, 가능한 위험사례(사용사례)를 파악하며, 각 사용 사례에 대하여 위험 우선순위와 알림 시간을 서비스 수준 목표(service level objectives, SLO)로 설정합니다. 우리는 또한 IEC/ISO 표준과의 일관성도 확인합니다. 표 1은 우선 순위가 매겨진 사용 사례와 특정 모니터링 조치의 예를 보여줍니다.

각 사례의 분석결과는 중앙에서 대시보드로 모니터링할 수 있습니다. 이를 통해 OT 네트워크 내 각 노드의 동작, 각 장치와 이벤트 간 상관 관계, IT 및 OT 보안을 종합적으로 시각화할 수 있습니다. 그림 10은 Kibana UI를 사용한 OT SOC 대시보드 스크린의 예를 보여줍니다.

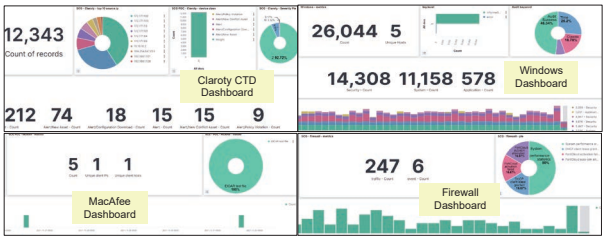

그림10 OT SOC 대시보드 스크린

우리는 사고가 감지된 이후 업무 흐름의 속도를 높였습니다. 사고 티켓은 Jira와 ServiceNow가 API를 통해 자동으로 생성합니다.

- SOC 레벨 1의 지역 SOC 엔지니어는 보안 모니터링, 장비 상태 점검 및 고객과의 연락을 담당합니다. 이들은 또한 사고 정보가 "참(true)" 또는 "거짓 긍정(false positive)"에 해당하는지 여부를 판단합니다. 참 긍정 (True positive)사고 내용을 SOC 레벨 2로 전송합니다 (escalated).
- SOC 레벨 2의 엔지니어는 관련 정보를 바탕으로 위협의 잠재성을 분석하고, 사고 티켓을 발행할 필요가 있다고 판단되면 사고 정보를 레벨 3로 에스컬레이션 합니다.
- SOC 레벨 3의 엔지니어는 사고에 대하여 그 처리, 추가 조사 및 복구 조치에 관한 보고서를 작성합니다.

업무 흐름에 있어서 일련의 단계는 API를 통해 Elastic Cloud에 연결된 Jira에 의해 자동으로 처리됩니다. 현지 레벨 1의 엔지니어는 고객 대시보드를 사용하여 고객에게 그 결과를 상세히 설명합니다. 각 사고 티켓의 상태가 시각화 되고, SLA 준수 상태가 명확히 표시됩니다. 그림 11은 OT SOC의 엔지니어 지원 시스템을 나타내고, 그림 12는 사고 티켓과 관련 대시보드 스크린의 예를 보여줍니다.

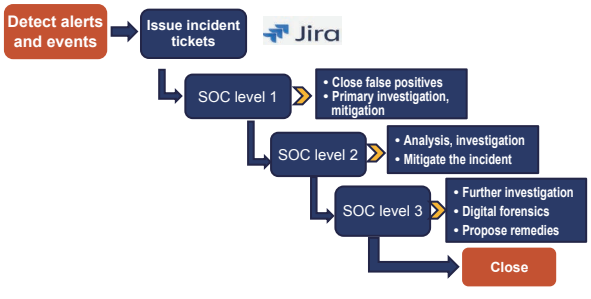

그림11 OT SOC의 엔지니어 지원 시스템

그림12 사고 티켓과 관련 대시보드 스크린의 예

향후 개발

우리는 Yokogawa Group의 보안 서비스 역량을 강화할 계획입니다. Y-SOC와 각 지역 SOC(일본, 싱가포르, 인도, 루마니아, 네덜란드, 태국) 간 협업을 촉진할 것입니다. Y-SOC의 사이버 보안 분석 노하우를 활용하여, 우리는 고급 IT/OT 보안 서비스를 전 세계적으로 공급할 것입니다.

Yokogawa는 자사의 OT 제품 외에도 다른 회사의 OT 제품으로 모니터링을 확대하고, 산업 제어 시스템용 MITRE ATT&CK[12]을 포함한 제어 시스템에 대한 사이버 보안 인텔리전스 개발을 목표로 하고 있습니다. 그림 13은 글로벌 보안 운영의 조직 구조를 보여줍니다.

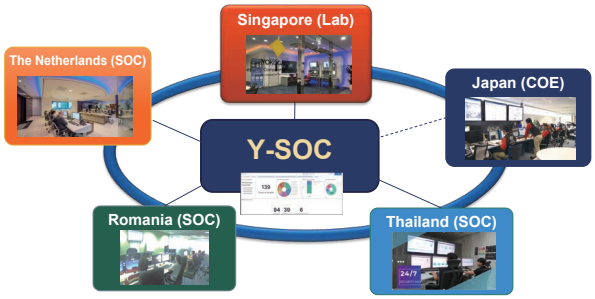

그림13 글로벌 보안 운영의 구조

결론

본 글에서는 IT와 OT의 지속적인 융합을 고려하여 보안 모니터링 서비스에 대한 Yokogawa의 접근 방식을 설명했습니다.

IT와 OT는 시스템 가용성 및 사고 대응 측면에서 서로 다릅니다. Yokogawa는 고객의 IT/OT 환경에 대한 고객과의 인터뷰를 바탕으로, 위험에 따른 로그 및 이벤트 정보의 수집과, 머신 러닝을 활용한 탐지 프로그램의 개발, 그리고 고객 자산의 모니터링에 대한 방법을 제시할 것입니다. 각 지역의 SOC 엔지니어들과 협력하여, 우리는 또한 사고 대응 조치나 우회 계획(workaround plans) 제시 및 사고 대응 교육을 제공하는 등 고객 맞춤형 DX 보안 서비스를 개발할 계획입니다.

참고문헌

(1) Edward Colbert, Daniel T. Sullivan, Alexander Kott, “Cyber-Physical War Gaming,” Journal of Information Warfare, Vol. 16, No. 3, 2017, pp. 119-133
(2) IDC Japan, “IDC Japan Releases Results of 2021 Survey on IoT/OT Security Measures for Enterprises in Japan,” 2021 (in Japanese), https://www.idc.com/getdoc.jsp?containerId=prJPJ47631521 (accessed on June 1, 2022)
(3) Carlock, P.G., et al., “System of Systems (SoS) Enterprise Systems for Information-Intensive Organizations,” Systems Engineering, Vol.4, No. 4, pp. 242-261, 2001
(4) Yokogawa Electric Corporation, “Yokogawa Draws Up New Midterm Business Plan, Accelerate Growth 2023,” press release, 2021, https://www.yokogawa.com/news/press-releases/2021/2021-05-11/(accessed on June 1, 2022)
(5) ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration
(6) Theodore J. Williams, “The Purdue enterprise reference architecture,” Computers in Industry, Vol. 24, No. 2-3, 1994, pp. 141-158
(7) Wenbin Dai, Hiroaki Nishi, et al., “Industrial edge computing: Enabling embedded intelligence,” IEEE Industrial Electronics Magazine, Vol. 13, No. 4, 2019, pp. 48-56
(8) Richard Paes, David C. Mazur, et al., “A guide to securing industrial control networks: Integrating IT and OT systems,” IEEE Industry Applications Magazine, Vol. 26, No. 2, 2020, pp. 47-53
(9) VERVE, “What is an OT SIEM and how is it different from IT SIEM,” 2020, https://verveindustrial.com/resources/blog/what-is-anot-siem-and-how-is-it-different-from-it-siem/ (accessed on June 1, 2022)
(10) Ease ISA/IEC 62443 compliance with EdgeLockTM SE05x (Rev. 1.1),2020, https://www.nxp.com/docs/en/application-note/AN12660.pdf (accessed on June 1, 2022)
(11) Tetsuo Shiozaki, “Yokogawa’s Approach to Cybersecurity in the IT/OT Convergence Environment,” Yokogawa Technical Report English Edition, Vol. 64, No. 1, 2021, pp. 27-32, https://webmaterial3. yokogawa.com/1/31643/files/rd-te-r06401-005.pdf?_ga=2.133994635.485524645.1655879796-1121227122.1655879796 (accessed on June 1, 2022)
(12) MITRE, ATT&CK® for Industrial Control Systems, https://collaborate.mitre.org/attackics/index.php/Main_Page (accessed on June 1, 2022)