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 [FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques](https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/) and its associated [GIAC Reverse Engineering Malware (GREM](https://www.giac.org/certifications/reverse-engineering-malware-grem/)) exam.

The information below clarifies how this training 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**

[FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques](https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/) will help me understanding the capabilities of malware is critical to your ability to derive threat intelligence, respond to cybersecurity incidents, and fortify enterprise defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

**Course Objectives**

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

* Build an isolated, controlled laboratory environment for analyzing the code and behavior of malicious programs
* Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
* Uncover and analyze malicious JavaScript and other components of web pages, which are often used by exploit kits for drive-by attacks
* Control relevant aspects of the malicious program's behavior through network traffic interception and code patching to perform effective malware analysis
* Use a disassembler and a debugger to examine the inner workings of malicious Windows executables
* Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse, and otherwise slow down the analyst
* Recognize and understand common assembly-level patterns in malicious code, such as code L injection, API hooking, and anti-analysis measures
* Assess the threat associated with malicious documents, such as PDF and Microsoft Office files
* Derive Indicators of Compromise (IOCs) from malicious executables to strengthen incident response and threat intelligence efforts.

**Associated Certification:** **GIAC Reverse Engineering Malware (GREM)**

* The GIAC Reverse Engineering Malware (GREM) certified technologists possess the knowledge and skills to reverse-engineer malicious software (malware) that targets common platforms, such as Microsoft Windows and web browsers. These individuals know how to examine inner-workings of malware in the context of forensic investigations, incident response, and Windows system administration.
* See the “Exam Certification and Outcomes Statements” section of the [GIAC Reverse Engineering Malware (GREM)](https://www.giac.org/certifications/reverse-engineering-malware-grem/) page for a list of covered topics.

**Expected Cost**

I’d like to take FOR610 [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 or SelfStudy] 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 | [$XXX] |
| OnDemand Bundle fee | [$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].

**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/reverse-engineering-malware-malware-analysis-tools-techniques/>

Thanks for your consideration,

[Add standard signature]

Attachment:

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