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 [SEC401: Security Essentials - Network, Endpoint, and Cloud](https://www.sans.org/SEC401) and its associated [GIAC Security Essentials](https://www.giac.org/certification/security-essentials-gsec) (GSEC) exam.

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**

[SEC401: Security Essentials - Network, Endpoint, and Cloud](https://www.sans.org/SEC401) provides the essential information security skills and techniques needed to protect and secure critical information and technology assets, whether on-premise or in the cloud. It contains nearly 45 hours of instruction, including many hands-on labs and a final full-day exercise which will enable me to prevent attacks and detect adversaries based on our unique needs.

After completing SEC401, I’ll be able to prioritize the core areas of security and cost-effectively prevent, detect, and respond to incidents, developing effective security metrics that provide a focused playbook that IT can implement, auditors can validate, and executives can understand. I will also be able to analyze and assess the risk to our environment and tie these assessments to a security roadmap for our organization.

**Course Objectives**

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

* Create a security program that is built on a foundation of Detection, Response, and Prevent
* Address high-priority security problems within the organization
* Adapt our defenses based on adversaries’ tactics and techniques
* Better defend against ransomware
* Leverage a defensible network architecture (VLANs, NAC, and 802.1x) based on advanced persistent threat indicators of compromise
* Understand the Identity and Access Management (IAM) methodology, including aspects of strong authentication (Multi-Factor Authentication)
* Understand and leverage the strengths and differences among the top three cloud providers (AWS, Microsoft Azure, and Google)
* Identify visible weaknesses of a system using various tools and, once vulnerabilities are discovered, configure the system to be more secure
* Determine the content of network communication using tools such as tcpdump and Wireshark
* Use Windows, Linux, and macOS command line tools to analyze a system looking for high-risk indicators of compromise
* Build a network visibility map that can be used to validate the attack surface and determine the best methodology to reduce the attack surface through hardening and configuration management

### Associated Certification: [[GIAC Security Essentials](https://www.giac.org/certification/certified-forensic-analyst-gcfa)](https://www.giac.org/certification/security-essentials-gsec) [(GSEC)](https://www.giac.org/certification/certified-forensic-analyst-gcfa)

* The GSEC certification is for security professionals who want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. It will certify that I can demonstrate an understanding of information security beyond simple terminology and concepts.
* See the “Exam Certification and Outcomes Statements” section of the [GSEC: GIAC Security Essentials](https://www.giac.org/certification/security-essentials-gsec) page for a list of covered topics.

**Expected Cost**

I’d like to take SEC401 [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) “online, with live virtual sessions and [select four (Simulcast) or six (vLive)] months of access via the SANS training platform [select Simulcast or vLive] from [start date] through [end date].”].

The attached an 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 | [$XXX] |
| OnDemand Bundle fee | [$XXX] |
| 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/course/security-essentials-network-endpoint-cloud>.

Thanks for your consideration,

[Add standard signature]

Attachment:

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