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 [SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise](https://www.sans.org/cyber-security-courses/defensible-security-architecture-and-engineering/) and its associated [GIAC Defensible Security Architecture (GDSA)](https://www.giac.org/certifications/defensible-security-architecture-gdsa/) 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**

[SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise](https://www.sans.org/cyber-security-courses/defensible-security-architecture-and-engineering/) is designed to help students build and maintain a truly defensible security architecture, while taking them on a journey towards implementing Zero Trust principles, pillars and capabilities. This six-day course focuses on combining strategic concepts of infrastructure and tool placement while also diving into their technical application. Students will learn how to assess, re-configure and validate existing technologies to significantly improve their organizations' prevention, detection and response capabilities, augment visibility, reduce attack surface, and even anticipate attacks in innovative ways.

After completing SEC530, I’ll walk away with recommendations and suggestions that will aid in my ability to build a robust security infrastructure, layer by layer, across hybrid environments, as I embark on a journey towards Zero Trust.

**Course Objectives**

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

* Analyze a security architecture for deficiencies
* Discover data, applications, assets and services, and assess compliance state
* Implement technologies for enhanced prevention, detection, and response capabilities
* Comprehend deficiencies in security solutions and understand how to tune and operate them
* Understand the impact of 'encrypt all' strategies
* Apply the principles learned in the course to design a defensible security architecture
* Determine appropriate security monitoring needs for organizations of all sizes
* Maximize existing investment in security architecture by reconfiguring existing technologies
* Determine capabilities required to support continuous monitoring of key Critical Security Controls
* Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program
* Design and Implement Zero Trust strategies leveraging current technologies and investment

### Associated Certification: [GIAC Defensible Security Architecture (GDSA)](https://www.giac.org/certifications/defensible-security-architecture-gdsa/)

* The GDSA certification is for security architects/analysts, network architects/engineers, technical Security Managers, and CND analysts. It is also for security monitoring specialists and cyber threat investigators. The exam will certify that I can design and implement an effective combination of network-centric and data-centric controls to balance prevention, detection, and response.
* See the “Exam Certification and Outcomes Statements” section of the [GDSA: GIAC Defensible Security Architecture](https://www.giac.org/certifications/defensible-security-architecture-gdsa/) page for a list of covered topics.

**Expected Cost**

I’d like to take SEC530 [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/defensible-security-architecture-and-engineering/>.

Thanks for your consideration,

[Add standard signature]

Attachment:

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