사례 연구

보안

Dubai Electricity and Water Authority

ArcSight는 정교한 SOC를 지원하며, OT와 IT를 성공적으로 연결하여 독보적인 지능형 보안을 제공합니다.

개요

Dubai Electricity and Water Authority (DEWA)는 두바이 시민과 주민에게 전기 및 수도를 지속적이고 안정적으로 공급하고 있습니다. DEWA는 세계 최고의 공익 사업체 중 하나이며, 세계 일류의 품질, 효율성, 가용성을 자랑하는 전기 및 수도 서비스를 두바이의 900,000여 고객에게 제공합니다. DEWA의 총 최대 출력은 일당 11,413MW의 전력, 4억7천만 영국 갤런의 수도 공급을 자랑합니다. UAE를 대표하는 DEWA는 World Bank의 Doing Business 2019 보고서에서 전력 수급 부문의 세계 1위로 2년 연속 선정되었습니다.

당면 과제

DEWA는 국가의 주요 인프라로서 보안 관리 부문에서 고유한 당면 과제를 갖고 있습니다. 바로 사이버 공격이 도시 전체를 무너뜨리고 국가 비상사태를 야기할 수 있다는 것입니다. 주요 인프라 제공업체들은 운영 기술(OT)에 과중하게 의존하여 유틸리티 네트워크를 관리하고 있습니다. 이는 일반적으로 외부 세상과 연결되지 않는 고립된 시스템입니다. 예전에는 이와 같은 방식으로 보안이 보장될 것이라 여겼지만, 이젠 그렇지 않습니다. DEWA의 사이버 보안 전문가인 Jacob Jacob은 다음과 같이 설명합니다. "우리는 수백만 개의 장치가 공용 ISP 네트워크를 통해 인터넷에 연결된 세상에 살고 있습니다. 사물 인터넷(IoT)은 태양열 발전기와 차량 충전소 등의 스마트 홈 부문에서 DEWA와 관련이 있습니다. 우리가 사이버 보안 여정을 시작했을 때, IT와 OT를 통합하여 시스템 간의 데이터를 공유하고, OT 장치에 대해 위협에 대처하는 인텔리전스를 확보하며, IT 장치에 대한 모니터링을 개선할 수 있는 솔루션을 원했습니다."

DEWA는 핵심 보안 우선순위를 정하여 모든 보안 이벤트로 인한 영향 완화, 보안 위협의 탐지와 차단, 업무 중단 시간 및 규정 미준수의 감소를 다루고 있습니다. 보안 데이터의 양이 끊임없이 증가하는 가운데, DEWA는 가시성을 제공하고 조사 역량을 가속하기 위한 향상된 데이터 분석 기능을 갖춘 인텔리전스 기반 보안 수단이 필요했습니다.

해결 방안

DEWA의 연구는 무질서한 데이터를 보안 인사이트로 전환하는 개방형 플랫폼인 Micro Focus ArcSight를 포함한 생태계를 구축하는 것으로 이어졌습니다. Jacob은 몇 가지 ArcSight 기능에 관심을 보였습니다. "데이터를 광범위한

"ArcSight를 통해 우리는 보안 이벤트를 모니터링하고 사고를 관리하는 플랫폼을 확보했습니다. 원활하게 데이터를 통합하고 있으며 관련 보안 표준 및 통제 기준을 준수하고 있습니다. 자산 가시성이 향상되어 99%의 가용성을 확보했습니다."

JACOB JACOB
사이버 보안 전문가
Dubai Electricity and Water Authority

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority

소개

- **업종**
  에너지 및 유틸리티
- **위치**
  아랍에미리트 두바이
- **당면 과제**
  IT와 OT를 통합하여 시스템 간에 데이터를 공유하고 위협 인텔리전스 및 장치 모니터링을 개선
- **제품 및 서비스**
  Micro Focus ArcSight Data Platform
  Micro Focus ArcSight Enterprise Security Manager
  Micro Focus ArcSight Investigate
- **결과**
  + 보안 알림 30% 감소
  + 98%의 위험 완화율
  + AI 기반 감지를 통한 계량기 부정행위 감소
  + 가시성 향상을 통한 99%의 장치 가용성

"우리의 위험 주제를 가시화하고, ArcSight와 같은 최신 비즈니스 지원 기술을 도입하며, 최첨단 보안 운영 센터(SOC)를 설립하는 등 다양한 접근 방식을 사용하여 알림을 30% 줄이고 리소스를 가장 효과적으로 전달되도록 할 수 있었습니다.

JACOB JACOB
사이버 보안 전문가
Dubai Electricity and Water Authority

문의하기:
www.microfocus.com

콘텐츠가 유익했다면 공유해 주세요.

소스에서 수집하여 분석에 기반이 되는 지능적인 상관관계를 제공할 수 있습니다. 저희는 Elastic과 협력하고 있으며 ArcSight와 Elastic 간의 기본적인 통합을 이루게 되어 기쁩니다. 이는 당사의 분석 능력을 강화하며 지리적인 맥락을 제공합니다. 수많은 장치를 모니터링해야 하기 때문에 다양한 소스에서 데이터를 확보하는 것이 매우 중요합니다. 예를 들어 밸브가 작동되고 있는지, 파이프라인의 일부 구역과 네트워크 간의 연결이 끊어졌는지를 파악할 필요가 있습니다. 이런 경우들은 서비스 제공에 잠재적으로 심각한 영향을 미치는 네트워크 이벤트입니다."

ArcSight Data Platform(ADP), ArcSight Enterprise Security Manager(ESM), ArcSight Investigate는 기존의 Hadoop, Spark, Elastic과 연결할 수 있는 정교한 보안 생태계의 일부입니다. ArcSight의 포트폴리오는 인공 지능(AI)과 결합되어 데이터 로그 관리, 데이터 분석, 실시간 경보 및 모니터링, 보안 분석, 지능형 보안 운영 기능을 제공합니다.

"우리는 사이버 보안 전문가로서 계량기 부정행위를 탐지하도록 요구받았으며, 이는 우리가 부정행위를 표시하도록 계량기 데이터를 수집, 연계, 해석하는 비즈니스 활용 사례를 보유하고 있기 때문입니다." 라고 Jacob은 설명합니다. "ArcSight는 우리가 다양한 데이터 소스를 결합하도록 지원했으며, 데이터 스트림에 AI를 구축하여 소비 패턴을 분석할 수 있었습니다. 이를 통해 현재는 부정 사용 사례들이 자동으로 탐지 및 표시되고 있습니다."

ArcSight를 이용한 분석 생태계는 차세대 보안 운영 모델을 만드는 데 도움이 되었습니다. 활성 이벤트 필터링 및 우선순위 지정 기능을 통해 DEWA는 중요한 알림에 집중할 수 있습니다. 12가지 최첨단 기술이 통합되어 10여 개의 연결된 소스에서 데이터를 수집합니다. 이러한 인프라는 DEWA가 관리하는 장치 및 네트워크의 80%에서 사용되며, 20여 개의 운영 대시보드가 자동으로 생성되어 보안 상태에 대한 실시간 가시성을 제공합니다.

이와 동시에, OT 또한 보안 생태계로 통합되었습니다. 현재 DEWA 지점 25곳 전반의 인텔리전스 기반 보안 수단은 3,000개에 달하는 장치들을 완벽하게 모니터링하고 있으며, 위험 완화율은 98%에 달합니다.

결과

사막으로 둘러싸인 도시에서 물은 희귀하고 구하기 어려운 재화입니다. DEWA는 적응형 시스템 생태계인 ArcSight를 포함한 기술을 활용하여 이제 AI 기반 이벤트 모니터링을 통해 수도 네트워크의 동작을 예측할 수 있습니다. 이를 통해 용량 계획을 더 정확하게 세우고 낭비를 줄일 수 있습니다.

Jacob은 다음과 같이 설명합니다. "ArcSight를 통해 우리는 보안 이벤트를 모니터링하고 사고를 관리하는 플랫폼을 확보했습니다. 원활하게 데이터를 통합하고 있으며 관련 보안 표준 및 통제 기준을 준수하고 있습니다. 자산 가시성이 향상되어 99%의 가용성을 확보했으며, 데이터 연결성이 더욱 정교해지면 당사의 단기 목표인 전체 100%로 향상될 것입니다."

Jacob은 다음과 같이 끝을 맺습니다. "우리의 위험 주제를 가시화하고, ArcSight와 같은 최신 비즈니스 지원 기술을 도입하며, 최첨단 보안 운영 센터(SOC)를 설립하는 등 다양한 접근 방식을 사용하여 알림을 30% 줄이고 리소스를 가장 효과적으로 전달되도록 할 수 있었습니다. 우리는 전략적인 파트너인 Micro Focus를 찾았으며, 혁신적인 사이버 보안 여정을 계속 함께하기를 기대하고 있습니다."

168-KO0609-001 | M | 06/20 | © 2020 Micro Focus or one of its affiliates. Micro Focus와 Micro Focus 로고는 영국, 미국 및 기타 국가에서 Micro Focus를 비롯해 그 계열사나 자회사의 상표 또는 등록 상표입니다. 기타 모든 마크는 각 소유사의 재산입니다.