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 [SEC555 Detection Engineering and SIEM Analytics](https://www.sans.org/cyber-security-courses/detection-engineering-siem-analytics/) and its associated [GIAC Certified Detection Analyst (GCDA)](https://www.giac.org/certifications/certified-detection-analyst-gcda/) 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**

[SEC555 Detection Engineering and SIEM Analytics](https://www.sans.org/cyber-security-courses/detection-engineering-siem-analytics/) equips defenders with the skills to design proactive detections, build effective logging strategies, and move beyond simply collecting logs to understanding what they represent, why they matter, and how to respond. Whether you’re a seasoned Security Analyst or new to detection work, this course offers hands-on experience with SOF-ELK—a free SANS-supported SIEM platform—so you can build and refine detection rules, tune your SIEM, map behavior to adversary tactics, and analyze activity across both on-prem and cloud environments. The course helps students evolve from basic logging to actionable security intelligence within a fully functioning SOC.

After completing SEC555, you’ll be able to dig into logs with confidence—understanding which data matters most, how to connect the dots, and how to pivot from detection to investigation to hunting. You'll know how to deploy internal detection mechanisms like tripwires and canaries to help catch intruders early. With a better grasp of how to enrich and analyze log data, you’ll be positioned to improve alerting, reduce noise, and highlight meaningful signals.

**Course Objectives**

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

* Set up a detection lab environment
* Write detection ules that track adversary behavior
* Tune and manage SIEM architecture for performance and relevance
* Emulate attacker activity to analyze logs and validate visibility
* Use log data to assess the effectiveness of security controls
* Streamline how large volumes of log data are collected, filtered, and processed
* Navigate both on-prem and cloud-based log sources and tools
* Apply the MITRE ATT&CK framework to map detections to specific tactics and techniques
* Monitor and evaluate detection coverage across multiple data sources
* Use SOAR platforms to improve detection workflows and response time
* Establish behavioral baselines and identify trends, anomalies, and threats
* Establish baselines, identify trends, and discover outliers, pointing to adversary activity

### Associated Certification: [GIAC Certified Detection Analyst (GCDA)](https://www.giac.org/certifications/certified-detection-analyst-gcda/)

* The GCDA certification is for Security Analysts/Architects, Senior Security Engineers, System Administrators, Technical Security Managers, CND Analysts, Cyber Threat Investigators, or individuals working to implement Continuous Security Monitoring or Network as well as individuals working in a hunt team capacity. It is also for SOC analysts, engineers, and managers. The exam will certify that I have the knowledge and ability to collect, analyze, and tactically use modern network and endpoint data sources to detect malicious or unauthorized activity.
* See the “Exam Certification and Outcomes Statements” section of the [GCDA: GIAC Certified Detection Analyst](https://www.giac.org/certifications/certified-detection-analyst-gcda/) page for a list of covered topics.

**Expected Cost**

I’d like to take SEC555 [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/siem-with-tactical-analytics/>.

Thanks for your consideration,

[Add standard signature]

Attachment:

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