Cyber Engineer Notes for requirements

**Description:**

Provide expertise in scripting/programming to maintain our Cyber operation systems. This is primarily a Linux environment that the systems run on top of. We need to support the various Cyber Security tools, applications and network and endpoint hardware we support. Builds, designs, tests, and deploys perimeter, cloud security systems to support firewalls, proxy devices and other security systems.

Will administer the core Cyber Security applications that we support such as Syslog and log systems, Splunk, RedSeal, Radius and various other security and system tools. Will interface with fellow Cyber and Firewall engineers to gather additional requirements and details to help support the mission of protecting our federal customers environment. Manage vendor ticket, information gathering, and troubleshooting in the event of a platform issue. This would cover network application issues, providing root cause determination and recommend resolution options.

Supports the planning, documents, and implements hardware and software refresh and upgrade of Cyber Security Systems. Supports periodic firewall rule set review and auditing for standards and use software. Attends weekly teleconferences, onsite meetings, and participates in working groups, as related to constant changing security environment.

Attends weekly teleconferences, onsite meetings, and participates in working groups, as related to constant changing security environment.

**Required Education/Experience:**

Bachelor degree in a computer science/computer engineering related discipline or 10 years of work experience.

5 of these years is maintaining linux systems with use of programming and scripting using Perl, Bash, and Python and other advanced languages

3 of these years in a Cyber Security environment in support of SIEM and or NOC

2 of these supporting IT systems at the enterprise level crossing between Cloud and On Premise environments

**Required Experience/Skills/Attributes:**

Excellent Linux user and admin skills demonstrating competency to maintain our Cyber Security systems.

Expert in scripting/programming in a Linux environment to support the various Cyber Security tools and applications required. This would include use of Shell scripting, Perl, Python 3 or above, Ruby that demonstrates the writing of your own projects and modules.

Good knowledge of Javascript, Powershell, and/or Visual Basic

Demonstrate the use of regular expressions

Knowledge of HTML and web scripting.

Great organizational skills

Good to excellent technical writing ability

Knowledge, understanding, and ideally experience with certificate generation and ideally operation of a Certificate Authority.

Excellent Excel skills. This is to help with reporting and to perform log analysis.

Good to excellent technical writing ability (use of language, use of Microsoft Word.).

Use of collaboration tools

**Desired Experience/Skills/Attributes:**

TCP/IP networking and advanced network concepts

Proficiency with TCP-IP and IPv4; IPv6 desired

Load Balancers

Firewall Experience/Knowledge supporting the configuration and maintenance of Firewall/DMZ infrastructure including Network and Application Firewall Packet Filtering technologies.

Packet Capture and log analysis experience

Core ITk technologies

Cloud Environment Knowledge and Admin Experience

Knowledgeable of RFCs (Requests For Comment).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**GDIT is looking for a #1: Ability to write scripts.**

Perl scripting at the expert level that includes writing your own projects and modules. In addition, they should have Python skills at the latest version Python 3.

**Good knowledge of Javascript, Powershell, and/or Visual Basic** for Applications would be plusses -- should be able to write basics. Ability to simply read other languages, well enough to see what a script does, would be a plus.

In any language they know, and in Linux, they should know how to write and use **regular expressions**. That's a technical term for complex pattern matching. It's critical for them to be able to use it.

**#2: Knowledge of HTML and web scripting**.  Knowledge of standard Internet protocols.

Examples of how used:

* take a web page apart, dig into it scripting, find what other web pages/services it calls.
* write a web page (though I'm no artist!).
* send mail using a Telnet connection directly to an SMTP server.
* read your email using a Telnet connection directly to a POP3 and/or IMAP server.
* control an FTP session using a Telnet connection directly to an FTP server.
* fetch a web page using a Telnet connection directly to an HTTP server.

These skills are used for debugging.

Knowledgeable of RFCs (Requests For Comment).  For example, the SMTP instructions are in RFC 5321 at <https://www.rfc-editor.org/rfc/rfc5321.txt> (among other locations).

​

**#3: Great organizational skills** to cope with the constant interruptions on multiple tasks within the day.

**#4: Knowledge**, understanding, and ideally experience with certificate generation and ideally operation of a **Certificate Authority**. This would be very helpful with the certificate generation process.

#5. **Excellent Excel skills.** This is to help with reporting and to perform log analysis.

#6: **Good to excellent technical writing ability** (use of language, use of Microsoft Word.). Good to excellent publishing (use of media: wikis, SharePoint, Confluence, &c).

#7: Good Linux administration skills – this is to maintain the current Cyber systems to keep updated and functioning properly.

​

**#8: Excellent Linux user skills** -- for example, if given a set of log files, could they use a multiple command pipeline to filter it down to the user traffic they want? Sample command we use to generate a list of domains blocked by the Squid for 123.12.123.12

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Builds, designs, tests and deploys perimeter, cloud security systems to support firewalls, proxy devices and other security systems.

Conducts troubleshooting of Systems that could include -Proxy, Splunk, Syslog, RedSeal, Radius, and other analysis security tool on premise and in the cloud. This would cover network application issues, providing root cause determination and recommend resolution options.

Manage vendor ticket, information gathering, and troubleshooting in the event of a platform issue.

Plans, documents, and implements hardware and software refresh and upgrade of Cyber Security Systems.

Supports periodic firewall rule set review and auditing for standards and use.
software.
Attends weekly teleconferences, onsite meetings, and participates in working groups, as related to constant changing security environment.

**Required Education/Experience:**
Bachelor degree in a computer science/computer engineering related discipline or 10 years of work experience.

Certifications: Two or more of the following or equivalent- PCPP , Linux related certificate, Network+, Security+, ITIL Foundation certification, AWS and Azure Cloud system admin knowledge, Linux scripting and programming in Python and or Pearl greatly desired.

**Required Experience/Skills/Attributes:**

Expert in scripting/programming in a Linux environment to support the various Cyber Security tools and applications required. (Use of Shell scripting, Perl, Python, Ruby)•Linux competency a must in order to support our various security platforms Maintain the log management systems and processes Expert level skills with Excel to manipulate data for analysis Experience with Palo Alto Networks, Cisco FWSM, Cisco ASA firewalls, proxy, pcap •Proficiency with Splunk as an administrator and user at an Enterprise level Proficiency with TCP-IP and IPv4; IPv6 desired

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

10+ years IT network engineering support experience (Tier II, Tier III, network infrastructure implementation and maintenance).
3+years supporting cloud environments such as AWS and Azure with a security specialty and focus.
Expert experience in one or more of the following security devices: Palo Alto Firewalls, Cisco ASA/FirePower, Checkpoint, Netscreen.
Experience supporting the configuration and maintenance of Firewall/DMZ infrastructure including Network and Application Firewall Packet Filtering technologies.
Firsthand experience in developing and providing quality assurance review of engineering change orders relating to the replacement or enhancement of perimeter security hardware and software.
Experienced with performing root cause analysis, risk identification and risk mitigation.
Experienced with network monitoring devices such as HP Openview, Nagios, Zenoss, NeuralStar or other similar monitoring tools.
**Desired Experience/Skills/Attributes:**
Certifications: PCPP , Linux related certificate, Network+, Security+, ITIL Foundation certification, AWS and Azure Cloud system admin knowledge, Linux scripting and programming in Python and or Pearl greatly desired.

Interpersonal skills including the ability to collaborate effectively, self-awareness, and excellent written and oral communications.

(Use of Shell scripting, Perl, Python, Ruby)•Linux competency a must in order to support our various security platforms and hardware•Maintain the log management systems and processes•Expert level skills with Excel to manipulate data for analysis•Experience with Palo Alto Networks, Cisco FWSM, Cisco ASA firewalls, proxy, pcap •Proficiency with Splunk as an administrator and user at an Enterprise level•Proficiency with TCP-IP and IPv4; IPv6 desired