Sample Training Request Letter

Use the following sample request letter, or elements of it, to justify the time and budget required to complete SANS training to your manager. Simply copy and paste text into an email to your manager, then make any necessary adjustments to personalize the information. Once you hit send, you’ll be one step closer to gaining the skills required to protect your organization and advance your career.

**Subject: Request for cybersecurity training from SANS Institute**

[Decision Maker Name],

### I’m writing to request time and budget approval to take the SANS Institute’s information security course [FOR577: LINUX Incident Response and Threat Hunting](https://www.sans.org/cyber-security-courses/linux-threat-hunting-incident-response/)

The information below clarifies how this training will benefit our organization’s security, the tasks I’ll be able to perform after completing the course, and relevant cost and travel information.

**Course Description**

[FOR577: LINUX Incident Response and Threat Hunting](https://www.sans.org/cyber-security-courses/linux-threat-hunting-incident-response/) teaches the skills needed to identify, analyze, and respond to attacks on Linux platforms and how to use threat hunting techniques to find stealthy attackers who can bypass existing controls. The course addresses today's incidents by teaching hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to combat real-world breach cases. It features 23 hands-on labs plus a CTF.

**Course Objectives**

Once I’ve completed the course, I’ll be able to:

* Use the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and to remediate incidents.
* Hunt through and perform incident response on Linux systems using the SIFT Workstation
* Identify and track malware beaconing outbound to its command and control (C2) channel via analytical techniques.
* Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms.
* Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis.
* Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection.
* Track data movement as the attackers collect critical data and shift those data to exfiltration collection points.
* Recover and analyze archives and archive files (.rar, .tar, etc.) used by APT-like attackers to exfiltrate sensitive data from the enterprise network.
* Use collected data to perform effective remediation across the entire enterprise.

**Expected Cost**

I’d like to take FOR577 [fill in either: (1) “at [event name], from [start date] through [end date].” or (2) “online, with four months of access to the SANS [select OnDemand] training platform.” or (3) “Live Online, virtual from [start date] through [end date].”].

The attached unpaid invoice shows the cost of the course [retrieve this from the course registration page and attach]. Details include:

|  |  |
| --- | --- |
| Course fee | [$X,XXX] |
| Subtract Early Bird / Online Training Discount | [-$XXX] |
| GIAC Certification fee | [$769] |
| OnDemand Bundle fee | [$769] |
| Travel and Hotel\* (for live training only) | [$XXX] |
| Meals (for live training only) | [$XXX] |
| **Total estimated cost:** | **[$X,XXX]** |

\*Special hotel rates for conference attendees range from [$XXX]/night, but I must register before [xx/xx/xxxx].

**Conclusion**

I believe this course will substantially improve my ability to do the specific work we need. It’s written and taught by globally recognized experts and will deliver practical, hands-on training that I can apply as soon as I return to work.

Additional course information can be found on the SANS website at <https://www.sans.org/cyber-security-courses/linux-threat-hunting-incident-response/>

Thanks for your consideration,

[Add standard signature]

Attachment:

Unpaid Invoice for SANS training [find at XXX and attach to email]