# Grid Cybersecurity: DLC Approaches and Considerations

November 22, 2022

# DLC Current Cybersecurity Approaches

## Discussing DLC's Present Day Approach to Grid Cybersecurity

# DLC Current Cybersecurity Approaches

## Configuration Monitoring, Incident Response, and Network Security

- Maintaining consistent and accurate configurations through Configuration Monitoring is essential to the security of any IT environment, especially those supporting OT and control center grid operations.

- DLC's Configuration Monitoring program covers more than basic software/OS versioning, ports and services, malware/IDS definitions, and security patches.
  - Recent enhancements to extend this program element to the file executable level further helps detect the deployment of malicious files/payloads within a network.

- To ensure the efficacy of our Incident Response plan, regular interactive drills are conducted throughout the year at various scales, focused on real-world industry events and attacks. These drills are carried out on both IT and OT systems alike.

- In order to enforce network security at the point of ingress into the IT transmission and distribution networks, DLC uses a combination of firewalls, security gateways, intrusion detection systems, and additional access controls such as MFA.
  - Network security controls are employed both at the control center end of the network, as well as down to the individual substation level.

# DLC Current Cybersecurity Approaches

## Security Event Monitoring, Vulnerability Management, and Patch Management

- In addition to typical security event monitoring activities, targeted alerting is employed on system events such as unexpected idle timeouts. These are critical to monitoring for potential malicious system outage actions, such as those performed under the guise of known operations.

- The risk of looking at NERC CIP compliance as an end-goal rather than a minimum guideline can lead to complacency around the frequency of Vulnerability Management practices.
  - Vulnerability scans are performed at the start and end of every month to align with patching cycles.
  - For Vulnerability Management on OT devices, a strict practice of passive packet monitoring should be used for identification of known vulnerabilities in field device firmware versions. When necessary to interrogate a device beyond firmware version identification, bench/test lab scanning is preferred.

- Our patch management program works not only to promptly address known system vulnerabilities, but also to mitigate vendor/supply chain risks during patching.
  - Careful inspection of patch sources as well as systematic validation of file hashes ensures the integrity and authenticity of every patch before entering the environment.

# DLC Grid Cybersecurity Concerns

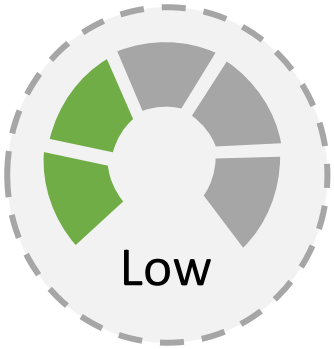
## Highlighting DLC's Areas of Concern for Grid Cybersecurity

# DLC Grid Cybersecurity Concerns

## Assessment of Current Risks/Concerns Facing The Energy Sector

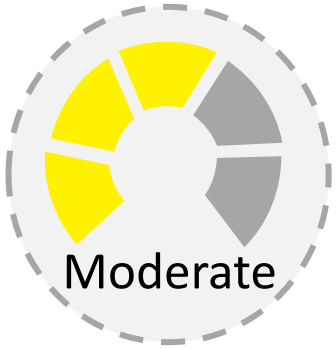

**Risks:**

- External DDOS and other rudimentary brute-force attacks.



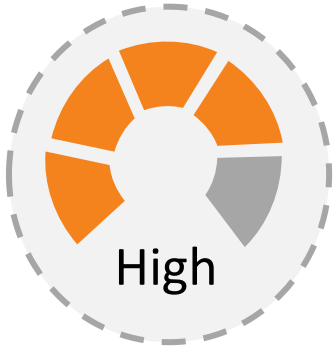

**Risks:**

- Operational time expenditures for demonstrating Compliance with evolving regulatory models and requirements.



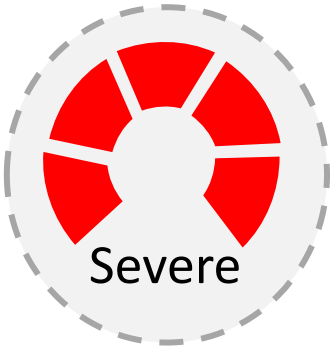

**Risks:**

- Inability to effectively leverage cloud-based security technologies.
- Coordination between Cyber and Physical Security teams.
- Proper implementation of identity management controls across IT and OT technologies.




**Risks:**

- Legacy OT equipment – patching, access control, and monitoring.
- Talent shortage of ICS-focused Cybersecurity professionals.
- Insider threat and 3rd party supply chain compromises.
- Proper Incident Response coordination and information sharing between IT and OT teams.




**Risks:**

- Proliferation of DERs/Microgrids and associated security controls.
- Lack of Cybersecurity visibility into device/network activity at distribution substation level.
- Ability to rapidly identify events such as grid misoperation and quickly isolate compromised assets/accounts from the network.
- Nation-state APTs and development of advanced malware/killware specifically targeting critical infrastructure.