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

Data Source: MITRE ATT&CK Groups

Monitoring & Mining Activity: The MITRE ATT&CK Groups are updated along with the biannual MITRE ATT&CK updates. Potential notifications of updates will come through email monthly from the MITRE 360 newsletter.

Workflow Trigger: When a new update is published to the APT group profiles on MITRE that targets the energy sector.

Workflow Steps:

1. CTI Analyst initiates the biannual review of MITRE ATT&CK Group profiles using the MITRE Sync tool.

2. Profiles are scanned using keyword filters such as “energy,” “ICS,” “infrastructure,” and “SCADA.”

3. Each group identified as targeting energy companies is compiled into a working list.

4. CTI Analyst cross-references each group against existing internal threat profiles.

5. If the group is already tracked internally:

    a. Document any changes in behavior, tools, or TTPs.

    b. Update the internal group profile

    c. STOP WORKFLOW.

6. If the group is newly identified:

    a. Create a new APT profile.

    b. Include details such as targeting scope, suspected nation-state affiliation, and TTPs.

    c. Forward the new profile to the threat modeling team for review.

7. A summary of findings and intelligence implications is drafted.

8. Profiles are logged in the CTI database and tagged accordingly.

Reporting Activity: A biannual report of newly identified or updated APT groups targeting the energy sector is delivered to the Threat Intelligence Manager, shared with the Threat Hunting and Incident Response Teams, and briefed during the quarterly cybersecurity risk review with the CISO.

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

Data Source: IDS logs

Monitoring & Mining Activity: Intrusion Detection System logs are monitored in real-time with automated rule sets for common recon indicators.

Workflow Trigger: An adversarial reconnaissance signature is detected in real-time logs. (i.e., port scanning, DNS enumeration, repeated unauthorized queries)

Workflow Steps:

1. IDS triggers an alert indicating potential reconnaissance activity.
2. Alert is automatically forwarded to the SIEM platform and assigned to a Tier 1 SOC Analyst.
3. Tier 1 SOC Analyst reviews source IP, destination, scan pattern, and time
    a. If the activity is determined to be a false positive:
        i. The analyst documents the false positive in the incident log.
        ii. Adds the scanner signature to the allowlist.
        iii. STOP WORKFLOW.
    b. If the alert is valid but not malicious:
        i. Log the event in the daily reconnaissance activity tracker.
        ii. Inform the system owner and flag the source.
        iii. STOP WORKFLOW.
4. If the alert is determined to be a credible reconnaissance threat:
    a. Escalate the incident to a Tier 2 SOC Analyst.
    b. Log the source IP and behavior indicators.

5. Tier 2 SOC Analyst performs more in-depth analysis using WHOIS, threat intelligence feeds, and geolocation if possible.

6. The analyst checks if the source IP is part of a known APT scan infrastructure or public scanner.

    a. If the source IP is known to be malicious:

        i. Add IP to firewall blocklist.

        ii. Notify the Network Security team.

    b. If the source is unknown:

        i. Flag IP to watchlisting, consider blacklist for repeats

7. The final summary is added to the incident management report.

Reporting Activity: Recon incidents are compiled into a daily report that is sent to the threat intel and network operations teams. A weekly recon summary with trends and attacker origin patterns is shared with the CISO and used for threat landscape reviews.

SIR-1.3: Identify TTPs recently used by APTs.

Data Source: CISA

Monitoring & Mining Activity:
Weekly CISA reports are manually reviewed by CTI analysts. The reports include threat briefings and public alerts about emerging TTPs used by adversaries.

Workflow Trigger: A new CISA report is released that describes TTPs used by threat actors relevant to the energy sector.

1. CTI Analyst receives and reviews the weekly CISA threat advisory.
2. Extract all techniques, tactics, and procedures mentioned, referencing MITRE ATT&CK techniques when possible.
3. TTPs are categorized based on phase.
4. Each TTP is compared to existing SIEM detection and threat-hunting capabilities.
    a. If TTP is already covered:
        i. Confirm detection efficacy through an alert test.
        ii. Document status in the TTP tracking sheet.
        iii. STOP WORKFLOW.
    b. If TTP is not covered or partially detected:
        i. Create new detection logic or update current rules.
        ii. Notify the SOC team for detection implementation.
5. Analyst updates TTP database and flags emerging trends for threat-hunting sprints.
6. New techniques are distributed to the red team for adversary emulation exercises

Reporting Activity:
A weekly TTP change report is shared with the SOC, threat hunting, and red team Units. A monthly TTP trend dashboard is presented to the CISO.

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

Data Source: Business Impact Assessment

Monitoring & Mining Activity: The business impact assessment is created internally and is reviewed annually or when significant changes in the organization's operations occur. The document is analyzed manually for indicators that may attract attention from threat actors.

Workflow Trigger
Release of an updated business impact assessment or announcement of a major corporate initiative, including geopolitical, economic, and environmental initiatives.

Workflow Steps

1. Cyber Risk Manager receives the latest BIA document from the risk and compliance team.

2. The document is parsed for key operations, intellectual property, leadership profiles, partnerships, and politically sensitive areas that are of interest to currently identified APTs.

3. CTI analyst maps identified elements to known APT group motivations.
    a. If no high-value or politically sensitive targets are found:
        i. Record the result in the annual risk posture report.
        ii. STOP WORKFLOW.
    b. If indicators of APT attracting assets or projects are found:
        i. Create an internal motivation map connecting assets to APT motivations.
        ii. Update the threat model used in the new Threat Intelligence Fusion Center.
        iii. Cross-reference with known APT campaigns and update intelligence profiles accordingly.

4. Deliver an internal intelligence memo explaining how business operations may increase threat exposure.

Reporting Activity:

An annual Threat Motivation Assessment report is shared with executive leadership, the Cybersecurity Strategic Planning Group, and the CISO. High-risk findings may trigger a risk response initiative.

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

Data Source: Third-party audit report

Monitoring & Mining Activity: Quarterly audit reports from vendors are reviewed manually. Reports include security questionnaires, vulnerability assessments, and compliance certifications

Workflow Trigger: Receipt of a new quarterly audit report from a third-party vendor, or identification of a vendor as newly high-risk.

Workflow Steps:

1. The vendor risk analyst retrieves the audit report from the shared governance folder.

2. The report is reviewed for unpatched CVEs, expired certificates, weak controls, and compliance gaps.

    a. If a critical vulnerability is found:

        i. Notify the vendor management/relations team

        ii. Demand a mitigation plan or timeline within 7 days.

    b. If vulnerabilities are minor or mitigated:

        i. Record status in the vendor risk tracking system.

3. Analyst rates vendor on impact on Tartan Energy Co.'s infrastructure based on system dependencies.

4. Vendor's risk level is updated in the centralized Vendor Risk Register.

5. If the vendor is deemed high-risk, security controls are reviewed, and third-party access is limited pending review.

Reporting Activity: Quarterly Vendor Risk Review sent to procurement, legal, and the fusion center. Critical issues trigger an executive summary for the CISO.

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

Data Source: OT monitoring logs

Monitoring & Mining Activity: Operational technology systems are continuously monitored using behavior analytics and anomaly detection tools. Logs are collected and analyzed in real-time with a SIEM platform.

Workflow Trigger: Detection of abnormal behavior or unauthorized access attempts in the OT environment, such as lateral movement, abnormal traffic, or unexpected user logins.

Workflow Steps:

1. OT anomaly detection engine flags a deviation from established device normal behavior baselines.

2. Alert is pushed to the OT Security Dashboard and assigned to the OT security engineer.

3. Engineer investigates:

    a. Validates alert source, time, and behavior pattern.

    b. Checks against known maintenance windows or OT activity schedule.

        i. If activity is benign:

            1. Document and whitelist the event.

            2. STOP WORKFLOW.

        ii. If activity is suspicious:

            1. Isolate the affected segment or device from the control network.

            2. Contact the asset owner for access validation.

            3. If an external IP is involved, notify the SOC for support.

4. Conduct a forensic snapshot.

5. Log activity in OT incident tracking platform and mark as under investigation until the investigation is completed.

Reporting Activity: Real-time incident alert sent to OT SOC, Engineering, and Facilities. Weekly summary of OT anomalies delivered to the OT Security Lead and monthly briefing to the CISO.

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

Data Source: CISA ICS

Monitoring & Mining Activity: CISA's ICS advisories are reviewed weekly by CTI analysts. The reports highlight active exploitation techniques and vulnerabilities affecting control systems, including industrial protocols and components.

Workflow Trigger: CISA publishes a new ICS advisory relevant to energy sector control systems or assets used within Tartan's infrastructure.

Workflow Steps:

1. CTI analyst receives an alert for a newly published ICS report.

2. The report is scanned for mentions of vendors, software, or devices used by Tartan Energy Co.

3. Analyst extracts affected components and CVEs and checks Tartan's asset inventory for matches.

    a. If Tartan uses the affected system or software:

        i. Notify the ICS engineering team and request vulnerability confirmation.

        ii. Check patch status and compensating controls.

    b. If Tartan is unaffected:

        i. Record the advisory in the archive

        ii. STOP WORKFLOW.

4. Risk level is assessed and assigned based on severity, ease of exploitation, and asset criticality.

5. Controls are reviewed, and additional detection or segmentation is recommended if needed.

Reporting Activity: Relevant ICS vulnerabilities and trends are summarized weekly and sent to the Control Systems Team and the CISO. Emergency advisories are escalated directly to Incident Response if a high risk is noted.

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

Data Source: Attack Surface Management tool

Monitoring & Mining Activity: ASM tools run daily scans to identify externally facing systems and applications. JSON-formatted alerts are generated for newly discovered IPs, services, or vulnerabilities exposed to the internet.

Workflow Trigger: Detection of a newly exposed system, port, or vulnerability on a previously known asset with changed exposure status.

Workflow Steps:

1. The ASM tool sends a daily JSON report to a monitoring dashboard.
2. Vulnerability analyst reviews the list of externally accessible assets and matches each entry with the approved asset list.
    a. If the asset is approved and unchanged:
        i. Mark as “Verified”
        ii. STOP WORKFLOW.
    b. If the asset is unapproved or the exposure has changed:
        i. Notify the asset owner and the infrastructure team.
3. Determine if the exposure was intentional, misconfigured, or unintended.
    a. If the asset is not needed externally:
        i. Request immediate removal or a firewall rule change.
    b. If the asset is required externally:
        i. Ensure it has secure configurations and has appropriate monitoring systems attached
4. Conduct a full vulnerability scan.

5. Add the asset to the Attack Surface Tracker with updated security controls.

Reporting Activity: Daily exposed asset report is generated and sent to the SOC and Vulnerability Management team. A monthly external risk posture update is provided to the CISO and SOC leadership.