How Rhebo secures OT networks in electric substations

PASSIVE SECURITY MONITORING

NON-INTRUSIVE INTRUSION DETECTION

CONTINUOUS MONITORING 24–7–365

Substations are a particularly attractive target for hybrid warfare adversaries. The utilities are highly distributed, remote-controlled, and lack on-site cybersecurity personnel. This is not the only reason why digital substations are particularly vulnerable to cyberattacks. There is a multitude of attack vectors that firewalls have a hard time securing (if at all):

- Engineering workstations (EWS) used by employees and 3rd party service providers
- Supply Chain Compromise (via vendors, integrators, service providers)
- Exposed network components
- Vulnerabilities in remote access technologies
- Local WAN connections
- Inadequate physical perimeter protection
- Security risks in current OT protocols such as SV, GOOSE, MMS, IEC-104, and IEC 61850.

That makes it all the more essential to keep an eye on the OT, telecontrol technology and station automation when considering the cybersecurity of a substation. Doing so also complies with the NIS2 requirement for stringent protection of critical processes and systems.

To ensure the security of station automation, operators and security managers can utilize three monitoring approaches:

1. Host-based intrusion detection system (HIDS)
2. General device log data
3. Network-based intrusion detection system (NIDS).

However, they strongly differ in effectiveness and practicability.

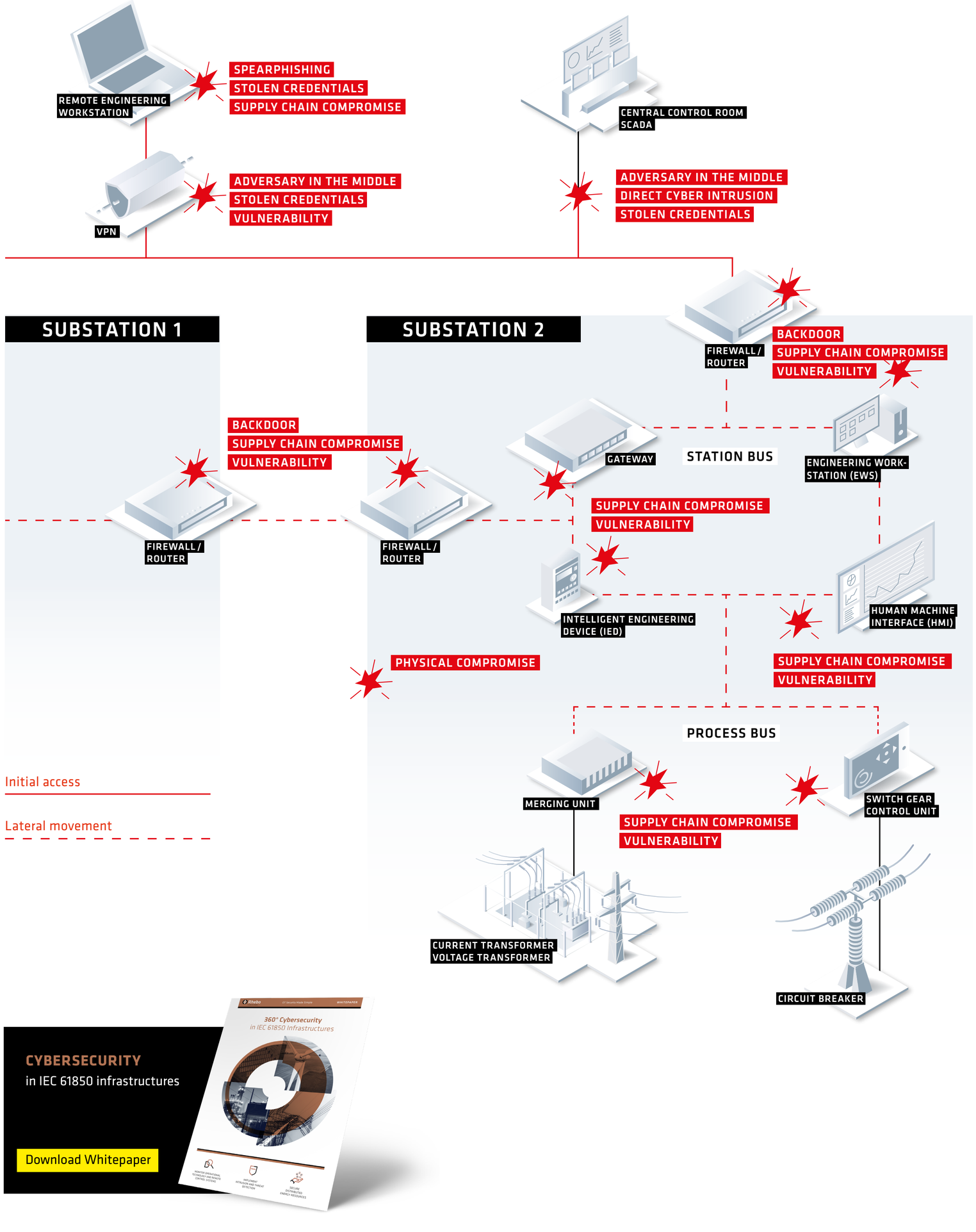
Host-based IDS can generally only be used on station bus-level IT systems, i.e. MS Windows servers and workstations, due to their limited capabilities in decoding industrial protocols and the resource constraints of substation components. This effectively leaves the OT itself in the dark.

OT device log data, if available at all, provides information about sessions but little insight into security issues. Furthermore, they can overwhelm operators and security staff due to the flood of data and different log formats.

A network-based IDS on the other hand, continuously analyzes all communication on both the station bus and the process bus on network level. Anomalies and security-relevant incidents are reported in real time. Integration is easy via mirror switch ports or network taps. The non-intrusive, purely passive analysis prevents both unwanted interference with critical processes and overload of the monitored components.

CYBER RISKS IN SUBSTATIONS

AND HOW THESE RISKS CAN BE DETECTED EARLY ON WITH NIDS RHEBO INDUSTRIAL PROTECTOR.



Rhebo Industrial Protector NIDS supports DOCUMENTATION with

- network map of active OT devices within substations
- information on connections, protocols and behavioral communication pattern between devices
- information on firmware version and known vulnerabilities (CVE)

Rhebo Industrial Protector NIDS enables real-time DETECTION of

Backdoor compromise, e.g. via
- downloads and uploads
- attempted internet connections (i.e. to public domains)

Direct cyber intrusions, e.g. via
- new devices communicating within or to OT
- new connections, protocols between devices
- internet connections (i.e. to public domains)
- network scans
- failed login attempts (e.g. via brute force or password spraying)
- downloads and uploads

Physical compromise, e.g. via
- new devices communicating within or to OT
- new connections, protocols between devices

Stolen credentials / adversary in the middle, e.g. via
- changed communication behavior
- new connections, protocols between devices

Supply Chain Compromise, e.g. via
- changed communication behavior
- downloads and uploads

Technical error states, e.g. via
- ICMP unreachable
- TCP retransmission
- checksum errors
- time sync errors

Vulnerabilities, e.g. via
- firmware version and known vulnerabilities (CVE entries)

Rhebo Industrial Protector NIDS supports INCIDENT RESPONSE with

- information on CVE risks for systems
- input for SIEM via syslog and alerts via SNMP
- forensic data of security incidents

NIDS IN ELECTRIC SUBSTATIONS 06-2025