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: SIEM with Tactical Analytics](https://www.sans.org/cyber-security-courses/siem-with-tactical-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: SIEM with Tactical Analytics](https://www.sans.org/cyber-security-courses/siem-with-tactical-analytics/) is designed to provide training, methods, and processes for enhancing existing logging solutions. This class will also provide the understanding of the when, what, and why behind the logs. SEC555 is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free SIEM solution, to train hands-on experience and provide the mindset for large-scale data analysis. This class serves as a switch from the typical churn and burn log systems, to achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

After completing SEC555, I’ll be able to iterate through the log data and events to analyze key components that will help me understand how rich this information is, how to correlate the data, start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. I will also be able to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions.

**Course Objectives**

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

* Deploy the SANS SOF-ELK VM in production environments
* Demonstrate ways most SIEMs commonly lag current open source solutions (e.g. SOF-ELK)
* Bring students up to speed on SIEM use, architecture, and best practices
* Know what type of data sources to collect logs from
* Deploy a scalable logs solution with multiple ways to retrieve logs
* Operationalize ordinary logs into tactical data
* Develop methods to handle billions of logs from many disparate data sources
* Understand best practice methods for collecting logs
* Dig into log manipulation techniques challenging many SIEM solutions
* Build out graphs and tables that can be used to detect adversary activities and abnormalities
* Combine data into active dashboards that make analyst review more tactical
* Utilize adversary techniques against them by using frequency analysis in large data sets
* Develop baselines of network activity based on users and devices
* Develop baselines of Windows systems with the ability to detect changes from the baseline
* Apply multiple forms of analysis such as long tail analysis to find abnormalities
* Correlate and combine multiple data sources to achieve more complete understanding
* Provide context to standard alerts to help understand and prioritize them
* Use log data to establish security control effectiveness
* Implement log alerts that create virtual tripwires for early breach detection
* Understand how to handle container monitoring and log collection
* Baseline and find unauthorized changes in cloud environments
* Integrate and write custom scripts against a SIEM

### 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]