**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:

* Develop a comprehensive security program that integrates proactive detection, rapid response, and prevention strategies to combat evolving cybersecurity threats
* Tackle critical security challenges by addressing high-priority vulnerabilities and implementing robust security measures within our organization
* Evolve defensive strategies to stay ahead of adversaries by analyzing and adapting to their tactics
* Prevent, detect, and respond to ransomware attacks more effectively by using advanced techniques
* Optimize network security architecture using VLANs, Network Access Control (NAC), and IEEE 802.1X based on indicators of compromise to fortify against advanced persistent threats
* Master Identity and Access Management (IAM) to ensure robust authentication processes including Multi-Factor Authentication (MFA) are in place, enhancing security across all systems
* Capitalize on cloud security strengths by leveraging the unique features and security capabilities of the top cloud providers: AWS, Microsoft Azure, and Google Cloud
* Identify and mitigate system vulnerabilities using sophisticated tools to scan, detect, and secure systems from visible and latent security weaknesses
* Analyze network traffic with tools like tcpdump and Wireshark to uncover malicious activities
* Conduct deep system analysis to detect high-risk indicators of compromise
* Construct a detailed network visibility map that supports comprehensive attack surface analysis and guides strategic security hardening and configuration management efforts

### 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) “live online at [event name], attending the virtual streaming session from [start date] to [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**

Enrolling in the SEC401 Security Essentials course will not only advance my capabilities as a cybersecurity professional but will also directly enhance our organization’s overall security posture. By equipping me with hands-on experience in combating the latest cybersecurity threats, I will be better prepared to identify vulnerabilities, implement robust defense strategies, and respond effectively to incidents. The practical skills and insights I gain will be instrumental in elevating our security measures.

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]