SANS 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 [SEC450: Blue Team Fundamentals: Security Operations and Analysis](https://www.sans.org/cyber-security-courses/blue-team-fundamentals-security-operations-analysis/) and its associated [GIAC Security Operations Certified (GSOC)](https://www.giac.org/certifications/security-operations-certified-gsoc/) exam.

The following information clarifies how this training and certification 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**

[SEC450: Blue Team Fundamentals: Security Operations and Analysis](https://www.sans.org/cyber-security-courses/blue-team-fundamentals-security-operations-analysis/) is designed for teams of all types who are looking to develop the critical skills needed for understanding how to defend a modern organization. SEC450 provides students with technical knowledge and key concepts essential for security operation center (SOC) analysts and new cyber defense team members. Through a detailed explanation of the mission and mindset of a modern cyber defense operation, this course will jumpstart and empower those on their way to becoming the next generation of blue team members.

After completing SEC450, I’ll be able to undertand and apply the critical skills and techniques to effectively defend a modern organization.

**Course Objectives**

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

* Understand and know how to make the most of security telemetry including endpoint, network, and cloud-based sensors (Security Data Collection )
* Identify the best opportunities for SOAR platform and other script-based automation
* Keep my security operations tempo on track with in-depth discussions on what a SOC or security operations team should be doing at every step from data generation to detection, triage, analysis, and incident response (Efficient Security Process)
* Quickly identify and separate typical commodity attack alerts from high-risk, high-impact advanced attacks, and how to do careful, thorough, and cognitive-bias free security incident analysis (Quality Triage and Analysis)
* Understand detailed explanations, processes, and techniques to reduce false positives to a minimum
* Effectively utilize SOC Tools, including hands-on exercises demonstrating:
  + How to collect, organize, and use relevant threat data in a Threat Intelligence Platform (TIP)
  + Principles of success for endpoint security data collection whether I use a SIEM, EDR, or XDR
  + Alert Triage - How to quickly and accurately triage security incidents, using clever data correlation and enrichment techniques that will immediately surface and sort true positives from false positives
  + How to best use incident management systems to effectively analyze, document, track, and extract critical metrics from my security incidents
  + Crafting automation workflows for common SOC activities, relieving analysts of boring tasks and freeing up time for better threat hunting and detection engineering

### Associated Certification: [GIAC Security Operations Certified (GSOC)](https://www.giac.org/certifications/security-operations-certified-gsoc/)

* The GSOC certification is for Incident Investigators, Technical Security Managers, SOC Managers, and anyone looking to start their career on the blue team. It is also beneficial to Security Analysts, Engineers, and Architects. The exam will certify that I have the ability to defend an enterprise using essential blue team incident response tools and techniques. It will also prove that I am well-versed in the technical knowledge and key concepts needed to run a security operations center (SOC).
* See the “Exam Certification and Outcomes Statements” section of the [GSOC: GIAC Security Operations Certified](https://www.giac.org/certifications/security-operations-certified-gsoc/) page for a list of covered topics.

**Expected Cost**

I’d like to take SEC450 [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 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 | [$849] |
| OnDemand Bundle fee | [$849] |
| Travel and Hotel\* (for live training only) | [$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/blue-team-fundamentals-security-operations-analysis/>.

Thanks for your consideration,

[Add standard signature]

Attachment:

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