



POWER UTILITY CYBER SECURITY APPLICATION

V1.0

Power Grid Digital Network is one of the most critical infrastructure in every country and protecting it from cyber-attacks and cyber-terrorism has becoming increasingly important due to its pivotal role in supporting the functioning of society, the economy, and various essential services and being a critical infrastructure backbone of the nation, it is always prone to cyber threats and cyber-attacks.

Overview:

Power Grid Infrastructure is vulnerable to cyberattacks, including ransomware, phishing, and malware. Breaches in these systems could disrupt exploration, distributions and supply, leading to substantial economic losses and potential safety hazards.

Many "Critical Infrastructure (CI)" sectors still rely on older, legacy systems and infrastructure that may not have robust cybersecurity measures in place. These systems are often more susceptible to cyber threats due to outdated technology and lack of regular updates.

A single breach in one area could potentially impact leading to widespread outages and damage.

Further, Power Grid Infrastructure relies on numerous vendors and suppliers for equipment and software. Weaknesses in the supply chain, such as compromised or insecure components, could pose significant cybersecurity risks.

The risk of insider threats, whether intentional or accidental, also remains a concern. Malicious insiders or employees with inadequate training might inadvertently compromise the system.

CXR Networks provides a comprehensive range of Cyber Security products and solutions with advanced features and advantages for utility sectors. These equipment include:

- **Advance Honey Pot (VCL-2143, Network MouseTrap):** This product is an essential network security and forensics tool that enables users to detect firewall breaches and unauthorized network intrusions in their network, in real-time. It is also unique as it provides alerts in real time - including audio and visual alerts – on detection of a network security breach / cyber-attack or ransomware attack etc. It fingerprints the credentials of the hostile entity who have entered the protected network by maintaining a complete log of their credentials such as IP address, domain and the originating location details of the intruder along with providing a trace-route of the intrusion.

This advanced Honeypot also fulfils the need to detect any trojan activity that may emanate from within the customer network.

Key features include:

- Detect network intrusion and firewall breach.
- Detect moles and trojans within existing network.
- Intrusion / Network breach detection alarms.
- Integrated real-time audio and visual alarms.
- Attacker trace root with forensics.
- Maintain complete log with time-stamp of intruder credentials such as IP address, domain and the originating location details.
- Create automated daily, weekly or monthly intrusion detection reports.
- Out-of-band access and security alerts.
- White-list / black-list option.
- Port based, IP Address based, and IP Domain based programmable filters.
- Graphical User Interface (GUI).

- **VCL-2702, Network Isolation (Kill) Switch)** This equipment provides manual and automatic isolation of the Local Area Network from Wide Area Network, in an event of a network security breach / cyber-attack or ransomware attack. It helps create Operational Zones or secure parameter zones with the external network, in the event of the detection of a network intrusion / breach in the cyber-security perimeter of the network's demilitarized zone, data storage servers, critical digital assets etc.

Key features include:

- Provides manual and automatic isolation of the Local Area Network from Wide Area Network, in an event of a network security breach / cyber-attack ransomware attack.
- Create Operational Zones or secure parameter zones with the external network isolate the network in the event of the detection of a network intrusion / breach in the cyber-security perimeter of the network's demilitarized zone.
- Port for isolation of Network Port and Management Port.
- External triggers using dry-contact alarm relay.
- Script assisted switching through serial interface.
- *Fail-safe. The unit itself should never becomes a point of failure, even in power down condition.*

Implementing an effective countering defence policy against cyber-attacks and cyber-terrorism is becoming increasingly critical as the utility communication systems migrate from legacy TDM infrastructure networks to IP packet-based networks. The transition to more advanced and efficient communication systems which serve a distributed energy grid and metering resources also results in an increase of such network's vulnerability.

Gaining sensitive operational data through undetected intrusions that result from firewall breaches, the presence of trojans as well as malware which can be planted or introduced from within, in any vulnerable point of the network may result in catastrophic outcomes. These threats may be result of the state sponsored adversaries or just bad-actors acting independently to initiate the cyberattacks.

In view of this, it has become imperative that effective mechanisms are put into place not only to prevent such attacks but also to detect any unlawful and unwarranted activities that may already be taking place within the network due the presence of trojans, viruses or

malware that would open “holes” for back-door entry from within the existing firewalls resulting in a cyber-attack and cripple a nation’s utility infrastructure.

Firewalls alone cannot form the centrepiece of the cyber-security strategy as firewall can be breached not only from outside but from the inside by trojans, viruses or malware which may have been planted or introduced these from within the most vulnerable points of the network.

The artificial air gap created between IT and OT Systems by deploying only firewalls between any IT and OT System can be easily circumvented by any insider or any outsider. In short, having only firewalls as a tool to address a cyber-security defence strategy is a myth.

Cyber-attacks can be initiated through techniques of initial access, execution, persistence, privileged access, defence evasion, from outside threats or trusted insiders, command and control.

The basis of any Cyber Security Defence Strategy will be to foil cyber-attacks and intrusions that may compromise the Utility communication infrastructure, Power Supply Systems and render the operations in-secure and vulnerable.

A few of the essential points that are identified and are being listed below for implementation of an effective and definitive counter cyber-defense strategy:

1. Install “Early Warning and Response Systems” behind firewalls to detect cyber security incidents for mitigation of such cyber threats.
2. Safeguarding computer systems using early cyber-attack warning and intrusion detection devices with suitable audio-visual alerting mechanisms.
3. Detecting cyber-attacks on SCADA and ICS systems.
4. Detecting cyber breaches in the IT and OT networks and installing suitable alerting mechanisms.
5. Detecting data leaks to protecting critical organizational data.
6. Installing capability of conducting forensic analysis in real time.
7. Creating Isolatable Operational Zones, which would include:
 - a) To have the capability to automatically carry out physical asset isolation (the ability to isolate a specific location or an individual telecom rack which may be source of the threat.

- b) Installing Network Isolation Switches to instantly disconnect the critical zones within the LAN network from the WAN network in the event of the detection of a cyber-attack.
 - c) Implementing automatic hard isolation of all **back-up** OT Systems (such as NAS/SAN, Data Storage Servers) from any network facing IT infrastructure in the event that a network breach is detected to ensure that the back-up sensitive data always remains un-compromised and protected.
 - d) Create operational zone isolation and mechanisms of islanding of all critical assets such as protection relays, bay-control units and data storage devices in the event that a network breach is detected.
- 8. Identification of the network vulnerabilities which may be specific and unique to a particular network and suitably addressing them.
 - 9. Maintaining network reliability and network resilience by implementing automatic failover switches which physically move and reconnect all critical zones and assets such as "RTUs", "SCADA Servers" and related "Critical Digital Assets" to standby transmission equipment and standby transmission routes.
 - 10. Conducting regular cyber security audits.
 - 11. Having a comprehensive and complete visual presentation of entire IT communication network with the help of a comprehensive Network management System (NMS) for monitoring of all network assets from a central and multiple remote locations with user assignment and strong access controls covering the following:
 - Real-time monitoring of Firewall, Routers, Data Storage Servers to detect against network intrusions, trojan or malware activity and to provide resilience to ransomware attacks, DoS attacks, etc.,
 - Creating locational redundancy to monitor the cyber-security status.

A comprehensive Network Management System will further enhance operational visibility of all cyber-security assets and greatly fortify the organizations IT infrastructure through improved surveillance and real-time management and control.

The overall comprehensive solution which would emerge would encompass the implementation of intrusion network-detection and early-warning alerting systems at various points or the network and effectively assist in the implementation of a comprehensive counter-defense strategy which shall automatically execute in an eventuality that a cyber-attack or network breach is detected and protect of all Utility communication infrastructure and Critical IT infrastructure, and Digital Assets.