Scotty Manufacturing Inc. CTIC Development Plan

Intelligence Center Model Selection

Physical CTIC

Feature	Physical	Hybrid	Cloud
Security Control	High	Moderate	High to Moderate (provider dependent)
Cost	High	Moderate	Low
Scalability	Low	Moderate	High
Collaboration	High	Moderate	Low

A hybrid CTIC offers a balanced approach, combining the control of on-premise systems with the flexibility and scalability of cloud services. It allows sensitive operations to remain in-house while leveraging the cloud for less critical functions or data processing. This model also supports business continuity, as cloud components can serve as a fallback during on-premise disruptions, and is more scalable than a purely physical setup. It's a strong middle-ground option for organizations looking for both control and adaptability.

A cloud CTIC presents the lowest upfront cost and offers rapid deployment, making it an attractive option for organizations needing to scale quickly. It provides high flexibility, access to advanced analytics tools, and ease of maintenance since updates and infrastructure are managed by the provider. Cloud-based models also support remote access, which can benefit distributed teams or organizations aiming for a more decentralized workforce.

A physical CTIC is the best choice in this case, though. A physical CTIC provies the most security control and allows for the highest collaboration between teams in real-time across not just the threat intelligence team, but also the organization as a whole. While the startup cost is the highest of the three options, it is a strategic investment that ensures the organization maintains direct control over sensitive data, infrastructure, and internal communications. This is particularly critical in a manufacturing environment like SMI, where integration with operational technology (OT) and real-time threat visibility is essential.

Implementaion Cost: $500,000

Staffing Plan

Position	NICE Role Title	NICE Category	Description	Priority 1 = Highest Priority	Salary
CTIC Director	Executive Cybersecurity Leadership	Oversight and Governance (OG)	Sets vision, oversees all CTIC operations, and interfaces with executive leadership	1	$150,000
SOC Manager	Defensive Cybersecurity	Protection and Defense (PD)	Manages SOC employees and reviews elevated incidents	1	$148,000 [2]
Senior Cyber Threat Intelligence Analyst	Threat Analysis	Protection and Defense (PD)	Analyzes cyber threats, adversary behavior, and develops intelligence products based on reports	1	$115,000 [1]
SOC Analyst	Defensive Cybersecurity	Protection and Defense (PD)	Monitors alerts, investigates anomalies, and performs real-time threat defense	1	$85,000[2]

Systems and Facilities Security Manager	Systems Security Manager	Implementation and Operation (IO)	Ensures system-level security through configuration, patching, and risk review, as well as heping to mainint employee physical access controls	1	$76,000 [2]
Intel Collection Manager	Intelligence Collection	Implemeantaion and Operation (IO)	Coordinates intake and management of intelligence sources from treat hunte and insider threat analyst for presentation to upper managemnt	2	$110,000 [2]
Incident Responder	Incident Response	Protection and Defense (PD)	Handles cybersecurity incidents, conducts forensics, coordinates containment	2	$80,000

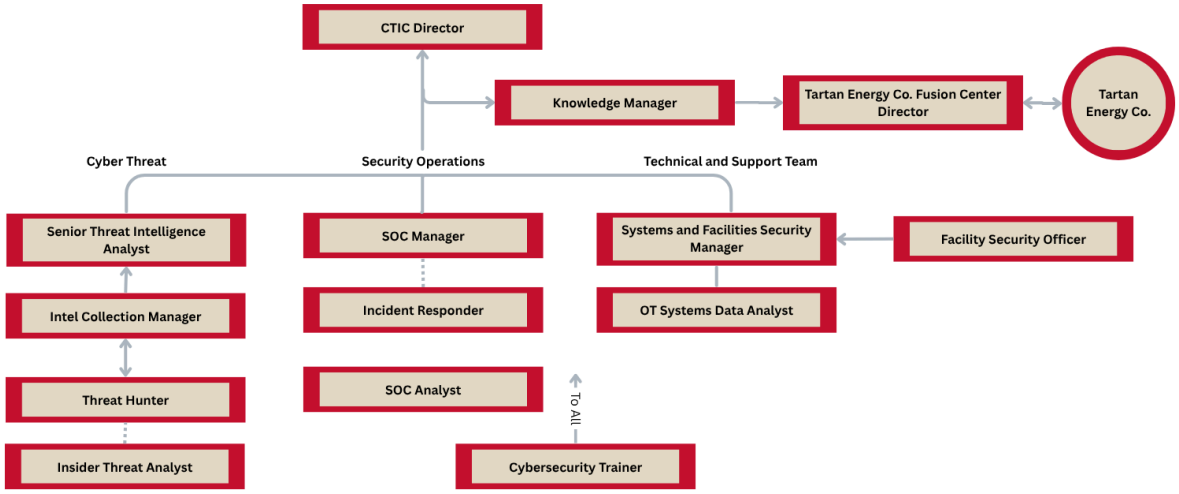
Threat Hunter	N/A	Protection and Defense (PD)	Proactively identifies advanced persistent threats within the network	2	$78,000 [2]
Insider Threat Analyst	Insider Threat Analysis	Protection and Defense (PD)	Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats	2	$78,000 [2]
OT Systems Data Analyst	Data Analysis	Implementation and Operation (IO)	Builds custom analytics, dashboards, and supports data-driven decision making	3	$75,000
Knowledge Manager	Knowledge Management	Implementation and Operation (IO)	Maintains CTIC documentation, SOPs, and structured threat knowledge	3	$83,000 [3]
Facility Security Officer	N/A	N/A	Provide physical security to the CTIC facility	3	$43,000 [5]

Cybersecurity Trainer	Cybersecurity Instruction	Oversight and Governance (OG)	Designs and delivers internal training and awareness for CTIC and org-wide users	5	$75,000
				TOTAL	$1,196,000

Technology and Tooling

Tool	**Purpose**	**Used By**	**Cost**
ELK Stack	Log analysis, SIEM functions	SOC, Data Analyst	Free (Will be self hosted)
MISP	IOC sharing and correlation	Intel Team	Free
Anomali	Threat intel aggregation	Intel Manager, SOC Manager	$50,000
VirusTotal	Quick file and URL scans	IR, Intel Team	Free
i2 Analyst's Notebook	Link analysis	Intel, Insider Threat Analyst	$50,000
Maltego	Infrastructure mapping, OSINT	Threat Hunter, Trainer	$50,000

Kali Linux	Training (possiblly red-teaming activities in the future)	Threat Hunter, Trainer	Free
Hadoop	Big data storage and analytics	Data Analyst	Free
DHS CISCP, FBI InfraGard	External threat sharing (gov)	Intel Manager, Director	Free



Year-One Budget Overview

Item	**Cost**	**Note**
Facility	**$500,000**	
Staffing	**$1,196,000**	
Software/Tooling	**$150,000**	
Data Center Upgrade	**$70,000**	To accommodate hosting the previously mentioned software, additional hardware will likely need to be purchased. Includes a new storage array with 4 new built out server nodes [6–8]
Total	**$1,916,000**	

Refrences

[1]https://www.dice.com/technologists/ebooks/tech-salary-report/salaries-by-skill.html#Skills-Appendix
[2]https://www.salary.com
[3]zippa.com
[5]govsalaries.com
[6]diskprices.com
[7]https://www.lenovo.com/us/en/p/servers-storage/servers/racks
[8]https://www.rackmountsolutions.net/