Cybersecurity Training Reimbursement Request

Summary

The **LOLBINS vs. LOLBINS: Endpoint Threat Hunting** training equips our security team with the means and experience to discover potential, commonly missed threats within the network through endpoint artifact analysis.

Employee Information

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

Training Course Details

- **Course Title:** LOLBINS vs. LOLBINS: Endpoint Threat Hunting
- **Training Provider:** Antisyphon Training
- **Course Format:** Live Virtual
- **Course Dates/Time:** June 19th 10:00am-6:00pm ET
- **Certificate of Completion:** Yes
- **CEU:** 8 hours

Total Cost

$295

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

Operational Impact

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

Business Justification

This training enables visibility into potential malicious action that can be missed by other network defenses.

Benefits:

- Methods for detecting threats that AV and EDR commonly miss
- Guidance in triaging endpoint indicators, including acquisition and analyzation

Cybersecurity Training Reimbursement Request

Organizational Alignment

- Provides redundancy in endpoint investigation independent of AV and EDR
- Aligns with NIST/NICE Framework: **Defensive Cybersecurity** PD-WRL-001

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, Patterson Cake, is a former SANS instructor and the Director of Incident Response for Black Hills Information Security and has trained law enforcement, military, and national cybersecurity organizations on four continents. **12 months** of Antisyphon Training Cyber Range access is included for continual practice and skill development.

Skills and Knowledge Gained

- Selecting the most useful investigative artifacts for Windows/Linux endpoints
- Acquiring artifacts from one-to-many endpoints
- Understanding and analyzing key investigative artifacts
- Performing baseline comparison and least-frequency-of-occurrence analysis
- Using SOF-ELK and Hayabusa for EVTX analysis at scale

Approval

Manager: _____

Decision: ☐ Approve ☐ Deny ☐ Pending

Comments:

Signature: _____

Date: _____