CYWARE™ | Datasheet

Cyware for State, Local, Tribal, Territorial (SLTT) Governments

Strengthen Your Cyber Defenses with Unified Threat Intelligence Management

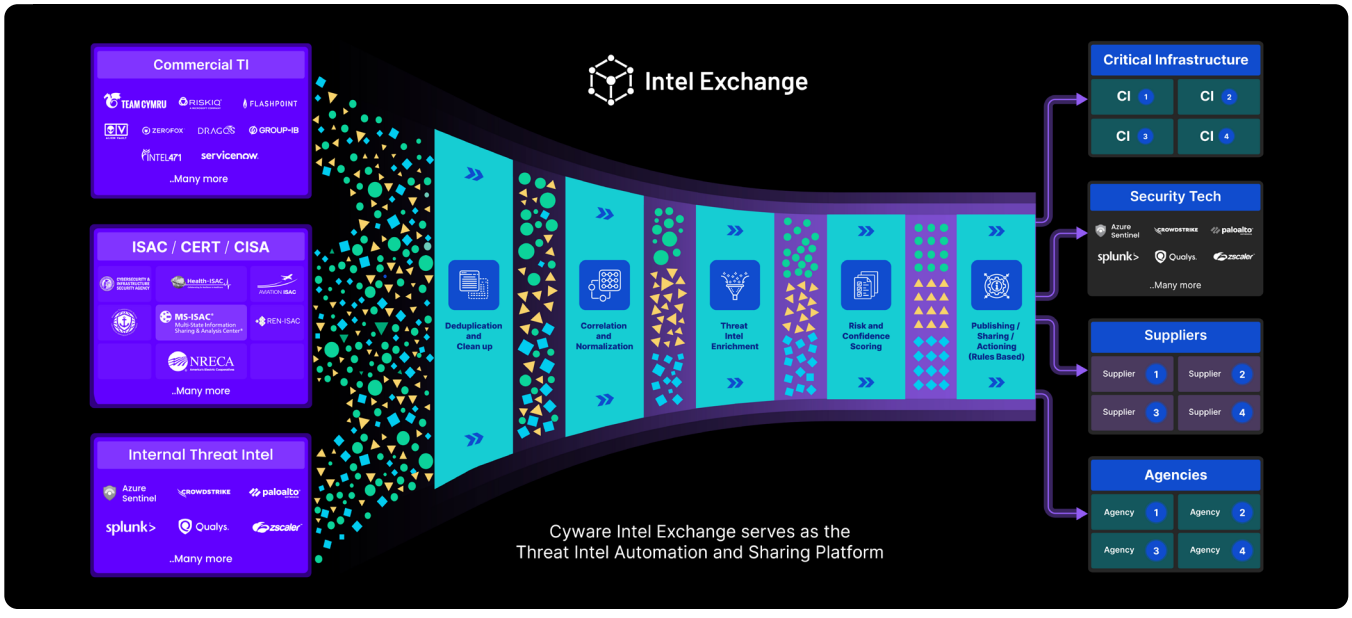
SLTT Cyber Threat Intelligence (CTI) teams play a mission-critical role in safeguarding sensitive data, ensuring seamless cyber operations, and coordinating cross-government threat mitigation. However, rising cyber threats—ransomware, DDoS attacks, and supply chain vulnerabilities—coupled with fragmented security tools, workforce shortages, and budget constraints make cyber defense increasingly complex.

To combat these threats, **SLTT CTI operations must evolve, shifting from traditional intelligence collection to real-time, actionable insights that drive rapid response.** Automating intelligence workflows, enhancing cross-agency collaboration, and integrating cost-effective, scalable security solutions are key to ensuring resilient, mission-critical cybersecurity operations.

How Cyware Transforms the Way SLTT Governments Defend Against Evolving Cyber Threats

Cyware's AI-powered solutions, deployable across cloud, on-premise, and hybrid environments, empower SLTT governments to strengthen their cybersecurity posture amid evolving threats and regulations. As a **StateRAMP Readiness-in-Process** platform, Cyware goes beyond monitoring—transforming cyber intelligence into action, streamlining security operations, enhancing cross-agency coordination, and delivering cost-efficient, mission-critical protection.

Your End-to-End Threat Intelligence Management System



CYWARE™

Unified Threat Intelligence Ingestion & Enrichment

Automated Data Collection – Ingest intelligence from Team Cymru (out-of-the-box), OSINT, ISAC/CERT advisories, and internal security tools like EDR, firewalls, and network sensors for full visibility.

Seamless ISAC & CISA AIS Integration – Directly integrate with CISA AIS, MS-ISAC, Aviation ISAC, Health ISAC, Maritime ISAC, REN-ISAC, and NRECA to strengthen collaboration.

Broad Format Compatibility – Normalize data from APIs (SQL, REST), structured formats (STIX, JSON, XML), and unstructured sources (PDFs, emails, social media).

Contextualized Threat Enrichment – Enrich intelligence with threat actor profiles, campaign analysis, attack infrastructure, and related incident data.

Intelligent Threat Normalization, Correlation & Prioritization

Automated Normalization & Scoring – De-duplicate, standardize, and rank threat intelligence using predefined/custom rules for actionable insights.

Confidence-Based Threat Evaluation – Assigns confidence scores based on source reliability, corroboration across feeds, and analyst-defined criteria.

Contextual Tagging & Marking – Categorizes threat intelligence with customizable tagging to streamline investigation and prioritization.

Optimized Threat Intelligence Utilization – Leverage scoring insights and the ROI dashboard to assess feed performance and maximize cost efficiency.

Accelerated Threat Investigation & Analysis

Actionable Threat Mapping – Visualize and correlate threats with TTPs using MITRE ATT&CK, Cyber Kill Chain, and the Diamond Model for deeper analysis.

Integrated Threat Analysis – Enhance investigations with visual threat mapping, historical linkages, and automated STIX 2.1-based correlations.

Automated Sandbox Detonation (Optional) – Analyze suspicious files in a secure environment and extract indicators to strengthen forensic investigations.

Seamless Investigation Workflow – Integrate with forensic tools, SIEMs, and external data sources to streamline threat hunting and response.

Custom Dashboards & Reporting – Build dynamic dashboards, manage threat actor libraries, track TTPs, and generate centralized intelligence reports.

Automated Actioning & Orchestration

Seamless Security Control Automation – Integrate with security tools commonly used by SLTT agencies, including SIEMs, firewalls, and endpoint security solutions for automated actioning.

Intelligent Threat Intelligence Sharing – Enable real-time, event-driven, or scheduled receipt of indicators with key stakeholders, including MS-ISAC, CISA AIS, and other critical infrastructure ISACs.

Bidirectional Data Exchange – Seamlessly integrate with ITSM tools like ServiceNow and CRM platforms to unify intelligence sharing and incident response workflows.

For more information:

111 Town Square Palace Suite 1203 #4 Jersey City, NJ 07310 **cyware.com** | government@cyware.com

CYWARE™