**Tratans Energy Co. Intelligence Requirements**

**IR-1:** Identify external cyber threats targeting the energy sector.

**PIR-1:** Identify Advanced Persistent Threat actors targeting the energy sector.

**SIR-1.1:** Identify what APT groups have recently targeted energy companies.

**Data Source:** MITRE ATT&CK Groups

**Internal/External:** External

**Funding:** No

**Frequency:** Biannually

**Format:** HTML or STIX

**Supports Info Sharing:** No

**Admiralty Code:** A2

**SIR-1.2:** Describe the threat reconnaissance activity that has occurred today.

**Data Source:** IDS logs

**Internal/External:** Internal

**Funding:** Yes

**Frequency:** Daily/Real Time

**Format:** JSON

**Supports Info Sharing:** No

**Admiralty Code:** A2

**SIR-1.3:** Identify TTPs recently used by APTs.

**Data Source:** CISA

**Internal/External:** External

**Funding:** No

**Frequency:** Weekly

**Format:** HTML

**Supports Info Sharing:** Yes

**Admiralty Code:** A1

**SIR-1.4:** Identify potential motivations of APT to target Tartans Energy Co.

**Data Source:** Business Impact Assessment

**Internal/External:** Internal

**Funding:** No

**Frequency:** Annually

**Format:** PDF

**Supports Info Sharing:** No

**Admiralty Code:** A3

**PIR-2:** Identify vulnerabilities in energy sector infrastructure commonly exploited by adversaries.

**SIR-2.1:** Identify risks and vulnerabilities associated with 3rd party vendors.

**Data Source:** Third-party audit report

**Internal/External:** External

**Funding:** Yes

**Frequency:** Quarterly

**Format:** PDF

**Supports Info Sharing:** No

**Admiralty Code:** B2

**SIR-2.2:** Identify unauthorized access or anomalies on OT systems.

**Data Source:** OT monitoring logs

**Internal/External:** Internal

**Funding:** Yes

**Frequency:** Real-time

**Format:** JSON

**Supports Info Sharing:** No

**Admiralty Code:** A2

**SIR-2.3:** Describe recent attack attempts on critical control systems.

**Data Source:** CISA ICS

**Internal/External:** External

**Funding Required:** No

**Collection Frequency:** Weekly

**Format:** HTML

**Supports Info Sharing:** Yes

**Admiralty Code:** A1

**SIR-2.4:** Identify externally accessible assets within the Tartanss Energy Co. infrastructure that may expose vulnerabilities.

**Data Source:** Attack Surface Management tool

**Internal/External:** External

**Funding Required:** Yes

**Collection Frequency:** Daily

**Format:** JSON

**Supports Info Sharing:** No

**Admiralty Code:** A3