

Cybersecurity Training Reimbursement Request

Summary

The **Cyber Threat Intelligence 101** training will provide our security team with the frameworks to develop, implement, and manage an effective threat intelligence program, tailored to our organization's needs.

Employee Information

- **Name:** _____
- **Job Title:** _____
- **Department:** _____
- **Manager Name:** _____
- **Date of Request:** _____

Training Course Details

- **Course Title:** Cyber Threat Intelligence 101
- **Training Provider:** Antisyphon Training
- **Course Format:** Live Virtual
- **Course Dates/Time:** June 22nd - 23rd 10:00am-6:00pm ET
- **Certificate of Completion:** Yes
- **CEU:** 16 hours

Total Cost

\$575

- *No Travel, Lodging, or Per Diem expenses*

Operational Impact

Minimal disruption. The course is live virtual with no off-site logistics required.

Business Justification

Increases our organization's capacity to make threat hunting efforts more efficient and targeted toward our needs.

Benefits:

- Identification of threats specific to our industry/organization
- Introduction to processes and frameworks that provide greater visibility on likely, potential threats

Cybersecurity Training Reimbursement Request

Organizational Alignment

- Equips our security team with another tool to identify threats before they affect business activities
- Aligns with NIST/NICE Framework: **Threat Analysis** PD-WRL-006

Value Vs Alternative Training

The cost of this training is around **\$35 per hour** of instruction. Training with a comparable level of instruction can cost up to **\$150 per hour**. The instructor, Wade Wells, is the Lead Detection Engineer for a Fortune 30 financial company with almost a decade of experience in threat hunting, CTI, and security operations. **12 months** of Antisyphon Training Cyber Range access is included for continual practice and skill development.

Skills and Knowledge Gained

- Learn CTI frameworks, analytic techniques, and cognitive-bias mitigation strategies
 - Develop the skills to transform raw data into actionable intelligence, craft effective PIRs, model threats, and profile adversaries
 - Gain hands-on experience with OSINT, dark-web monitoring, OPSEC, AI-assisted analysis, and sector-specific intelligence use cases
-
-

Approval

Manager: _____

Decision: Approve Deny Pending

Comments:

Signature: _____

Date: _____