

Cybersecurity Training Reimbursement Request

Summary

The **Intro to Network Threat Hunting** training will improve our security posture with expert guidance and hands-on instruction that prepares our security team for proactive defense of our systems through threat hunting.

Employee Information

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

Training Course Details

- **Course Title:** Intro to Network Threat Hunting
- **Training Provider:** Antisyphon Training
- **Course Format:** Live Virtual
- **Course Dates/Time:** June 24th 10:00am-6:00pm ET
- **Certificate of Completion:** Yes
- **CEU:** 8 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

Equips our security team with the means and experience to conduct threat hunting within our systems.

Benefits:

- A professional, expert grounding in threat hunting, including tools and methodology
- Immediately applicable threat hunting skills added to our security team

Cybersecurity Training Reimbursement Request

Organizational Alignment

- Will increase the mitigation of risk by allowing our security team to find threats before they have had an impact on the organization
- 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, John Strand, is the founder of Black Hills Information Security and former SANS instructor who has consulted hundreds of organizations concerning information security, regulatory compliance, and penetration testing. **12 months** of Antisyphon Training Cyber Range access is included for continual practice and skill development.

Skills and Knowledge Gained

- Hands-on deep packet and protocol inspection using capture and analysis tools such as tcpdump, Wireshark, and Zeek.
 - Learn to identify suspicious behaviors such as long connections, beacons, denylisted communication, and other network anomalies.
 - Develop strong log analysis skills across firewall logs, Windows Event Logs, Active Directory logs, PowerShell logs, and Sysmon.
 - Gain experience using open-source threat hunting tools such as RITA, Security Onion, Zeek, Sysmon, and Velociraptor.
-
-

Approval

Manager: _____

Decision: Approve Deny Pending

Comments:

Signature: _____

Date: _____