A key regulatory agency in the Middle East for the telecom & IT sector was looking to modernize its cybersecurity infrastructure to better protect public and private sector entities in the sector through collective defense. They sought a suite of solutions that would allow them to automate and centralize investigations for incidents reported by the entities while engaging in bidirectional threat intelligence to boost overall incident response and vulnerability management processes.

**CHALLENGES**

1. **Limited Threat Intelligence Sharing**
   Limited and delayed sharing of threat intelligence among the agency’s internal security teams and connected entities.

2. **Manual Security Operations**
   Slow, manual processes for vulnerability scanning, threat enrichment, and investigations and management of reported incidents.

3. **Missing Orchestration Capability**
   Extra efforts required for data transfer and actioning due to missing connecting layer between SOC tools.

4. **Ineffective Vulnerability Alerting**
   Reliance on traditional communication channels for alerting stakeholders about critical vulnerabilities.
SOLUTION

Cyware’s Intel Exchange (CTIX), Respond (CFTR), and Orchestrate platforms were deployed on the agency’s network to foster collective defense.

**Intel Exchange** is a STIX/TAXII-compliant automated Threat Intelligence Platform (TIP) designed for ingestion, enrichment, analysis, prioritization, actioning, and bidirectional sharing of threat data. The platform ingests and processes enriched threat intelligence from various sources augmenting incident response and vulnerability management workflows for the agency’s SOC.

**Respond** is an automated incident analysis and threat response platform purpose-built to enhance threat visibility and threat management. It allows the agency to connect the dots between reported incidents and enriched intelligence, and manage response workflows in a fully automated manner while engaging all stakeholders.

**Orchestrate** is a vendor-neutral, low-code orchestration and automation platform that serves as a connecting fiber between all the cybersecurity and IT tools deployed in the agency’s SOC. The platform eliminates manual efforts needed in orchestrating data and triggering automated actions among the agency’s existing ITSM, vulnerability scanning, Intel Exchange, and Respond platforms.

Collective Defense Network for Telecom and IT Sector with Fully Automated Threat Response, Vulnerability Management, and Threat Intelligence Sharing
Cyware’s platforms together transformed the agency’s security operations by streamlining incident response, enabling extensive intelligence sharing, and amplifying vulnerability management by integrating enriched threat intelligence. The key use cases solved include:

1. **Threat Intelligence Aggregation and Enrichment**
   Multi-source threat intelligence aggregation, indicators of compromise (IOC) parsing, enrichment, and dissemination to all public and private entities to improve threat triaging and prioritization.

2. **Bidirectional Threat Intelligence Sharing**
   Automated rules-based sharing of actionable indicators of compromise (IOCs) as STIX packages via TAXII protocol from the agency to public and private entities for proactive threat blocking.

3. **Threat Intelligence Notifications and Incident Ticketing**
   Automated threat intelligence notifications and incident ticketing for the Penetration Testing and Vulnerability Assessment (PTVA) team of the agency.

4. **Incident Response Automation**
   Automated incident response and management by fetching incident data, performing automated analysis, IOC enrichment, and sending back incident updates, through orchestration playbooks.

5. **Automated Vulnerability Scanning and Management**
   Simplified vulnerability management by enabling automated scans, creating incidents for critical issues, collecting enriched threat intelligence, and syncing up the data across all tools in real time.

6. **Automated Vulnerability Alerting**
   Enhanced vulnerability alerting for public and private entities by collecting enrichment details from the TIP and vulnerability scanning tools, and updating alerts in the incident response tool.

7. **SOC Roster Management**
   Enabled 24x7 functioning of incident response teams in an organized manner for round-the-clock threat management for all the sectoral public and private entities.
BENEFITS AND OUTCOMES

The deployment of Cyware’s platforms reinforced the agency’s security posture and allowed it to safeguard its group entities.

- **Collective Defense**
  Cyware helped stimulate collaboration among the agency’s internal teams and its ecosystem by providing automated threat intelligence sharing and operationalization.

- **Streamlined Security Operations**
  Cyware solutions streamlined incident response, vulnerability management, intelligence enrichment, and sharing, thereby making all connected entities more resilient.

- **Proactive Threat Actioning**
  Cyware’s solutions helped the stakeholders perform effective threat lifecycle management and proactively counter threats using enriched intelligence.

- **Enhanced Incident Response**
  Cyware’s platforms accelerated the agency’s incident response processes with their advanced orchestration and automated incident analysis features.

- **Comprehensive Threat Visibility**
  Cyware helped unlock 360-degree threat visibility and oversight over the agency’s security operations through its roster management features.