

Cybersecurity Training Reimbursement Request

Summary

The **Threat Hunting on the Edge** training will increase our organization's ability to proactively defend our systems and data. Hands-on training based on real-world threats will add preemptive identification of malicious behavior occurring on the network perimeter to our security arsenal.

Employee Information

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

Training Course Details

- **Course Title:** Threat Hunting on the Edge
- **Training Provider:** Antisyphon Training
- **Course Format:** Live Virtual
- **Course Dates/Time:** June 18th 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

Prepares our security team to identify, detect, and investigate adversary activity where our systems have outside contact.

Benefits:

- Opportunity for preemptive knowledge of threats on the perimeter of our network
- Expanded awareness of threats commonly missed by traditional monitoring
- Immediate, structured process for conducting threat hunts

Cybersecurity Training Reimbursement Request

Organizational Alignment

- Enables a more secure perimeter around our systems and data by looking for threats before they have impact
- Aligns with NIST/NICE Framework: **Threat Analysis** PD-WRL-006, **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 course instructor is Troy Wojewoda, a security consultant at Black Hills Information Security and has previously held roles in host and network intrusion detection, DFIR, and threat hunting among others. 12 months of Antisyphon Training Cyber Range access is included for continual practice and skill development.

Skills and Knowledge Gained

- How to identify, detect, and investigate adversary activity at the network perimeter
 - Overcoming the unique challenges of monitoring Internet-facing infrastructure
 - How to tune sensor deployments on the perimeter
 - How to interpret telemetry from edge devices under high-volume, encrypted, or evasive traffic conditions
 - How to build hunt hypotheses grounded in adversary tradecraft
-
-

Approval

Manager: _____

Decision: Approve Deny Pending

Comments:

Signature: _____

Date: _____