Cybersecurity Training Reimbursement Request

Summary

The **Incident Response Simplified** course will increase the depth of leadership ability during an incident as well as the speed and efficiency of the IR process with a high quality of instruction at a lower price than other options.

Employee Information

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

Training Course Details

- **Course Title:** Incident Response Simplified
- **Training Provider:** Antisyphon Training
- **Course Format:** Live Virtual
- **Course Dates/Time:** April 3rd 10:00am-6:00pm ET
- **Certificate of Completion:** Yes
- **CEU:** 8 hours

Total Cost

$295.00

Operational Impact

Minimal disruption. The course is a 1-day, live virtual training with no off-site logistics required.

Business Justification

This training course teaches how to simplify the incident response process into an effective, repeatable plan that removes unnecessary steps and increases the speed of response.

Benefits:

- Study of the three primary threat vectors
- Outline of the two most important IR playbooks
- Review the two most critical IT assets: identity and endpoint
- Assistance in developing runbooks and playbooks for the organization

Cybersecurity Training Reimbursement Request

Organizational Alignment

- Increases organizational preparedness for a cyber incident
- Aligns with NIST/NICE Framework: **Incident Response** PD-WRL-003

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 instructor, Patterson Cake, is a former SANS instructor and the Director of Incident Response for Black Hills Information Security with two decades of experience in the development of incident-response teams, programs, and processes. **12 months** of Antisyphon Training Cyber Range access for continual practice and skill development.

Skills and Knowledge Gained

- Creating a tactical IR plan
- Simplifying an incident-response workflow
- Prioritizing operating system artifact collection and review
- Using “rapid triage workflow” scripts, Velociraptor offline collector, and KAPE for rapid endpoint investigations
- Investigating a real-world business compromise case

Approval

Manager: _____

Decision: ☐ Approve ☐ Deny ☐ Pending

Comments:

Signature: _____

Date: _____