Final Project, Part I: Cyber Threat Intelligence Program Plan - Proposal

Joshua A. Wortz

University of San Diego

CSOL-580

Dr Hollandsworth

04/06/2026

TABLE OF CONTENTS

TABLE OF CONTENTS
Executive Summary
CTI Program Plan
Introduction
Threat Intelligence Requirements
Data Collection and Sources
Analysis and Processing
Operationalizing Intelligence
Incident Response and Management
Evaluation and Improvement
References

Executive Summary

CyberTech Innovations Inc. faces a sophisticated, global threat landscape targeting its core software development assets and distributed workforce. To address these challenges, this proposal outlines the transition to an intelligence-led security posture.

The Cyber Threat Intelligence (CTI) Program moves the organization beyond reactive defense by integrating high-fidelity data collection, advanced analytical frameworks, and proactive incident response. By leveraging global intelligence sources and internal telemetry, the program aims to anticipate adversary tactics, such as intellectual property theft and ransomware, before they impact operations.

Key outcomes include a measurable reduction in detection times, optimized resource allocation for vulnerability management, and enhanced strategic decision-making for leadership. This plan provides a scalable roadmap to protect CyberTech's innovations and maintain a resilient defense across its North American, European, and Asian offices.

CTI Program Plan

Introduction

At its core, the Cyber Threat Intelligence Program at CyberTech Innovations is about one thing: keeping our software development lifecycle secure and protecting our brand from a global field of adversaries. In today's world, we cannot just think about network boundaries; our "attack surface" lives in our CI/CD pipelines, third-party code repositories, and even the personal identities of our remote team members. Because of this, our CTI efforts cover everything from internal telemetry and cloud environments to the external actors actively targeting the tech sector.

We are not just collecting data for the sake of it. Our goal is to find actionable insights that actually help us make better, risk-based decisions. By setting clear requirements, we can stop chasing every alert and start prioritizing the threats that truly matter to our global operations, like intellectual property theft or a compromise in our supply chain.

Threat Intelligence Requirements

A solid CTI program has to start with a real understanding of what we are up against. For a company like ours, the biggest threats come from those looking to exploit the software supply chain. We have seen a trend in which attackers target intermediaries to abuse trusted relationships, with a massive ripple effect. We are essentially facing two fronts: cybercriminals looking for a quick payout, and state-sponsored groups like ChamelGang, known for hiding in networks using the very tools we use at work.

To stay ahead, we focus on three levels of intelligence. First, we need tactical data, the real-time indicators that help our security controls block attacks. Next is operational intelligence, where we dig into the specific techniques used by groups like APT41 and Andariel, focusing on their use of custom malware. Finally, we need strategic intelligence for our leadership team. This helps them see the big picture, like how geopolitical shifts might change the threat level for our offices in Asia or Europe.

Data Collection and Sources

For a global software firm, effective data collection means blending internal telemetry with external threat signals. Inside the company, our priority is "forensic readiness." This involves capturing high-fidelity logs from Endpoint Detection and Response (EDR) platforms and all cloud-native management portals. Since our software development happens across distributed environments, we must monitor GitHub repositories using Security APIs. This step is critical for detecting unauthorized commits or any secret leakage (Reco, 2026). Ultimately, this internal visibility helps the CTI team compare normal baseline activity against potential anomalies, such as those suspicious POST requests to script directories that could signal a web shell presence (CERT-EU, 2026).

On the external side, we use a tiered strategy that carefully balances open-source intelligence (OSINT) with commercial and community-driven feeds. The program automatically ingests data from industry platforms such as Recorded Future and CrowdStrike to generate sector-specific insights. Crucially, our active participation in the IT-ISAC and engagement with CERT-EU creates a collaborative defense layer. This ensures that when a peer organization detects a threat, CyberTech can immediately implement preventive measures (NIST, 2016).

Finally, all collected data moves through a centralized Threat Intelligence Platform (TIP). This platform normalizes and processes the data, deduplicates indicators, and most importantly, prevents analysts from being flooded with high volumes of low-fidelity alerts.

Analysis and Processing

The analysis phase is where raw data is transformed into a cohesive narrative that drives defensive action. At CyberTech Innovations, we utilize the Diamond Model of Intrusion Analysis to map the intricate relationships between adversaries, their underlying infrastructure, their specific capabilities, and the victims they target. When integrated with the MITRE ATT&CK matrix, this approach enables our analysts to visualize the entire "kill chain" and pinpoint critical gaps in our current defensive architecture. By closely examining the reconnaissance and initial access phases, such as spear-phishing attempts using sophisticated malicious lures, the team can develop highly targeted detections to intercept threats at their earliest stages.

Furthermore, our processing includes a rigorous peer-review and validation workflow designed to uphold the scientific integrity of the intelligence we produce. Technical artifacts unearthed during incident response, ranging from memory dumps to disk images, are meticulously analyzed to determine if they correlate with known threat actor clusters. By assigning clear confidence levels to every intelligence report, the CTI program ensures that all stakeholders understand the degree of uncertainty behind each assessment, helping prevent over-reliance on speculative data.

The output of the analysis phase is tailored to its audience. Strategic intelligence reports are delivered via Weekly Executive Briefings in PDF format to senior leadership. Tactical and

operational intelligence, including validated indicators, is disseminated through real-time dashboards integrated into Jira and the Security Operations Center (SOC) platform.

Operationalizing Intelligence

Intelligence only provides value when it is integrated into the security team's daily operations. At CyberTech, CTI is operationalized through a direct feedback loop with the Security Operations Center (SOC). Analysts use tactical intelligence to automate the enrichment of alerts, allowing for rapid triage and a significant reduction in the "mean time to respond." Furthermore, intelligence informs the vulnerability management process; rather than patching based on generic severity scores, the organization prioritizes vulnerabilities that CTI indicates are being actively exploited by adversaries targeting the technology sector (Recorded Future, 2022).

Beyond technical integration, intelligence is used to drive proactive defense strategies such as threat hunting and red teaming. By simulating the TTPs of sophisticated actors who use ransomware as a distraction to destroy anti-forensic evidence, the organization can test its resilience against the most catastrophic scenarios (KPMG, 2025). This proactive approach ensures the organization is not merely waiting for an alert but actively searching for subtle signs of compromise before they escalate to exfiltration.

Incident Response and Management

CTI is not just integrated into the incident response lifecycle; it transforms every security event into a valuable source of new intelligence. When an event is first identified, CTI provides the necessary context to determine if it is an isolated occurrence or part of a larger, coordinated campaign. For containment and eradication, intelligence on the adversary's command-and-

control (C2) infrastructure is key, enabling surgical blocking that minimizes disruption to operations.

A key pillar of the incident management plan is ensuring forensic readiness. Because sophisticated attackers frequently use encryption tools such as BitLocker or Jetico BestCrypt to obscure their activities, the CTI program requires preserving volatile data as an essential first response (CERT-EU, 2026). We then use this captured data to refine the organization's "collection management framework," ensuring all future defenses are built upon the technical realities observed in past incidents (NIST, 2016).

Evaluation and Improvement

CyberTech Innovations achieves long-term maturity by implementing a continuous improvement lifecycle guided by key performance indicators (KPIs). A primary metric for the program is the Mean Time to Detect (MTTD), targeting a significant 25% year-over-year reduction. We also measure intelligence effectiveness using the "signal-to-noise" ratio of the feeds ingested into the TIP, ensuring our resources are focused exclusively on high-value data. Quarterly reviews are held with key stakeholders, including Legal, HR, and the Board of Directors, to align intelligence requirements with evolving business goals. This process guarantees that the CTI program scales effectively to meet new challenges as CyberTech Innovations expands or enters new markets. Crucially, by institutionalizing a "lessons learned" phase following every major exercise, the program commits to a trajectory of constant refinement, cementing its role as an indispensable component of the organization's global resilience (Forbes, 2021).

Conclusion

The proposed Cyber Threat Intelligence Program is not merely a technical upgrade; it represents a fundamental shift toward a proactive and intelligence-driven security culture at CyberTech Innovations. By moving beyond simple indicators and focusing on adversary motivation, tactics, and strategic intent, the program will deliver measurable value: shrinking our detection window, optimizing our defensive investments, and providing senior leadership with the clarity needed to manage global risk. This program is essential for protecting our core intellectual property, ensuring the continuity of our development operations, and maintaining the trust of our customers and partners worldwide. Implementing this plan ensures that CyberTech remains resilient in the face of an ever-evolving, hostile global threat landscape.

References

CERT-EU. (2026). *Cyber threat intelligence framework and industry deep-dives*.

Forbes Technology Council. (2021). *Six key principles to building an effective cyber threat intelligence program*.

KPMG Advisory. (2025). *A decade of ransomware: Defense mechanisms and rapid response*.

National Institute of Standards and Technology (NIST). (2016). *Guide to cyber threat information sharing (SP 800-150)*.

Reco. (2026). *A guide to GitHub security APIs for enhancing repository security*.

Recorded Future. (2022). *The intelligence handbook: A roadmap for building an intelligence-led security program* (4th ed.). CyberEdge Group.