<붙임 2> 시나리오 제출양식

시나리오 제목
풍력발전소 대상 다단계 사이버 공격 시뮬레이션 및 계층적 사이버 방어 체계 구축
시나리오 단계
3
시나리오 목적
OT/ICS 환경의 사이버 킬체인과 보안 솔루션(NIDS, HIDS, SOAR)의 이해 및 사이버 침해 대응 실무 적용 능력 함양
시나리오 줄거리
[배경] - 국가 주요기반시설인 24MW 규모 풍력발전단지는 30기의 풍력터빈으로 구성되어 있으며, 각 터빈은 0.8MW의 전력을 생산하고 있음. - 최근 재생에너지 시설을 표적으로 삼는 APT 그룹의 공격 사례가 다수 발생하였으며, 공격자들은 국가 전력망 교란을 통한 사보타주를 목표로 침투를 시도함. **[1단계]: 원격 침투 공격** - 해커는 먼저 풍력터빈 제조사 엔지니어에게 가짜 이메일을 송신. "긴급 유지보수 안내"라는 제목의 이메일에는 악성 파일이 숨어있고, 엔지니어가 이를 열자 VPN 접속 정보가 해커에게 전송됨. - 해커는 훔친 VPN 계정으로 풍력발전제어 네트워크에 원격 접속. VPN 서버를 통해 내부망에 들어온 해커는 네트워크를 스캔하여 풍력터빈을 제어하는 메인 컴퓨터(통합 제어기)를 식별. 이 컴퓨터는 오래된 Windows 7을 사용하고 있어 알려진 취약점(EternalBlue)이 존재함. - 해커는 이 취약점을 이용해 시스템 최고 권한을 획득하고, 몰래 백도어 계정을 생성. 또한 5분마다 해커의 서버로 신호를 보내는 프로그램을 설치해 지속적인 접근을 유지함. - 마침내 해커는 풍력터빈과 통신하는 산업용 프로토콜(Modbus)을 조작하여 20개 터빈의 출력을 정상의 20%로 떨어뜨림. 원래 24MW를 생산하던 발전소는 순식간에 11.2MW로 출력이 감소하고, 전력망에 심각한 불안정이 발생. **[2단계]: 내부 침투 공격** - 유지보수 업체 직원으로 위장한 침입자가 발전소 현장에 직접 접근. 보안이 취약한 Wi-Fi나 관리되지 않은 네트워크 포트를 통해 내부 제어망에 접속. - 침입자는 먼저 네트워크를 스캔하여 제어 시스템의 원격 접속 서비스(RDP)를

식별. 자동화 도구를 사용해 'admin', 'password' 같은 흔한 비밀번호를 수백 번 시도하는 무차별 대입 공격 수행.

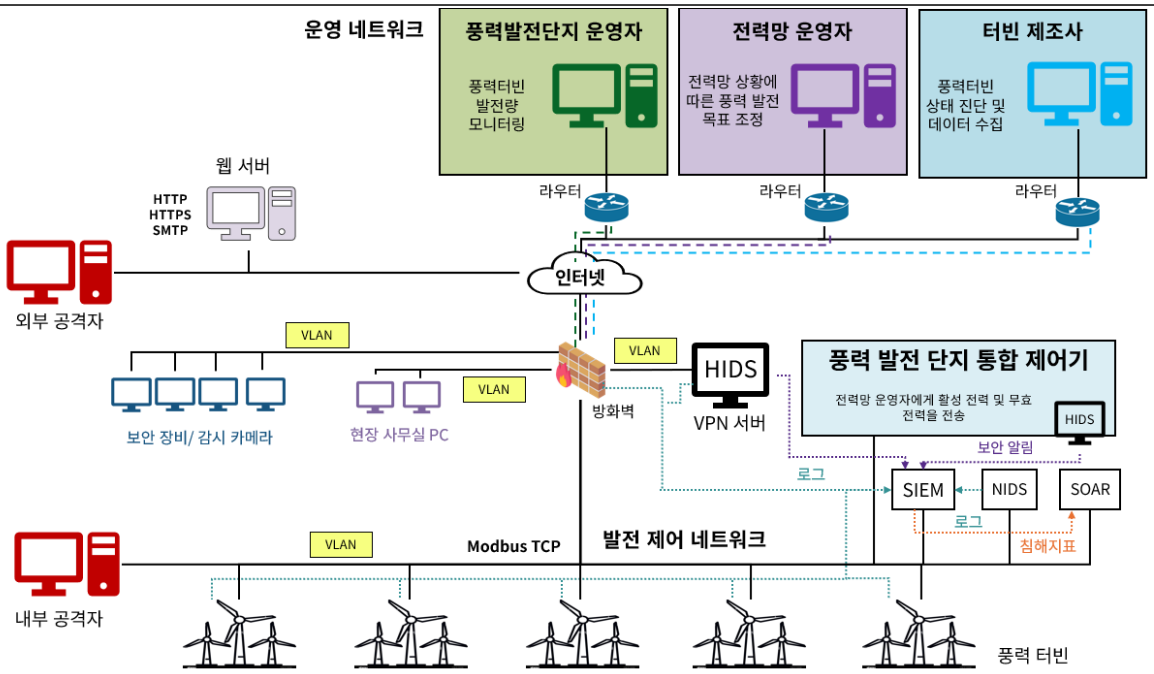
- 동시에 대량의 네트워크 패킷을 보내는 서비스 거부 공격을 실행하여 제어 시스템의 성능 마비. CPU 사용률이 100%에 달하면서 정상적인 운영 불가능.
- 이어서 각 풍력터빈의 관리 인터페이스(Telnet)에도 같은 방식으로 접근을 시도. 기본 비밀번호인 'admin123'이 그대로 사용되고 있어 손쉽게 계정이 탈취됨. 침입자는 30개 터빈 전체를 장악하여 출력을 20%로 제한하고, 발전단지는 겨우 4.8MW만 생산되는 상태.

[3단계]: 공격 탐지 및 대응

- [탐지] NIDS(Zeek)에서 "EternalBlue Exploit Attempt" 알람 발생. "Abnormal Modbus Traffic", "TCP SYN Flood", "RDP Brute Force" 등의 알람이 연속적으로 표시됨. HIDS(Wazuh)에서도 "신규 계정 생성: svchost", "예약 작업 등록", "다중 로그인 실패 " 등의 이벤트가 실시간으로 보고됨.
- [초기 대응] 보안팀은 공격 타임라인을 재구성하여 두 개의 독립적인 공격이 동시 진행 중임을 파악. 외부 VPN 침투와 내부 물리적 침투가 동시에 발생한 조직적 APT 공격으로 판단. 방화벽 콘솔에 접속하여 공격자 IP를 긴급 차단하고, VPN 서버에서 의심 세션을 모두 종료.
- [복구] 통합 제어기에 원격 접속하여 백도어 계정 'svchost' 삭제, 악성 예약 작업 제거. MS17-010 보안 패치 긴급 적용 및 모든 계정 패스워드 강제 리셋. Python 스크립트를 실행하여 30개 풍력터빈의 출력 설정을 정상값(0.8MW)으로 복구. 전력 생산량 24MW로 회복.
- [자동 대응] StackStorm 플레이북 활성화. RDP 무차별 공격 감지 시 13.8초 내 해당 MAC 주소의 스위치 포트 자동 차단. 새로운 악성 IP 발견 시 5.8초 내 방화벽 규칙 자동 업데이트.

시나리오 네트워크 구성도

- 약 30대의 가상머신을 활용하여 풍력발전단지 인프라를 구현. VyOS 기반 라우터로 네트워크를 구성하고, Windows/Linux 혼합 환경으로 OT 환경과 유사하게 재현.
- 인터넷 망, 운영 네트워크, 발전 제어 네트워크를 VLAN으로 분리하여 실제 풍력발전소의 보안 아키텍처를 구현. 방화벽과 라우터를 통해 각 영역 간 접근을 통제하며, VPN 서버가 유일한 원격 접속 경로 역할을 수행함.
- 방어자는 발전 제어망에 구축된 NIDS, HIDS, SIEM, SOAR 등의 보안 솔루션을 종합적으로 활용하여, 외부와 내부에서 동시에 발생하는 복합적인 공격에 대응
- Metasploit, Hydra, 커스텀 Python 스크립트를 사전 설치하여 공격 시연을 자동화. 방어 측면에서는 Zeek, Wazuh, StackStorm의 설정 파일과 플레이북을 미리 구성하여 즉시 탐지-대응 실습을 진행할 수 있도록 준비함.

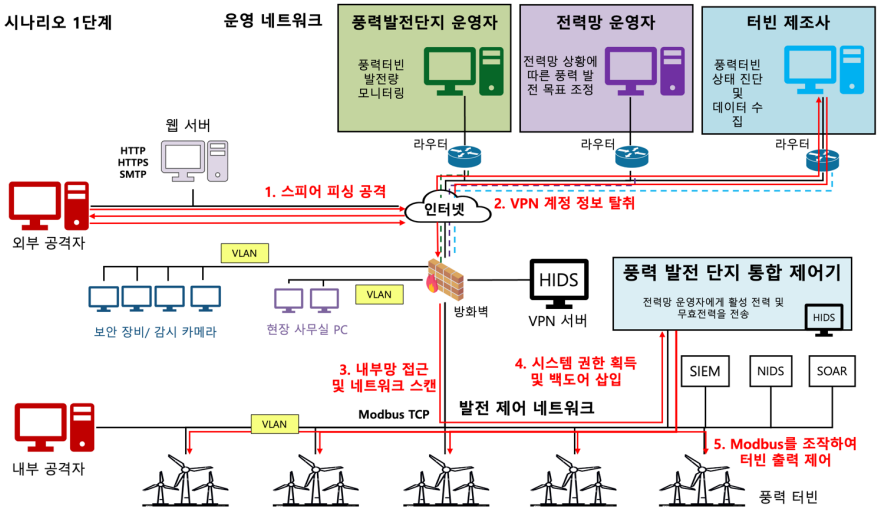


<시나리오 네트워크 구성도>

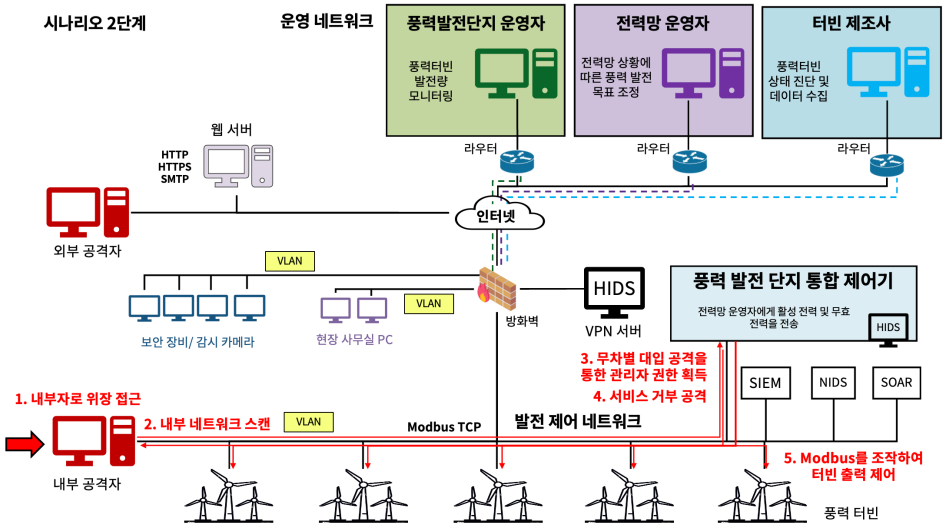
망 구분	명칭	운영체제/소프트웨어	역할
인터넷	공격자 1	Kali Linux	외부 공격 시나리오 수행
	웹 서버	Ubuntu	웹/메일 트래픽 생성 (내부망 사무 PC 시뮬레이션)
	VPN 클라이언트	Ubuntu/wireguard	발전 제어 네트워크 접속
운영 네트워크	풍력발전 운영자	Windows	풍력발전단지 관리 인터페이스 접속
	전력망 운영자	Windows	전력망 모니터링 및 발전량 조정
	터빈 제조사	Windows	풍력 터빈 원격 유지보수
발전 제어 네트워크	사무실 PC	ubuntu	현장 사무 환경 모사를 위한 시뮬레이션
	보안 장비	ubuntu	운영망 내 보안 장비 및 감시 카메라 모사를 위한 시뮬레이션
	VPN 서버	Ubuntu/wireguard	원격 접속 관리, 호스트기반 침입 탐지
	IDS	Linux/Zeek	이상행위 탐지, 보안 이벤트 로깅
	SOAR	Linux/StackStorm	플레이북 기반 위협 대응 자동화
	SIEM	Linux/wazuh	중앙 로그 수집 및 HIDS 관리
	풍력 터빈	Linux	풍력 터빈 시뮬레이터(Modbus 서버)
	통합 제어기	Windows	풍력 터빈 제어, SCADA 인터페이스
	공격자 2	Kali Linux	내부 공격 시나리오 수행
네트워크 인프라	ISP 라우터	Linux/Vyos	인터넷 망 구성 (ISP 백본)
	방화벽	Linux/Vyos	인터넷 ↔ 운영 네트워크 경계 연결
	운영 라우터	Linux/Vyos	풍력발전단지 운영자, 전력망 운영자, 터빈 제조사 ↔ 인터넷 망 연결 운영 네트워크 내부 VLAN 구성
	발전제어 라우터	Linux/Vyos	방화벽(인터넷 ↔ 터빈) 및 VLAN을 통한 제어 네트워크 망 분리
기타	전력 계통 시뮬레이터	Windows/Powerworld	풍력 터빈으로부터 전력 데이터 수신하여 전력 계통 반영

<시나리오 구현에 필요한 가상머신 목록>

단계 번호		1
단계 명		APT 그룹의 원격 침투 공격 (Remote Attack)
주요 목표		VPN 계정 탈취를 이용한 내부망 침투 및 EternalBlue 취약점 악용을 통한 통합 제어기 장악, Modbus 프로토콜 조작으로 20개 풍력터빈 출력을 20%로 제한하여 전력 생산 감소
유형	**공격**	정찰, 전달, 취약점 악용, 설치, 명령 및 제어, 목표 달성
	방어	
주요 활동		- **(전달)**: 공격자는 OEM 업체를 대상으로 한 스피어 피싱 공격으로 사전에 탈취한 VPN 자격 증명을 사용하여, 외부 인터넷에서 발전소 내부 네트워크의 VPN서버로 원격 접속. - **(정찰)**: 내부망 접속 후, Nmap 도구를 사용하여 네트워크 스캐닝을 수행하고 공격 목표인 Windows 7 운영체제의 통합 제어기가 온라인 상태임을 확인. - **(취약점 악용)**: Metasploit 프레임워크를 통해 EternalBlue 익스플로잇을 실행하여 통합 제어기의 원격 제어 권한을 획득하고, 원격 관리 트로이목마(RAT) 페이로드를 시스템에 주입. - **(설치/권한 상승)**: 탐지를 회피하고 권한을 상승시키기 위해, 공격자는 Meterpreter 세션을 정상 프로세스인 explorer.exe로 마이그레이션하여 시스템 최고 권한 획득. - **(명령 및 제어)**: 공격자는 영구적인 접근을 위해 시스템에 백도어 사용자를 추가하고, Meterpreter 세션이 끊어질 경우를 대비하여 원격 C2(Command & Control) 서버로 다시 접속을 시도하는 예약 작업 생성. 또한, 제어 서버의 SAM(Security Account Manager) 데이터베이스에서 비밀번호 해시를 덤프하여 외부로 유출. - **(목표 달성)**: 장악한 통합 제어기에 포트 포워딩(Port Forwarding) 규칙을 생성하여, 내부망의 풍력 터빈 Modbus 서버에 접근할 수 있는 경로를 확보. 30기의 풍력 터빈 중 20기에 Modbus 쓰기(Write) 명령을 전송하여 각 터빈의 유효 전력(Active Power) 출력을 정격 용량의 20%로 강제로 변경.
주요 사용 도구 및 기술		**[사용 도구 및 기술]** - Metasploit Framework: EternalBlue 취약점 공격 코드를 실행하고, 시스템 제어를 위한 페이로드(Meterpreter)를 주입하며, 권한을 상승시키는 등 핵심적인 침투 공격을 수행하는 데 사용되는 오픈소스 프레임워크.

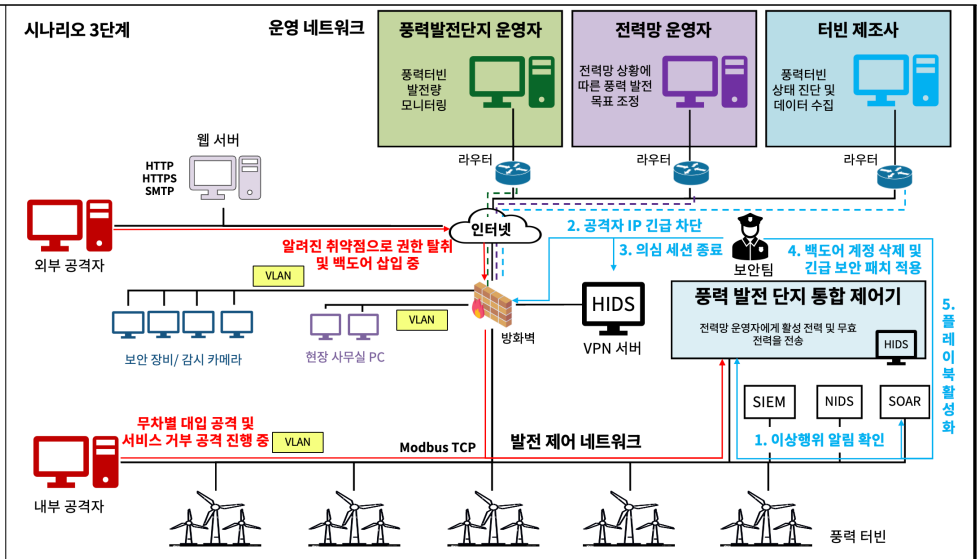
	– Nmap: 공격 초기 단계에서 목표 네트워크의 구조, 활성화된 호스트, 운영체제, 열려있는 서비스 포트 등을 파악하는 정찰 활동에 사용되는 네트워크 스캐닝 도구 **[필요한 기술 역량]** – 산업용 제어 프로토콜(Modbus TCP): 풍력 터빈의 출력을 직접 조작하는 데 사용된 산업용 제어 프로토콜로, 이 프로토콜의 쓰기(Write) 기능을 악용하여 물리적 피해를 유발함
예상 결과물 및 상태	– 통합 제어기 완전 장악 (SYSTEM 권한) – 지속적 백도어 접근 확보 – 20개 터빈 출력 감소 (24MW에서 11.2 MW)  <시나리오 1단계 공격 흐름도>

단계 번호		2
단계 명		내부 침투 및 서비스 마비 공격 (Local Attack)
주요 목표		내부 OT 네트워크에 접근한 공격자가 무차별 대입 공격과 서비스 거부(DoS) 공격을 통해 시스템을 마비시키고, 최종적으로 풍력 터빈 전체의 출력 중단
유형	**공격**	정찰, 취약점 악용, 목표 달성
	방어	
주요 활동		- **(정찰)**: 공격자는 유지보수 업체 직원으로 위장하여 풍력발전소 현장에 물리적으로 침투하여 발전 제어 네트워크에 접속 상황 가정, Nmap으로 내부망을 스캔하여 통합 제어기와 같은 핵심 자산과 활성화된 서비스(RDP, Telnet 등)를 식별 - **(취약점 악용)**: Hydra 도구를 사용하여 통합 제어기의 RDP 서비스에 대해 무차별 대입 공격 수행. admin, administrator, operator 등의 계정명과 password, 123456, wind2024 등 250개 조합을 초당 수십 번씩 시도하여 접근 권한 획득 시도. - **(목표 달성)**: Hping3를 사용한 TCP SYN Flood 공격을 실행하여 통합 제어기에 초당 수천 개의 패킷을 전송. CPU 사용률을 100%로 포화시켜 정상적인 운영자의 시스템 접근을 차단하고 보안 모니터링 기능을 마비. - **(목표 달성)**: 자동화 스크립트를 실행하여 30개 풍력터빈의 텔넷 서비스에 순차적으로 접속 시도. 대부분의 터빈이 기본 패스워드을 그대로 사용하고 있어 전체 터빈의 관리자 권한 획득. - **(목표 달성)**: Python으로 작성된 Modbus 공격 스크립트를 실행하여 30개 전체 터빈에 동시 접속. 각 터빈의 Active Power Setpoint 레지스터(40084)에 0.16MW(정격의 20%) 값을 강제 입력하여 전체 발전소 출력을 24MW에서 4.8MW로 제한.
주요 사용 도구 및 기술		- Hydra: RDP, Telnet 등 다양한 프로토콜을 대상으로 온라인 무차별 대입 공격을 수행하여 암호 크래킹하는 데 사용되는 도구. - Hping3: TCP/IP 패킷을 생성하고 전송할 수 있는 도구로, 본 시나리오에서는 DoS 공격을 수행하는 데 사용. - Python : 산업용 프로토콜인 Modbus TCP 통신을 자동화하고, 다수의 터빈에 동시 다발적인 제어 명령을 보내는 데 사용. - Nmap: 내부 네트워크의 자산을 식별하고 공격 표면을 분석하는 정찰 활동에 사용.

예상 결과물 및 상태	- 30개 전체 터빈 관리자 권한 획득 - 전력 생산 80% 감소 (24MW → 4.8MW) - 시스템 CPU 100% 포화 상태 유지 - 네트워크 트래픽 1Gbps 포화  <시나리오 2단계 공격 흐름도>

단계 번호		3
단계 명		APT 공격 탐지 및 대응
주요 목표		VPN 취약점을 악용한 원격 침투로 Wind Site Controller 장악 및 풍력터빈 출력 조작
유형	**공격**	
	방어	탐지, 분석, 대응
주요 활동		**[탐지]** – (네트워크 이상행위 탐지): NIDS(Zeek)가 발전 제어 네트워크의 미러 포트에서 실시간 패킷 분석 수행. · EternalBlue Exploit Attempt 알람 발생 · Abnormal Modbus Traffic(Function Code 16 비정상 사용) · TCP SYN Flood (초당 수천 개 패킷) · RDP Brute Force"(250회 로그인 시도) 알람 표시. – (호스트 이상행위 탐지): HIDS(Wazuh) 에이전트가 통합 제어기에서 의심스러운 활동을 실시간 감지. · 신규 계정 생성: svchost(Event ID 4720) · 예약 작업 등록: Windows Defender Update · 다중 RDP 로그인 실패 이벤트 – (물리적 영향 감지): SIEM 대시보드에서 전력 생산량이 24MW에서 11.2MW로 감소 확인. **[초기 대응 – 수동 조치]** – (상황 분석): SIEM에 수집된 모든 알람을 통합 분석하여 공격 타임라인 재구성. · ex) 10:15 VPN 접속, 10:31 EternalBlue 공격, 10:45 Modbus 조작(외부), 10:50 RDP 로그인 시도(내부) 등 두 개의 독립적인 Kill Chain이 동시 진행되는 조직적 APT 공격임을 확인. – (차단): 방화벽 관리 콘솔에 접속하여 식별된 공격자 IP(외부/내부)를 iptables 명령으로 즉시 차단. VPN 서버에서 모든 원격 세션 강제 종료.

	[복구] - (악성 요소 제거): 통합 제어기에 안전한 경로로 원격 접속하여 백도어 계정 'svchost' 삭제. Windows 작업 스케줄러에서 "Windows Defender Update"로 위장한 악성 예약 작업 제거. 레지스트리에서 지속성 관련 항목 정리. - (보안 패치 적용): MS17-010(EternalBlue) 보안 업데이트를 WSUS를 통해 긴급 배포. 모든 시스템 계정의 패스워드를 복잡도 정책에 따라 강제 리셋. 텔넷 서비스 비활성화 및 RDP 접속 IP 화이트리스트 적용. - (전력 생산 복구): Python 스크립트를 실행하여 30개 모든 풍력터빈의 Active Power Setpoint 레지스터를 정상값 0.8MW(800)로 일괄 변경. 전력 생산량이 4.8MW에서 24MW로 회복됨을 확인 [자동 대응 - SOAR 플레이북 실행] - (EternalBlue 자동 차단): StackStorm이 NIDS의 EternalBlue 알람을 트리거로 자동 플레이북 실행. Elasticsearch에서 공격자 IP 추출 → SSH로 방화벽 접속 → iptables 규칙 자동 추가 → VPN 세션 종료 명령 실행. - (RDP 무차별 대입 공격 차단): HIDS가 8회 이상 RDP 로그인 실패 감지 시 자동 플레이북 활성화. 공격 근원지 MAC 주소 식별 → 스위치 API 호출 → 해당 포트 shutdown 명령 → 계정 잠금 처리.
주요 사용 도구 및 기술	- Zeek(NIDS): 네트워크 트래픽을 실시간 분석하여 EternalBlue, DoS, 무차별 대입 공격, 비정상 Modbus 통신 등을 탐지하는 오픈소스 네트워크 보안 모니터링 플랫폼 - Wazuh(HIDS/SIEM): 호스트 기반 침입 탐지, 로그 수집, 취약점 스캔, 컴플라이언스 모니터링을 통합 제공하는 보안 플랫폼 - Grafana + Elasticsearch: 보안 이벤트와 전력 시스템 데이터를 실시간으로 시각화하고 상관관계를 분석하는 대시보드 솔루션 - StackStorm(SOAR): 이벤트 기반 자동화 엔진으로, Python 기반 플레이북을 통해 보안 인시던트에 대한 자동 대응 수행
예상 결과물 및 상태	- 전력 생산 완전 복구: 24MW (100% 정상화) - 모든 공격 경로 차단 완료 - 침해대응 대응 보고서 작성



<시나리오 3단계 방어 흐름도>