Cybersecurity Training Reimbursement Request

Summary

The **Network Forensics and Incident Response** training will increase the IR capability of our security team and shorten the time between “alert” and “contained” with the study of real-world incidents and hands-on exercises.

Employee Information

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

Training Course Details

- **Course Title:** Network Forensics and Incident Response
- **Training Provider:** Antisyphon Training
- **Course Format:** Live Virtual
- **Course Dates/Time:** March 30th-31st 10:00am-6:00pm ET
- **Certificate of Completion:** Yes
- **CEU:** 16 hours

Total Cost

$575.00

Operational Impact

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

Business Justification

The Network Forensics and Incident Response course teaches the concepts, process, and techniques of network analysis for incident response, increasing the speed of the IR process.

Benefits:

- Understanding technical concepts of incident handling and response
- Insight into attacker methodologies
- Various techniques and tools to uncover adversarial activity
- How to detect abuse against common protocols found in enterprise environments

Cybersecurity Training Reimbursement Request

Organizational Alignment

- Increases organizational preparedness for a cyber incident
- Aligns with NIST/NICE Framework: **Digital Forensics** PD-WRL-002

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** of instruction. The course uses real-world attack scenarios to explore an attacker's methodology, reinforcing the training with 11 hands-on exercises. **12 months** of Antisyphon Training Cyber Range access for continual practice and skill development.

Skills and Knowledge Gained

- Analyzing network packet captures with a variety of tools, techniques, and filtering options
- Extracting files and metadata from network packet captures
- Creating custom Zeek scripts to support incident response efforts
- Creating custom Zeek scripts for Zeek log enrichment
- Analyzing network flow data
- Real-world attack scenarios and techniques for response
- Methods to aid investigators when dealing with the challenges of encrypted communications

---

Approval

Manager: _____

Decision: ☐ Approve ☐ Deny ☐ Pending

Comments:

Signature: _____

Date: _____