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 [LDR551: Building and Leading Security Operations Centers](https://www.sans.org/cyber-security-courses/building-leading-security-operations-centers/) and its associated [GIAC Security Operations Manager](https://www.giac.org/certifications/security-operations-manager-gsom/) exam.

**Why we need this course?**

Unlock the power of proactive, intelligence-informed cyber defense. In a world where IT environments and threat actors evolve faster than many teams can track, position your SOC to defend against highly motivated threat actors. Highly dynamic modern environments require a cyber defense capability that is forward-looking, fast-paced, and intelligence-driven. This SOC manager training course will guide you through these critical activities from start to finish and teach you how to design defenses with *your* *organization’s* unique risk profile in mind. Walk away with the ability to align your SOC activities with organizational goals.

I will also have interactive learning by playing through seventeen [Cyber42](https://www.sans.org/blog/cyber42/) activities throughout the class.

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

* Construct a strong SOC foundation based on a clear mission, charter, and organizational goals
* Collect the most important logs and network data
* Build, train, and empower a diverse team
* Create playbooks and manage detection use cases
* Use threat intelligence to focus detection efforts on true priorities
* Apply threat hunting process and active defense strategies
* Implement efficient alert triage and investigation workflow
* Operate effective incident response planning and execution
* Choose metrics and long-term strategy to improve the SOC
* Employ team member training, retention, and prevention of burnout
* Perform SOC assessment through capacity planning, purple team testing, and adversary emulation

**Which translate into business benefits for our company of:**

* Implement strategies for aligning cyber defense to organizational goals
* Decrease our risk profile due to improved security validation tools and techniques
* Apply methodologies for recruiting, hiring, training, and retaining talented cyber defenders
* Streamline effective cross-team coordination and collaboration
* Employ immediate security optimization improvements using current assets
* Reduce financial spend due to smoother cyber security operations

**Associated Certification:** [[**GIAC Securitiy Operations Manager**](https://www.giac.org/certifications/security-operations-manager-gsom/)](https://www.giac.org/certification/network-forensic-analyst-gnfa)

The GSOM certification validates a professional’s ability to run an effective security operations center. GSOM-certified professionals are well-versed in the management skills and process frameworks needed to strategically operate and improve a SOC and its team.

* Designing, planning, and managing an effective SOC program
* Prioritization and collection of logs, development of alert use cases, and response playbook generation
* Selecting metrics, analytics, and long-term strategy to assess and continuously improve SOC operations

See the “Exam Certification and Outcomes Statements” section of the [**GIAC Security Operations Manager**](https://www.giac.org/certifications/security-operations-manager-gsom/) page for a list of covered topics.

**Expected Cost**

I’d like to take LDR551 [fill in either: (1) “at [event name], from [start date] through [end date].” or (2) “online, with four months of access to the SANS OnDemand training platform.” or (3) “online, via Live Online 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 | [$XXX] |
| OnDemand Bundle fee | [$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].

**Testimonials**

**“This course is great at explaining the higher-level management of a SOC and the different solutions one can bring to their team to improve morale, become more efficient at securing the network, and optimize the cost-benefits of implementing new products or services. Great course!”** *– Michael A., US Military*

**“A ton of useful things I will take back and use starting Monday. This week I learned more thing than I could have learned in months on my own.”** *– Zak Scholl, Zendesk*

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/building-leading-security-operations-centers/>

Thanks for your consideration,

[Add standard signature]

Attachment:

Unpaid Invoice for SANS training [find at https://www.sans.org/cyber-security-courses/building-leading-security-operations-centers/ and attach to email]