Hardened Splunk: Crash Course in Making Splunk Environments More Secure

TRU1537C .conf20

Mason Morales

Senior Manager, Splunk@Splunk | Splunk

SPLUNK TRUST

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Mason Morales

Senior Manager, Splunk@Splunk | Splunk

splunk> .conf20

Agenda

1) Security Fundamentals

2) General Best Practices

3) Forwarders

4) Deployment Servers

5) Indexers

6) Search Heads

Security Fundamentals

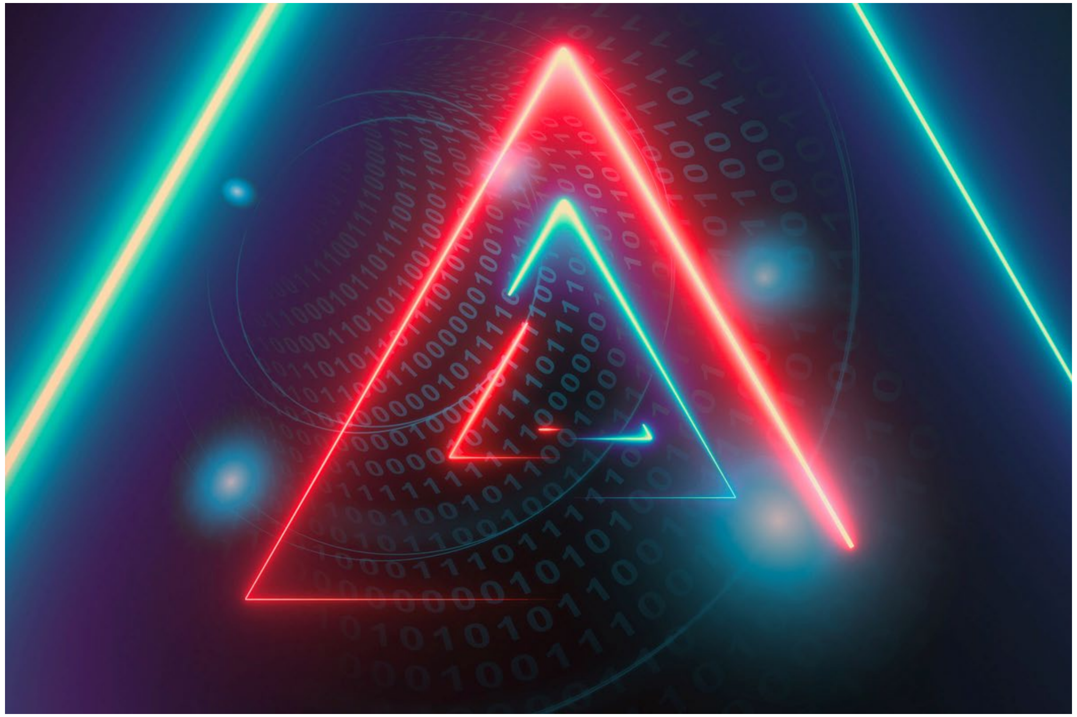
Concepts for Splunk Admins

Confidentiality, Integrity, Availability

The CIA triad

Confidentiality 🔒

- Only authorized users can access data



Confidentiality, Integrity, Availability

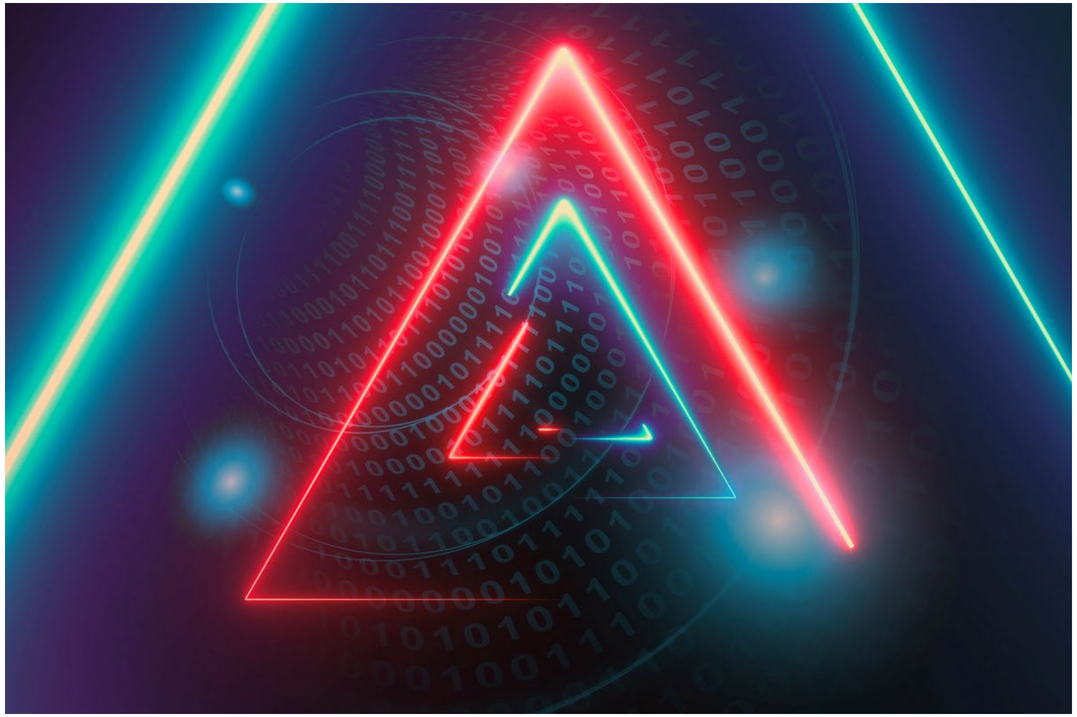
The CIA triad

Confidentiality 🔒

- Only authorized users can access data

Integrity 🔍

- Data has not been tampered with and can therefore be trusted; it is correct, authentic, and reliable



Confidentiality, Integrity, Availability

The CIA triad

Confidentiality 🔒

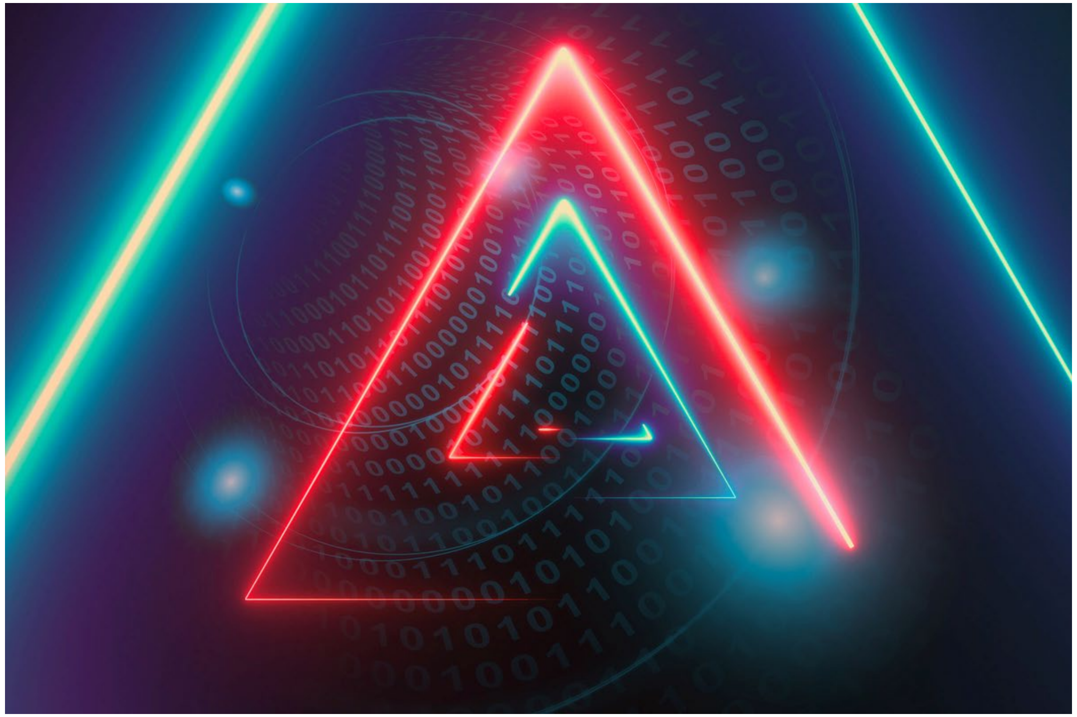
- Only authorized users can access data

Integrity 🔍

- Data has not been tampered with and can therefore be trusted; it is correct, authentic, and reliable

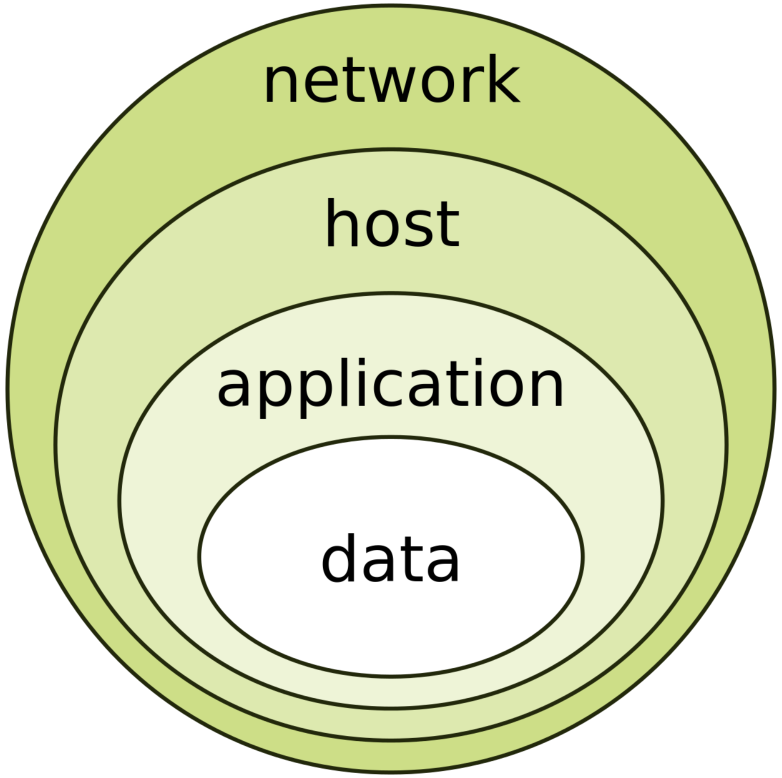
Availability ✅

- Authorized users can access data whenever they need to do so



Layered Security

Defense in depth

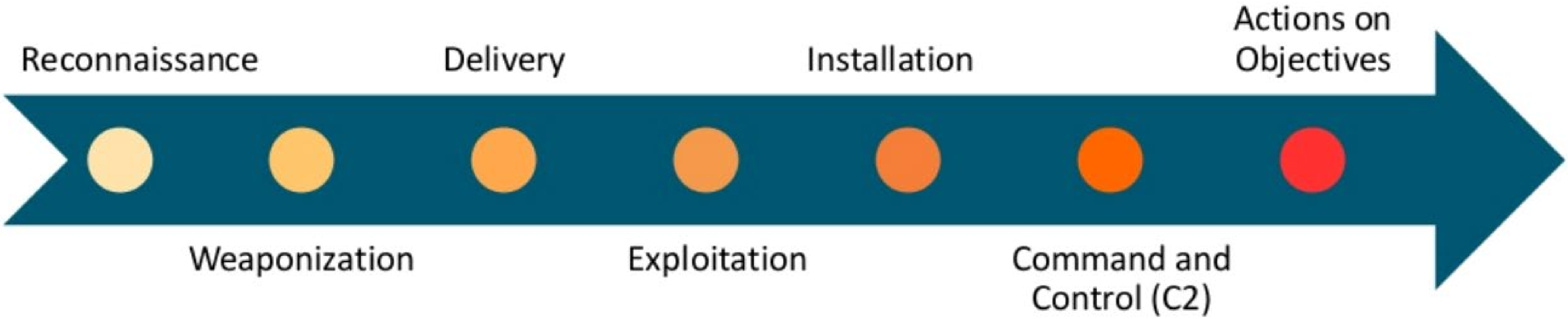


Controls at each layer help protect our data

- Network
  - – Firewall ACLs
  - – Dedicated security zone for Splunk
  - – Security groups in Cloud
- System
  - – Host-based firewall rules
  - – Sudoers configuration
  - – Many other controls in CIS benchmarks
- Application
  - – What we'll primarily be focusing on

Attack Kill Chain

Adversary perspective



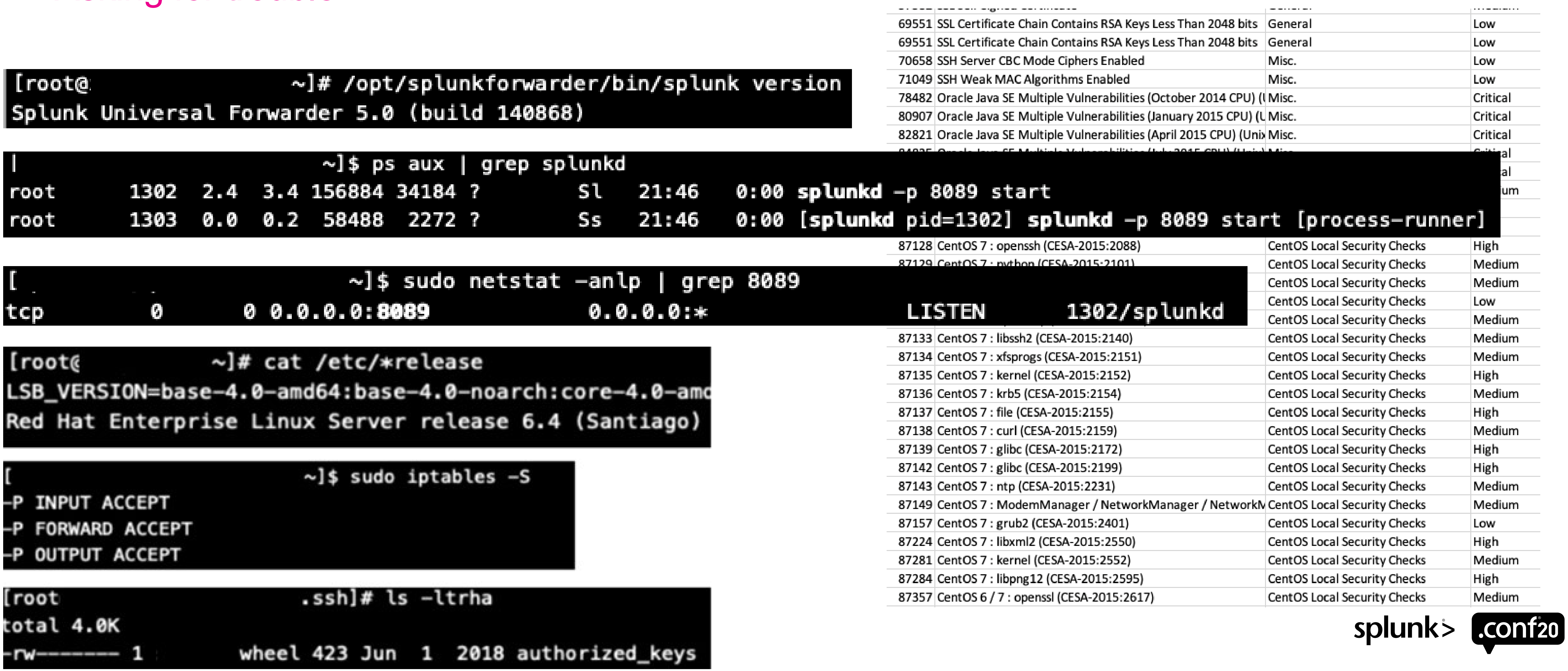
Learn more at https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

General Best Practices

TLDR Security for Splunk Admins

Operating System Security

Asking for trouble



```
[root@[redacted] ~]# /opt/splunkforwarder/bin/splunk version
Splunk Universal Forwarder 5.0 (build 140868)
```

```
[redacted] ~]$ ps aux | grep splunkd
root      1302  2.4  3.4 156884 34184 ?      Sl   21:46   0:00 splunkd -p 8089 start
root      1303  0.0  0.2  58488  2272 ?      Ss   21:46   0:00 [splunkd pid=1302] splunkd -p 8089 start [process-runner]
```

```
[[redacted] ~]$ sudo netstat -anlp | grep 8089
tcp        0      0 0.0.0.0:8089          0.0.0.0:*               LISTEN      1302/splunkd
```

```
[root@[redacted] ~]# cat /etc/*release
LSB_VERSION=base-4.0-amd64:base-4.0-noarch:core-4.0-amc
Red Hat Enterprise Linux Server release 6.4 (Santiago)
```

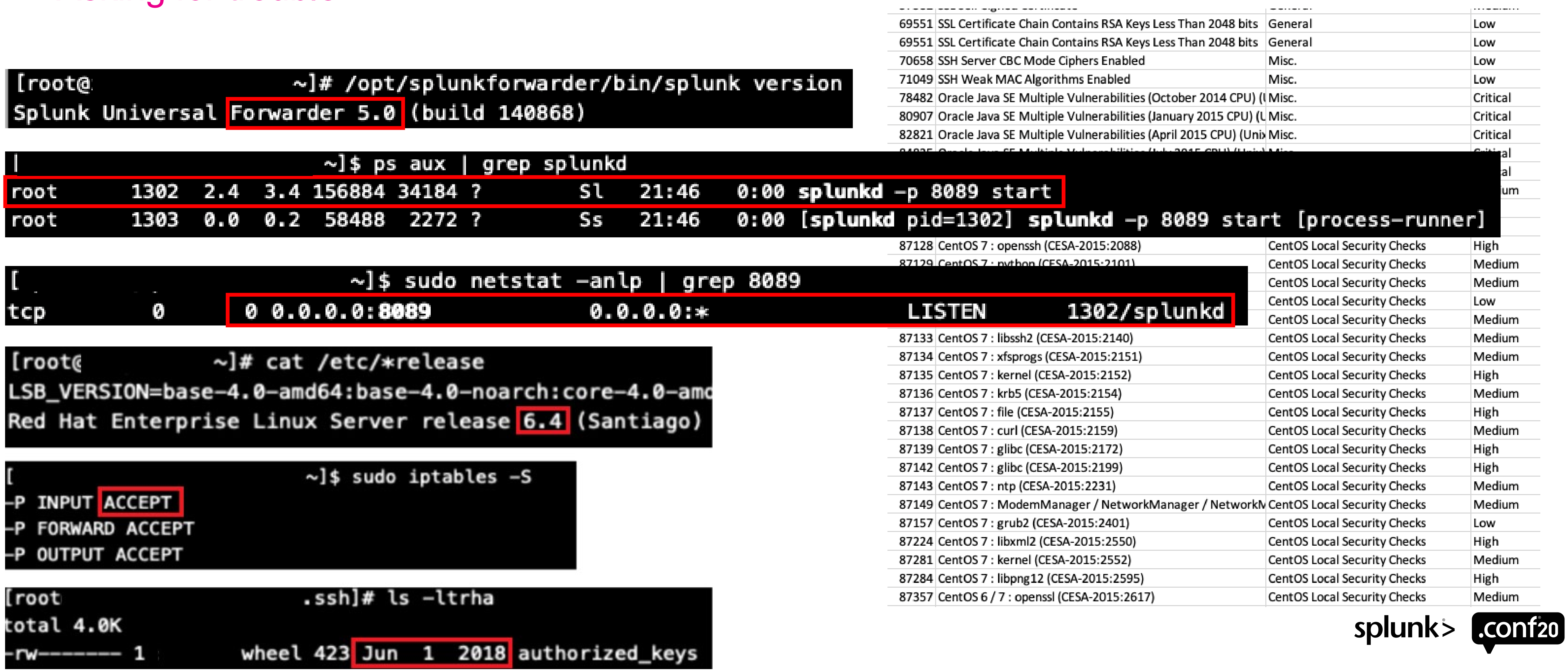
```
[[redacted] ~]$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
```

```
[root[redacted] .ssh]# ls -ltrha
total 4.0K
-rw------- 1 [redacted] wheel 423 Jun  1  2018 authorized_keys
```

69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	Low
69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	Low
70658	SSH Server CBC Mode Ciphers Enabled	Misc.	Low
71049	SSH Weak MAC Algorithms Enabled	Misc.	Low
78482	Oracle Java SE Multiple Vulnerabilities (October 2014 CPU) (U	Misc.	Critical
80907	Oracle Java SE Multiple Vulnerabilities (January 2015 CPU) (U	Misc.	Critical
82821	Oracle Java SE Multiple Vulnerabilities (April 2015 CPU) (Unix	Misc.	Critical
87128	CentOS 7 : openssh (CESA-2015:2088)	CentOS Local Security Checks	High
87129	CentOS 7 : python (CESA-2015:2101)	CentOS Local Security Checks	Medium
		CentOS Local Security Checks	Medium
		CentOS Local Security Checks	Low
		CentOS Local Security Checks	Medium
87133	CentOS 7 : libssh2 (CESA-2015:2140)	CentOS Local Security Checks	Medium
87134	CentOS 7 : xfsprogs (CESA-2015:2151)	CentOS Local Security Checks	Medium
87135	CentOS 7 : kernel (CESA-2015:2152)	CentOS Local Security Checks	High
87136	CentOS 7 : krb5 (CESA-2015:2154)	CentOS Local Security Checks	Medium
87137	CentOS 7 : file (CESA-2015:2155)	CentOS Local Security Checks	High
87138	CentOS 7 : curl (CESA-2015:2159)	CentOS Local Security Checks	Medium
87139	CentOS 7 : glibc (CESA-2015:2172)	CentOS Local Security Checks	High
87142	CentOS 7 : glibc (CESA-2015:2199)	CentOS Local Security Checks	High
87143	CentOS 7 : ntp (CESA-2015:2231)	CentOS Local Security Checks	Medium
87149	CentOS 7 : ModemManager / NetworkManager / NetworkM	CentOS Local Security Checks	Medium
87157	CentOS 7 : grub2 (CESA-2015:2401)	CentOS Local Security Checks	Low
87224	CentOS 7 : libxml2 (CESA-2015:2550)	CentOS Local Security Checks	High
87281	CentOS 7 : kernel (CESA-2015:2552)	CentOS Local Security Checks	Medium
87284	CentOS 7 : libpng12 (CESA-2015:2595)	CentOS Local Security Checks	High
87357	CentOS 6 / 7 : openssl (CESA-2015:2617)	CentOS Local Security Checks	Medium

Operating System Security

Asking for trouble



```
[root@[redacted] ~]# /opt/splunkforwarder/bin/splunk version
Splunk Universal Forwarder 5.0 (build 140868)
```

```
[[redacted] ~]$ ps aux | grep splunkd
root      1302  2.4  3.4 156884 34184 ?       Sl   21:46   0:00 splunkd -p 8089 start
root      1303  0.0  0.2  58488  2272 ?       Ss   21:46   0:00 [splunkd pid=1302] splunkd -p 8089 start [process-runner]
```

```
[[redacted] ~]$ sudo netstat -anlp | grep 8089
tcp        0      0 0.0.0.0:8089            0.0.0.0:*               LISTEN      1302/splunkd
```

```
[root@[redacted] ~]# cat /etc/*release
LSB_VERSION=base-4.0-amd64:base-4.0-noarch:core-4.0-amd
Red Hat Enterprise Linux Server release 6.4 (Santiago)
```

```
[[redacted] ~]$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
```

```
[root[redacted] .ssh]# ls -ltrha
total 4.0K
-rw------- 1 [redacted] wheel 423 Jun  1  2018 authorized_keys
```

69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	Low
69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	Low
70658	SSH Server CBC Mode Ciphers Enabled	Misc.	Low
71049	SSH Weak MAC Algorithms Enabled	Misc.	Low
78482	Oracle Java SE Multiple Vulnerabilities (October 2014 CPU) (l	Misc.	Critical
80907	Oracle Java SE Multiple Vulnerabilities (January 2015 CPU) (L	Misc.	Critical
82821	Oracle Java SE Multiple Vulnerabilities (April 2015 CPU) (Unix	Misc.	Critical
			al
			al
			um
87128	CentOS 7 : openssh (CESA-2015:2088)	CentOS Local Security Checks	High
87129	CentOS 7 : python (CESA-2015:2101)	CentOS Local Security Checks	Medium
		CentOS Local Security Checks	Medium
		CentOS Local Security Checks	Low
		CentOS Local Security Checks	Medium
87133	CentOS 7 : libssh2 (CESA-2015:2140)	CentOS Local Security Checks	Medium
87134	CentOS 7 : xfsprogs (CESA-2015:2151)	CentOS Local Security Checks	Medium
87135	CentOS 7 : kernel (CESA-2015:2152)	CentOS Local Security Checks	High
87136	CentOS 7 : krb5 (CESA-2015:2154)	CentOS Local Security Checks	Medium
87137	CentOS 7 : file (CESA-2015:2155)	CentOS Local Security Checks	High
87138	CentOS 7 : curl (CESA-2015:2159)	CentOS Local Security Checks	Medium
87139	CentOS 7 : glibc (CESA-2015:2172)	CentOS Local Security Checks	High
87142	CentOS 7 : glibc (CESA-2015:2199)	CentOS Local Security Checks	High
87143	CentOS 7 : ntp (CESA-2015:2231)	CentOS Local Security Checks	Medium
87149	CentOS 7 : ModemManager / NetworkManager / NetworkM	CentOS Local Security Checks	Medium
87157	CentOS 7 : grub2 (CESA-2015:2401)	CentOS Local Security Checks	Low
87224	CentOS 7 : libxml2 (CESA-2015:2550)	CentOS Local Security Checks	High
87281	CentOS 7 : kernel (CESA-2015:2552)	CentOS Local Security Checks	Medium
87284	CentOS 7 : libpng12 (CESA-2015:2595)	CentOS Local Security Checks	High
87357	CentOS 6 / 7 : openssl (CESA-2015:2617)	CentOS Local Security Checks	Medium

Operating System Security

Hardening guidelines

Patch regularly 🔒 ✅

- Or, better automate patching https://opensource.com/article/18/3/ansible-patch-systems

Operating System Security

Hardening guidelines

Patch regularly 🔒✅

- Or, better automate patching https://opensource.com/article/18/3/ansible-patch-systems

Implement CIS Benchmarks 🔒🔍✅

- https://downloads.cisecurity.org/download-issues/benchmarks

Operating System Security

Hardening guidelines

Patch regularly 🔒✅

- Or, better automate patching https://opensource.com/article/18/3/ansible-patch-systems

Implement CIS Benchmarks 🔒🔍✅

- https://downloads.cisecurity.org/download-issues/benchmarks

Rotate SSH keys periodically 🔒

Operating System Security

Hardening guidelines

Patch regularly 🔒 ✅

- Or, better automate patching https://opensource.com/article/18/3/ansible-patch-systems

Implement CIS Benchmarks 🔒 🔍 ✅

- https://downloads.cisecurity.org/download-issues/benchmarks

Rotate SSH keys periodically 🔒

Install splunk as a non-privileged user 🔒 🔍

- Use FACLs to read root-owned files
- Checkout TRU1504 Ansible Starter Pack for Automating Splunk Administration

Operating System Security

Hardening guidelines

Patch regularly 🔒 ✅

- Or, better automate patching https://opensource.com/article/18/3/ansible-patch-systems

Implement CIS Benchmarks 🔒 🔍 ✅

- https://downloads.cisecurity.org/download-issues/benchmarks

Rotate SSH keys periodically 🔒

Install splunk as a non-privileged user 🔒 🔍

- Use FACLs to read root-owned files
- Checkout TRU1504 Ansible Starter Pack for Automating Splunk Administration

For more, see Appendix: OS Checklist

Managing Your Splunk Deployment

PEBCAK

Common mistakes

- Not testing
- Manual config management
- No version control
- Local Splunk user accounts
- Lack of password complexity

Implications

- Outages
- Inability to roll-back
- No audit trail for backend config changes
- Account compromises

Managing Your Splunk Deployment

Done right

Version control all configs in Git 🔒✅🔍

- Git Version Control for Splunk App https://splunkbase.splunk.com/app/4182/

Managing Your Splunk Deployment

Done right

Version control all configs in Git 🔒✅🔍

- Git Version Control for Splunk App https://splunkbase.splunk.com/app/4182/

Test everything ✅🔍

- Dev|staging environment

Managing Your Splunk Deployment

Done right

Version control all configs in Git 🔒 ✅ 🔍

- Git Version Control for Splunk App https://splunkbase.splunk.com/app/4182/

Test everything ✅ 🔍

- Dev|staging environment

Use automation to deploy Splunk and its configs securely ✅ 🔍

- Checkout TRU1504 Ansible Starter Pack for Automating Splunk Administration

Managing Your Splunk Deployment

Done right

Version control all configs in Git 🔒 ✅ 🔍

- Git Version Control for Splunk App https://splunkbase.splunk.com/app/4182/

Test everything ✅ 🔍

- Dev|staging environment

Use automation to deploy Splunk and its configs securely ✅ 🔍

- Checkout TRU1504 Ansible Starter Pack for Automating Splunk Administration

Follow Securing the Splunk Platform manual 🔒 ✅ 🔍

- https://docs.splunk.com/Documentation/Splunk/latest/Security/

Forwarder Security

Concepts for Splunk Admins

Universal Forwarders

Hardening guidelines

Install UF as non-root user and keep it up-to-date 🔒✅🔍

Universal Forwarders

Hardening guidelines

Install UF as non-root user and keep it up-to-date 🔒✅🔍

Disable listening Splunkd port (TCP/8089) in server.conf 🔒✅

- Tip: Deploy this as an app from DS

```
[httpServer]
disableDefaultPort = true
```

Universal Forwarders

Hardening guidelines

Install UF as non-root user and keep it up-to-date 🔒✅🔍

Disable listening Splunkd port (TCP/8089) in server.conf 🔒✅

- Tip: Deploy this as an app from DS

```
[httpServer]
disableDefaultPort = true
```

Use DS to configure inputs/outputs 🔒✅

- Also, forward _internal and _audit to your indexers via outputs.conf
  - https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Forwardsearchheaddata

Universal Forwarders

Hardening guidelines

Install UF as non-root user and keep it up-to-date 🔒 ✓ 🔍

Disable listening Splunkd port (TCP/8089) in server.conf 🔒 ✓

- Tip: Deploy this as an app from DS

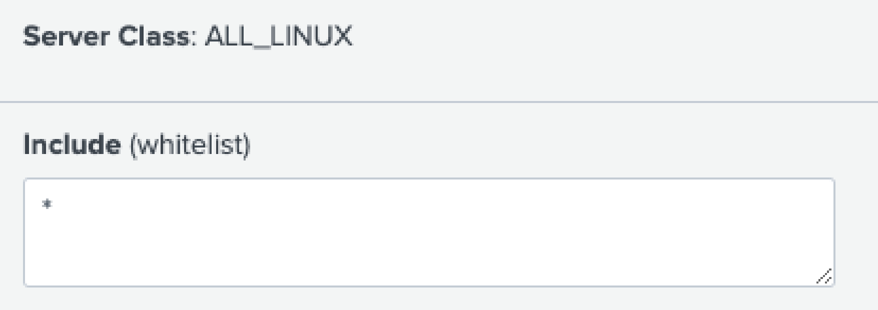
```
[httpServer]
disableDefaultPort = true
```

Use DS to configure inputs/outputs 🔒 ✓

- Also, forward _internal and _audit to your indexers via outputs.conf
  - https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Forwardsearchheaddata

Deploy OS addons to all clients matching specific platform

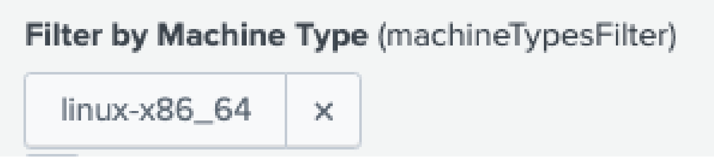
- Splunk Add-on for Unix and Linux (enable /var/log input)
- Splunk Add-on for Microsoft Windows



Server Class: ALL_LINUX

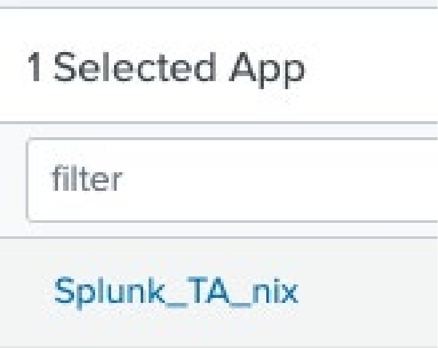
Include (whitelist)

*



Filter by Machine Type (machineTypesFilter)

linux-x86_64 ×



1 Selected App

filter

Splunk_TA_nix

Heavy Forwarders

Hardening guidelines

Follow UF Guidelines PLUS…

Heavy Forwarders

Hardening guidelines

Follow UF Guidelines PLUS…

Disable unnecessary services (web, kvstore, rest) 🔒✓

Heavy Forwarders

Hardening guidelines

Follow UF Guidelines PLUS…

Disable unnecessary services (web, kvstore, rest) 🔒✅

Deploy passwords securely (e.g. via ansible-vault) 🔒

- Do not put plaintext credentials in git repos

Heavy Forwarders

Hardening guidelines

Follow UF Guidelines PLUS…

Disable unnecessary services (web, kvstore, rest) 🔒✅

Deploy passwords securely (e.g. via ansible-vault) 🔒

- Do not put plaintext credentials in git repos

Manage credentials using a secret manager 🔒✅

- TA-VaultSync will pull creds for any passwords.conf-based TA from Hashicorp Vault
  - Checkout TRU1240C Automated Credential Synchronization with Hashicorp Vault

Heavy Forwarders

Hardening guidelines

Follow UF Guidelines PLUS…

Disable unnecessary services (web, kvstore, rest) 🔒✅

Deploy passwords securely (e.g. via ansible-vault) 🔒

- Do not put plaintext credentials in git repos

Manage credentials using a secret manager 🔒✅

- TA-VaultSync will pull creds for any passwords.conf-based TA from Hashicorp Vault
  - Checkout TRU1240C Automated Credential Synchronization with Hashicorp Vault

Consider using Docker Swarm to run HFs for high-availability and built-in security 🔒✅🔍

- https://github.com/splunk/docker-swarm-splunk-hf

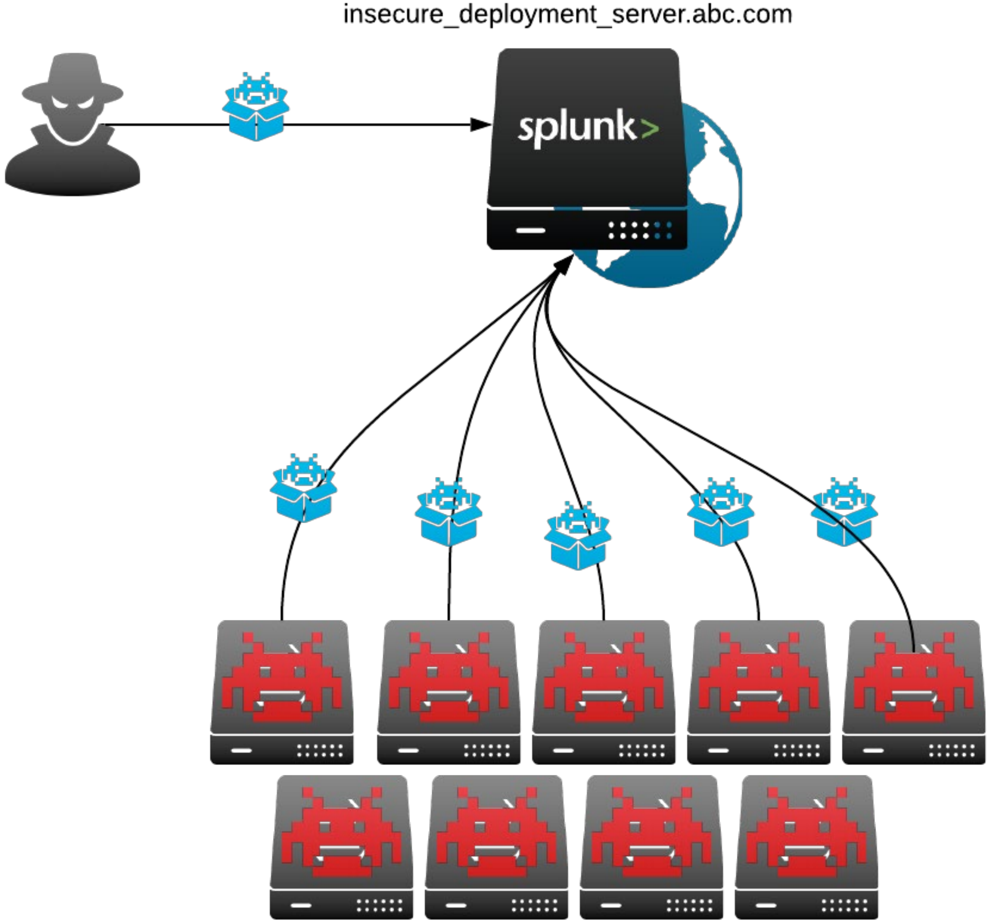
Deployment Server Security

Concepts for Splunk Admins

Deployment Server

Attack scenario A

1) Internet-exposed DS is compromised via a known vulnerability by attacker

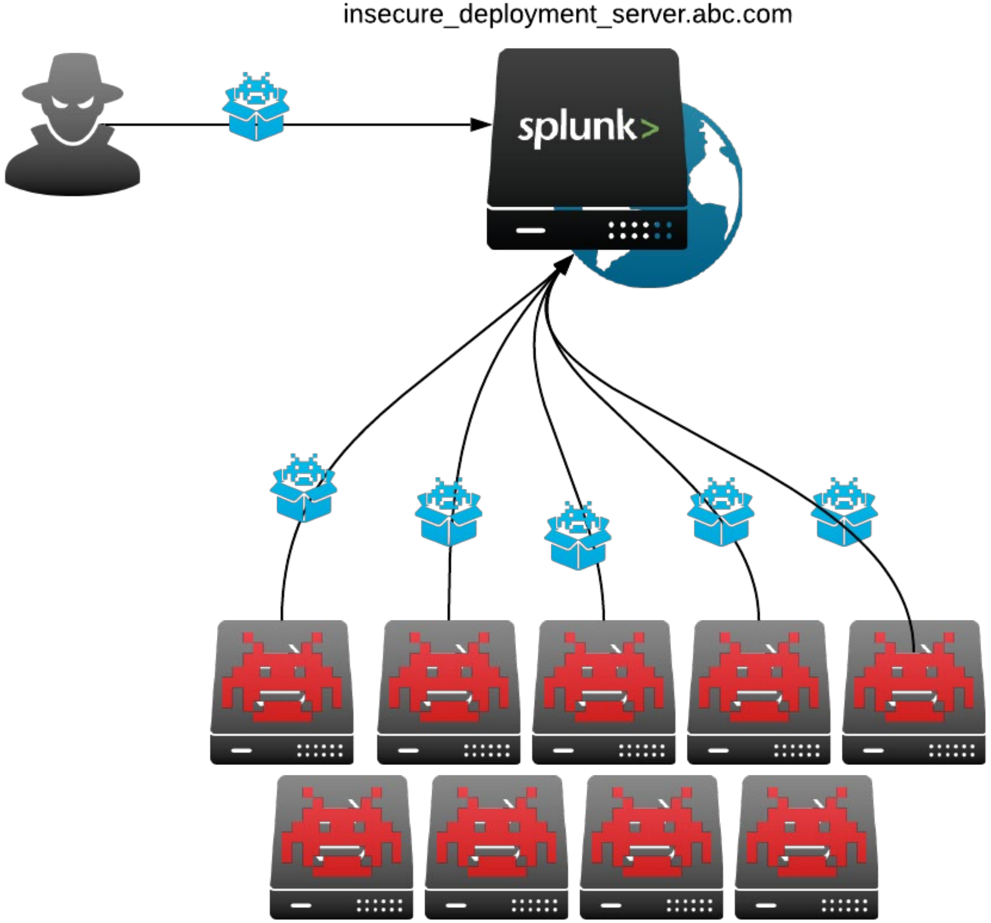


Deployment Server

Attack scenario A

1) Internet-exposed DS is compromised via a known vulnerability by attacker

2) Attacker packages malware as a Splunk app, uploads it to DS, and assigns it to an allowlist=* server class



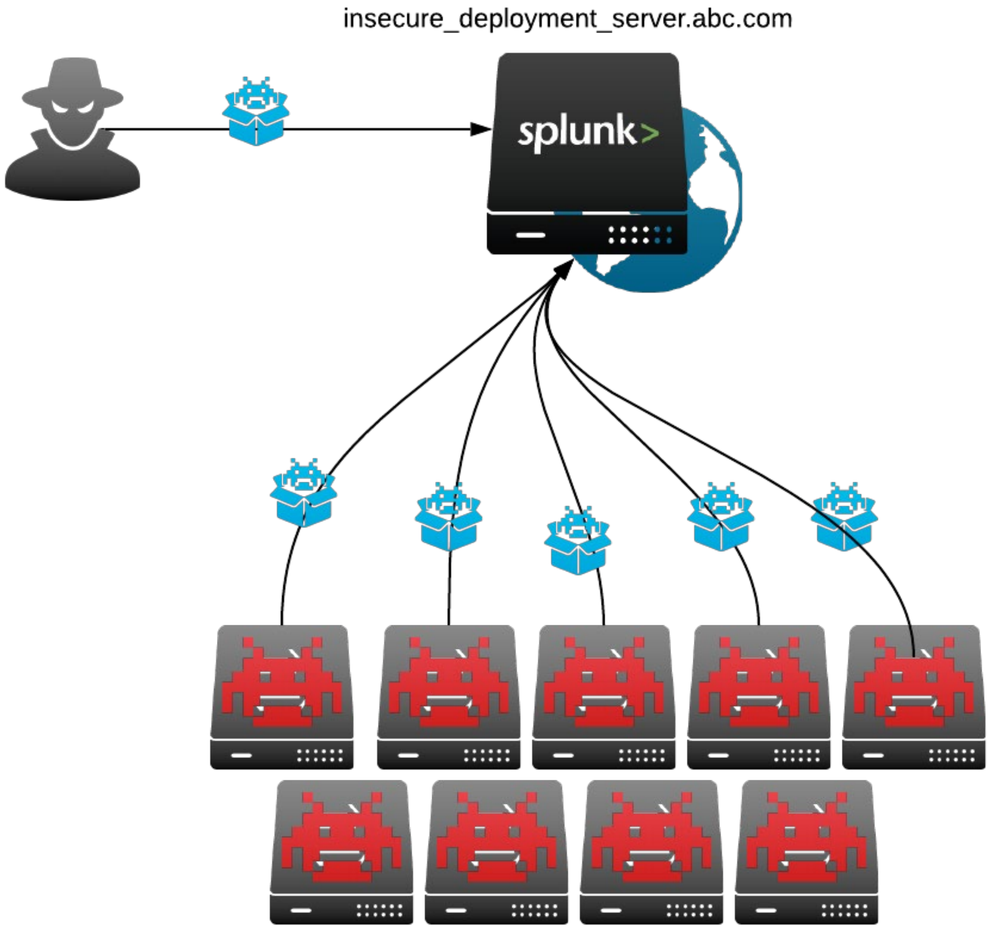
Deployment Server

Attack scenario A

1) Internet-exposed DS is compromised via a known vulnerability by attacker

2) Attacker packages malware as a Splunk app, uploads it to DS, and assigns it to an allowlist=* server class

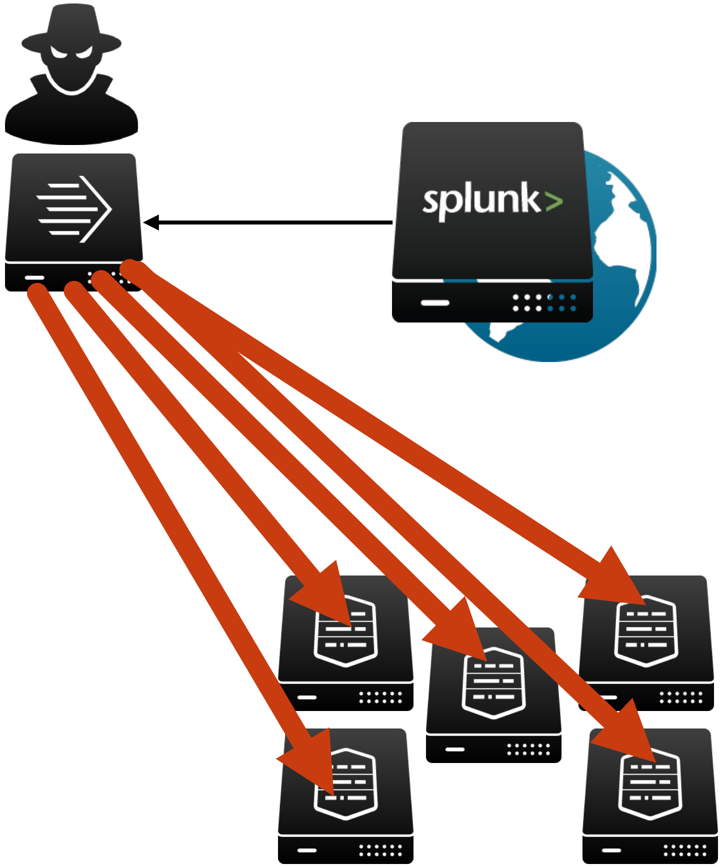
3) All clients phone home to DS, download the malware, and execute it



Deployment Server

Attack scenario B

1) Attacker connects a UF to an Internet-exposed DS

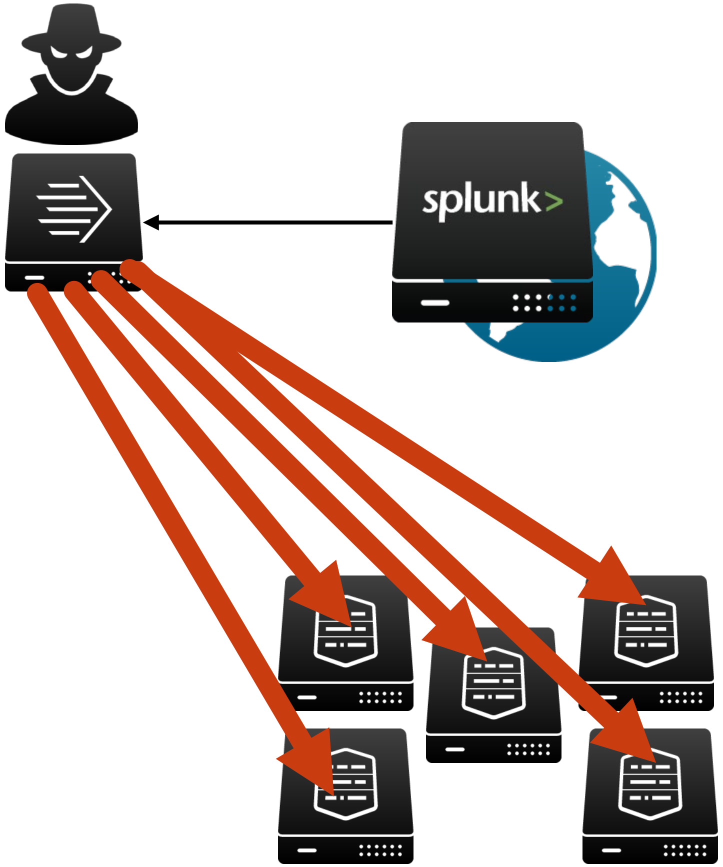


Deployment Server

Attack scenario B

1) Attacker connects a UF to an Internet-exposed DS

2) DS auto-assigns outputs TA to attacker's UF along with the certificates needed to send to Internet-exposed indexers



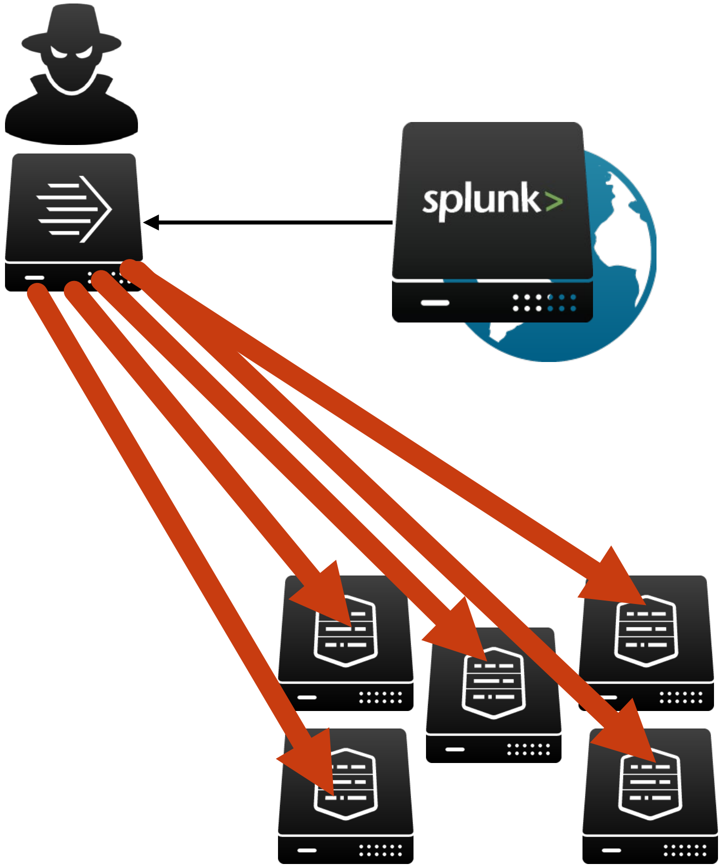
Deployment Server

Attack scenario B

1) Attacker connects a UF to an Internet-exposed DS

2) DS auto-assigns outputs TA to attacker's UF along with the certificates needed to send to Internet-exposed indexers

3) Attacker leverages outputs.conf server list and certificates to perform a Denial of Service (DOS) attack against the indexers



Deployment Server

Hardening guidelines

Use pass4symmkey to authenticate clients 🔒

- https://www.duanewaddle.com/splunk-pass4symmkey-for-deployment-client-deployment-server/

Deployment Server

Hardening guidelines

Use pass4symmkey to authenticate clients 🔒

- https://www.duanewaddle.com/splunk-pass4symmkey-for-deployment-client-deployment-server/

Configure a non-standard port for splunkd connections in web.conf 🔒✓

```
[settings]
mgmtHostPort = 0.0.0.0:38089
```

Deployment Server

Hardening guidelines

Use pass4symmkey to authenticate clients 🔒

- https://www.duanewaddle.com/splunk-pass4symmkey-for-deployment-client-deployment-server/

Configure a non-standard port for splunkd connections in web.conf 🔒✅

```
[settings]
mgmtHostPort = 0.0.0.0:38089
```

Use a Web Application Firewall (WAF) in front of the DS 🔒✅🔍

```
UserAgent ^Splunk
HTTP Method = POST
```

Deployment Server

Hardening guidelines

Use pass4symmkey to authenticate clients 🔒

- https://www.duanewaddle.com/splunk-pass4symmkey-for-deployment-client-deployment-server/

Configure a non-standard port for splunkd connections in web.conf 🔒✅

```
[settings]
mgmtHostPort = 0.0.0.0:38089
```

Use a Web Application Firewall (WAF) in front of the DS 🔒✅🔍

```
UserAgent ^Splunk
HTTP Method = POST
```

Consider separate DS for internal vs external clients 🔒✅

Deployment Server (Cont.)

Hardening guidelines

Limit Splunk web access to internal networks via firewall|iptables|security group 🔒✅

- And if possible, splunkd access

Deployment Server (Cont.)

Hardening guidelines

Limit Splunk web access to internal networks via firewall|iptables|security group 🔒✅

- And if possible, splunkd access

Consider client certificates 🔒

Deployment Server (Cont.)

Hardening guidelines

Limit Splunk web access to internal networks via firewall|iptables|security group 🔒✅

- And if possible, splunkd access

Consider client certificates 🔒

Consider MFA for SSH and web access🔒

Deployment Server (Cont.)

Hardening guidelines

Limit Splunk web access to internal networks via firewall|iptables|security group 🔒✅

- And if possible, splunkd access

Consider client certificates 🔒

Consider MFA for SSH and web access🔒

Change default splunk certificates🔒✅🔍

- https://wiki.splunk.com/images/f/fb/SplunkTrustApril-SSLipperySlopeRevisited.pdf

Deployment Server (Cont.)

Hardening guidelines

Limit Splunk web access to internal networks via firewall|iptables|security group🔒✅

- And if possible, splunkd access

Consider client certificates 🔒

Consider MFA for SSH and web access🔒

Change default splunk certificates🔒✅🔍

- https://wiki.splunk.com/images/f/fb/SplunkTrustApril-SSLipperySlopeRevisited.pdf

Install Splunk as non-root user and keep it up-to-date🔒✅🔍

Indexer Security

Concepts for Splunk Admins

Indexers

Hardening guidelines

Configure pass4symmkey on indexer clusters 🔒

Indexers

Hardening guidelines

Configure pass4symmkey on indexer clusters 🔒

Enable SSL for HTTP Event Collector (HEC) and Splunk2Splunk (TCP/9997) 🔒

Indexers

Hardening guidelines

Configure pass4symmkey on indexer clusters 🔒

Enable SSL for HTTP Event Collector (HEC) and Splunk2Splunk (TCP/9997) 🔒

Disable splunk web ✅

Indexers

Hardening guidelines

Configure pass4symmkey on indexer clusters 🔒

Enable SSL for HTTP Event Collector (HEC) and Splunk2Splunk (TCP/9997) 🔒

Disable splunk web ✅

Use a dedicated volume for $SPLUNK_DB limited to the splunk user 🔒

Indexers

Hardening guidelines

Configure pass4symmkey on indexer clusters 🔒

Enable SSL for HTTP Event Collector (HEC) and Splunk2Splunk (TCP/9997) 🔒

Disable splunk web ✅

Use a dedicated volume for $SPLUNK_DB limited to the splunk user 🔒

Enable data integrity control in default stanza of indexes.conf 🔍

- https://docs.splunk.com/Documentation/Splunk/latest/Security/Dataintegritycontrol#Configure_data_integrity_control

Indexers (Cont.)

Hardening guidelines

Limit Splunk2Splunk (TCP/9997) network connectivity to expected networks 🔒✅

- `acceptFrom = <network_acl>` in inputs.conf

Indexers (Cont.)

Hardening guidelines

Limit Splunk2Splunk (TCP/9997) network connectivity to expected networks 🔒 ✅

- `acceptFrom = <network_acl>` in inputs.conf

SSH access

- Limit access, consider MFA or ZeroTrust solutions (e.g. ScaleFT) 🔒 ✅
- Use LDAP for authentication or if using SSH keys, rotate periodically 🔒 ✅

Indexers (Cont.)

Hardening guidelines

Limit Splunk2Splunk (TCP/9997) network connectivity to expected networks 🔒 ✅

- `acceptFrom = <network_acl>` in inputs.conf

SSH access

- Limit access, consider MFA or ZeroTrust solutions (e.g. ScaleFT) 🔒 ✅
- Use LDAP for authentication or if using SSH keys, rotate periodically 🔒 ✅

Enable indexer acknowledgment 🔍

- https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Protectagainstthelossofin-flightdata
- https://docs.splunk.com/Documentation/Splunk/latest/Data/AboutHECIDXAck

Indexers (Cont.)

Hardening guidelines

Limit Splunk2Splunk (TCP/9997) network connectivity to expected networks 🔒 ✅

- `acceptFrom = <network_acl>` in inputs.conf

SSH access

- Limit access, consider MFA or ZeroTrust solutions (e.g. ScaleFT) 🔒 ✅
- Use LDAP for authentication or if using SSH keys, rotate periodically 🔒 ✅

Enable indexer acknowledgment 🔍

- https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Protectagainstthelossofin-flightdata
- https://docs.splunk.com/Documentation/Splunk/latest/Data/AboutHECIDXAck

Change default splunk certificates 🔒 ✅ 🔍

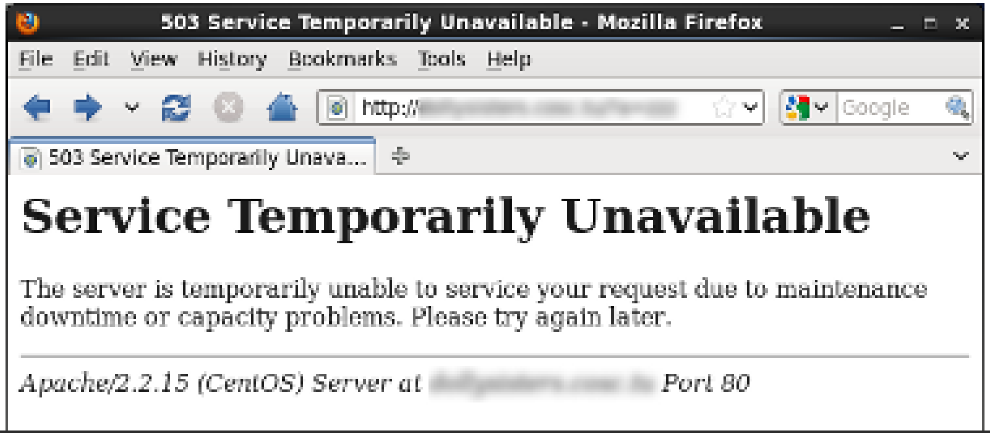
- https://wiki.splunk.com/images/f/fb/SplunkTrustApril-SSLipperySlopeRevisited.pdf

Search Head Security

Concepts for Splunk Admins

Search Heads

Has this ever happened to you?

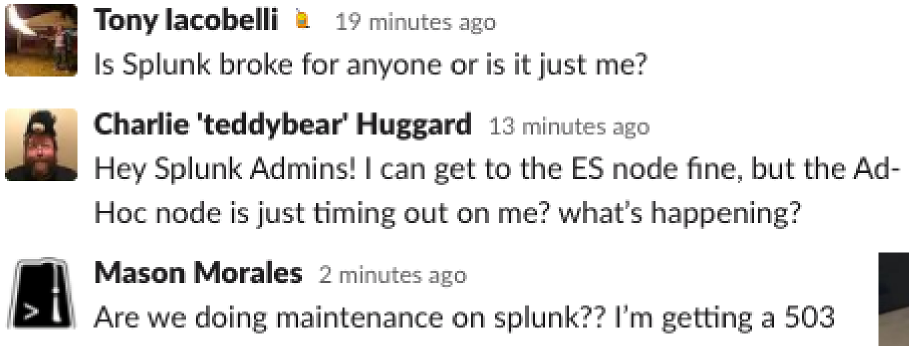


503 Service Temporarily Unavailable - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://[redacted]
Google
503 Service Temporarily Unava...

Service Temporarily Unavailable

The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.

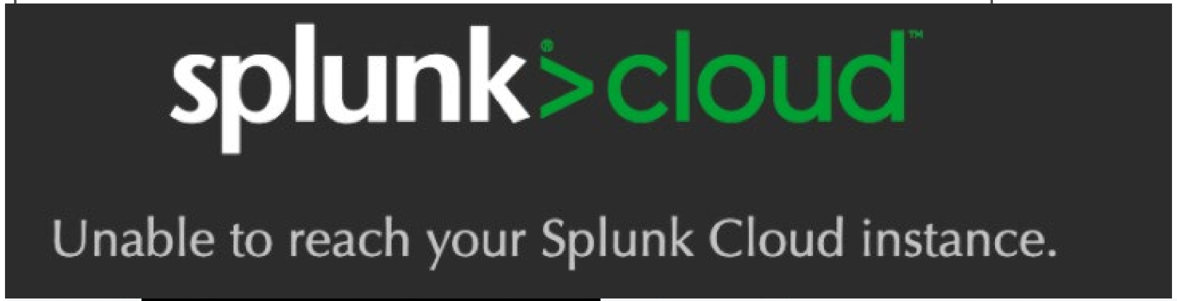
Apache/2.2.15 (CentOS) Server at [redacted] Port 80



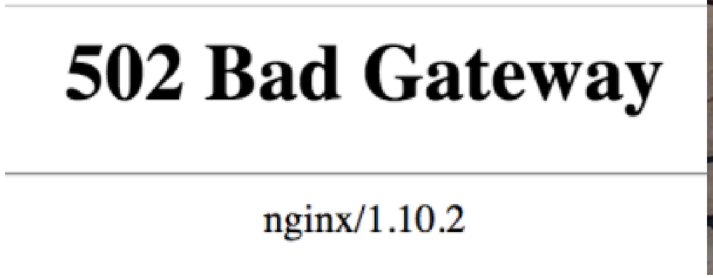
Tony Iacobelli 19 minutes ago
Is Splunk broke for anyone or is it just me?

Charlie 'teddybear' Huggard 13 minutes ago
Hey Splunk Admins! I can get to the ES node fine, but the Ad-Hoc node is just timing out on me? what's happening?

Mason Morales 2 minutes ago
Are we doing maintenance on splunk?? I'm getting a 503

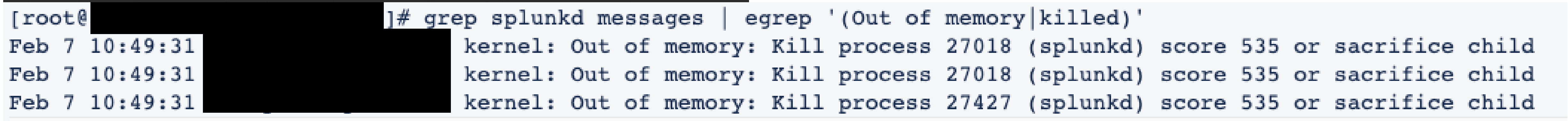


Unable to reach your Splunk Cloud instance.



502 Bad Gateway

nginx/1.10.2



```
[root@[redacted]]# grep splunkd messages | egrep '(Out of memory|killed)'
Feb 7 10:49:31 [redacted] kernel: Out of memory: Kill process 27018 (splunkd) score 535 or sacrifice child
Feb 7 10:49:31            kernel: Out of memory: Kill process 27018 (splunkd) score 535 or sacrifice child
Feb 7 10:49:31            kernel: Out of memory: Kill process 27427 (splunkd) score 535 or sacrifice child
```

Search Heads

Hardening guidelines

Limit search bundle max lookup size in distsearch.conf ✓

```
[replicationSettings]
excludeReplicatedLookupSize = 10
```

Search Heads

Hardening guidelines

Limit search bundle max lookup size in distsearch.conf ✓

```
[replicationSettings]
excludeReplicatedLookupSize = 10
```

Limit max memory searches can consume in limits.conf ✓

```
[search]
enable_memory_tracker = true
search_process_memory_usage_percentage_threshold = 20
```

Search Heads

Hardening guidelines

Limit search bundle max lookup size in distsearch.conf ✓

```
[replicationSettings]
excludeReplicatedLookupSize = 10
```

Limit max memory searches can consume in limits.conf ✓

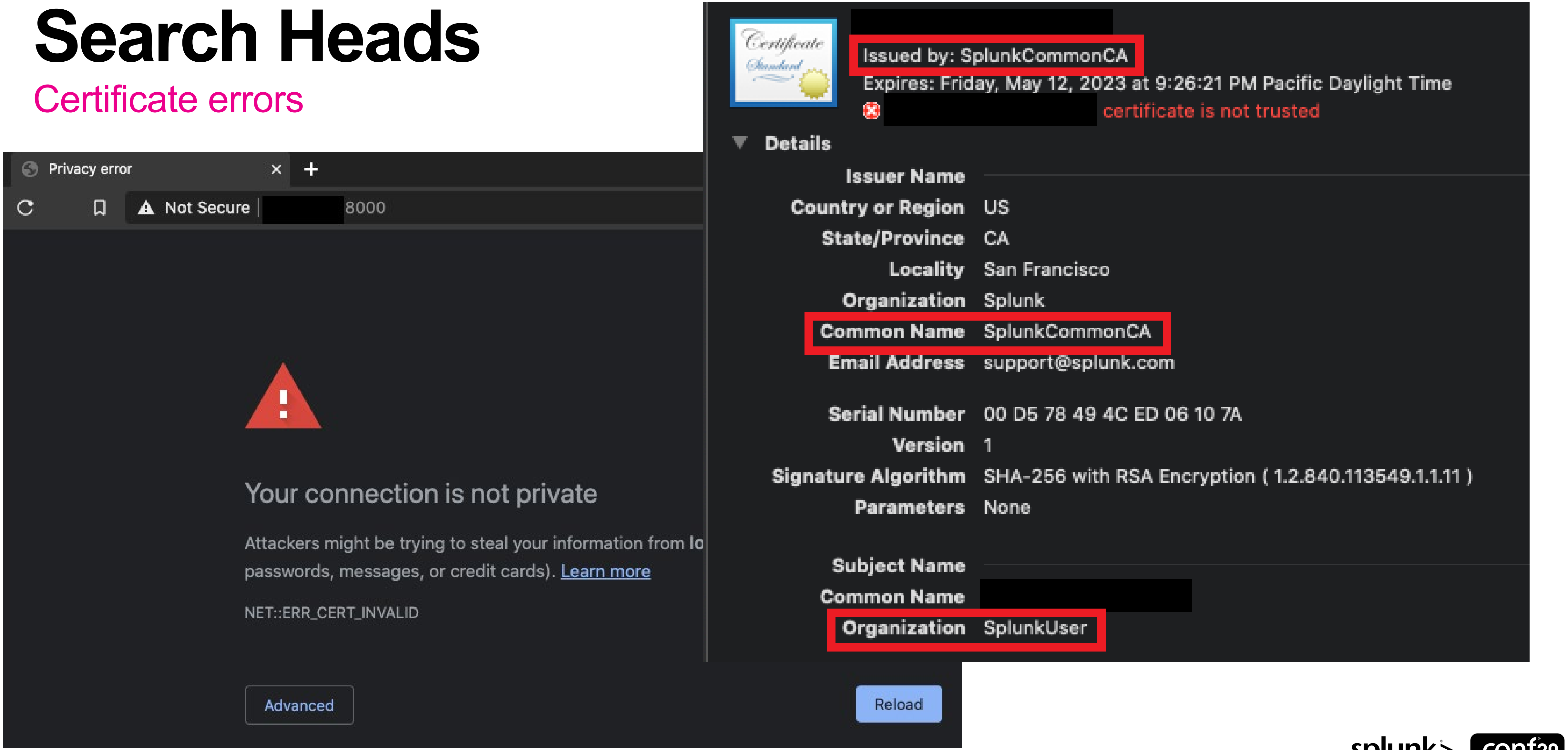
```
[search]
enable_memory_tracker = true
search_process_memory_usage_percentage_threshold = 20
```

Limit max search run time in authorize.conf (role-level and/or default stanza) ✓

```
[role_foo]
srchMaxTime = 2h
```

Search Heads

Certificate errors



[redacted]8000

Your connection is not private

Attackers might be trying to steal your information from lo
passwords, messages, or credit cards). Learn more

NET::ERR_CERT_INVALID

[redacted]

Issued by: SplunkCommonCA
Expires: Friday, May 12, 2023 at 9:26:21 PM Pacific Daylight Time
☒ [redacted] certificate is not trusted

▼ Details

Issuer Name
Country or Region US
State/Province CA
Locality San Francisco
Organization Splunk
Common Name SplunkCommonCA
Email Address support@splunk.com

Serial Number 00 D5 78 49 4C ED 06 10 7A
Version 1
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None

Subject Name
Common Name [redacted]
Organization SplunkUser

Search Heads

Hardening guidelines

Enable SSL and use signed certificates from a trusted root CA for Splunk Web🔒✅🔍

Search Heads

Hardening guidelines

Enable SSL and use signed certificates from a trusted root CA for Splunk Web🔒✅🔍

Limit number of users with the admin role 🔒✅🔍

Search Heads

Hardening guidelines

Enable SSL and use signed certificates from a trusted root CA for Splunk Web🔒✅🔍

Limit number of users with the admin role 🔒✅🔍

Use Single Sign-On (SSO) for web access (if available)🔒

- Consider MFA as well https://docs.splunk.com/Documentation/Splunk/latest/Security/AboutMultiFactorAuth

Search Heads

Hardening guidelines

Enable SSL and use signed certificates from a trusted root CA for Splunk Web🔒✅🔍

Limit number of users with the admin role 🔒✅🔍

Use Single Sign-On (SSO) for web access (if available)🔒

- Consider MFA as well https://docs.splunk.com/Documentation/Splunk/latest/Security/AboutMultiFactorAuth

Ensure that insecure encryption algorithms are disabled (SSL3, TLS 1.0, TLS 1.1)🔒✅

- Applicable only to below Splunk v7.0.0 https://www.duanewaddle.com/quick-hit-disabling-sslv3-in-splunk/

Search Heads

Hardening guidelines

Enable SSL and use signed certificates from a trusted root CA for Splunk Web🔒✅🔍

Limit number of users with the admin role 🔒✅🔍

Use Single Sign-On (SSO) for web access (if available)🔒

- Consider MFA as well https://docs.splunk.com/Documentation/Splunk/latest/Security/AboutMultiFactorAuth

Ensure that insecure encryption algorithms are disabled (SSL3, TLS 1.0, TLS 1.1)🔒✅

- Applicable only to below Splunk v7.0.0 https://www.duanewaddle.com/quick-hit-disabling-sslv3-in-splunk/

Use token-based authentication for REST API access🔒

Search Heads

Hardening guidelines

Enable SSL and use signed certificates from a trusted root CA for Splunk Web🔒✅🔍

Limit number of users with the admin role 🔒✅🔍

Use Single Sign-On (SSO) for web access (if available)🔒

- Consider MFA as well https://docs.splunk.com/Documentation/Splunk/latest/Security/AboutMultiFactorAuth

Ensure that insecure encryption algorithms are disabled (SSL3, TLS 1.0, TLS 1.1)🔒✅

- Applicable only to below Splunk v7.0.0 https://www.duanewaddle.com/quick-hit-disabling-sslv3-in-splunk/

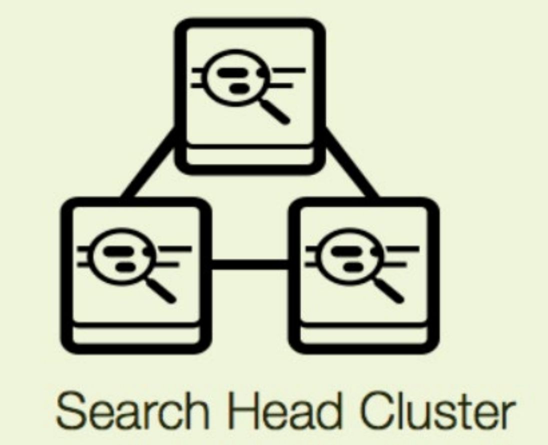
Use token-based authentication for REST API access🔒

Configure reasonable search concurrency and disk quotas in splunk roles✅

Search Head Clusters

Hardening guidelines

Configure pass4symmkey for shcluster🔒✅

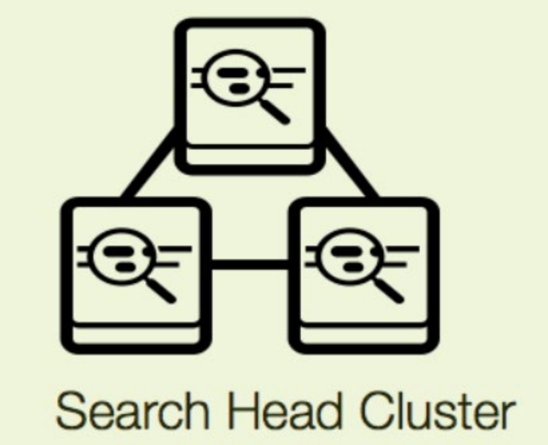


Search Head Clusters

Hardening guidelines

Configure pass4symmkey for shcluster 🔒 ✅

Lock-down SHC replication ports to only SHC members 🔒 ✅



Search Head Clusters

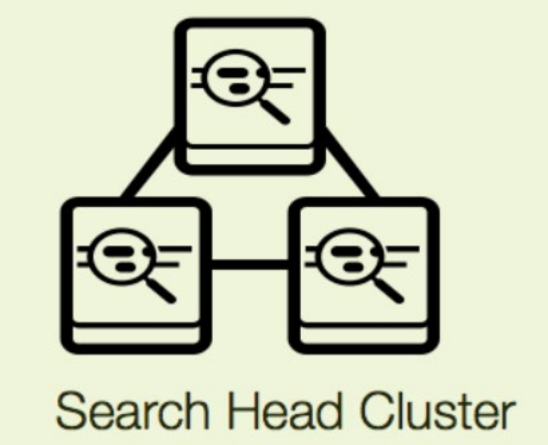
Hardening guidelines

Configure pass4symmkey for shcluster 🔒 ✅

Lock-down SHC replication ports to only SHC members 🔒 ✅

Forward logs from your load balancer or reverse proxy

- Splunk Add-on for HAProxy
- Splunk Add-on for NGINX
- More on Splunkbase



Search Head Clusters

Hardening guidelines

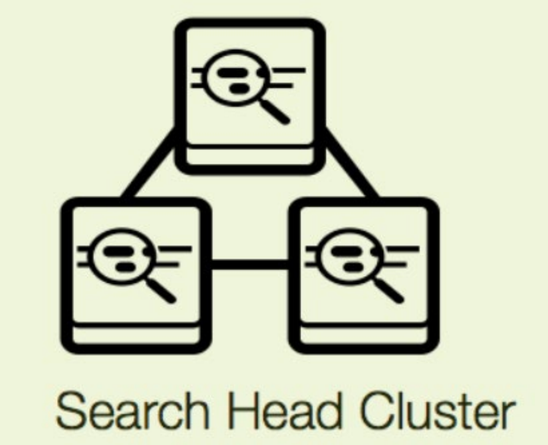
Configure pass4symmkey for shcluster🔒✅

Lock-down SHC replication ports to only SHC members 🔒✅

Forward logs from your load balancer or reverse proxy

- Splunk Add-on for HAProxy
- Splunk Add-on for NGINX
- More on Splunkbase

As always, more in the Appendix



What’s Next?

1) Download this deck

2) Identify one component to secure

3) Block out time on your calendar

4) Start with that

5) Questions?

Ask now

Read Securing Splunk manual on docs.splunk.com

Reach out via Splunk Answers

Reach out via Splunk-Usergroups Slack

Email me mason@splunk.com

Thank You

Please provide feedback via the

SESSION SURVEY

.conf20

splunk>

Appendix

All the Splunk security info you could have ever wanted…

Important Links

- https://docs.splunk.com/Documentation/Splunk/latest/InheritedDeployment/Ports
- https://docs.splunk.com/Documentation/Splunk/latest/Security
- https://docs.splunk.com/Documentation/Splunk/latest/Security/AboutMultiFactorAuth
- https://docs.splunk.com/Documentation/Splunk/latest/Security/Setupauthenticationwithtokens
- https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Forwardsearchheaddata
- https://www.duanewaddle.com/quick-hit-disabling-sslv3-in-splunk/
- https://docs.splunk.com/Documentation/Splunk/latest/Security/Dataintegritycontrol#Configure_data_integrity_control
- https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Protectagainstthelossofin-flightdata
- https://docs.splunk.com/Documentation/Splunk/latest/Data/AboutHECIDXAck
- https://docs.splunk.com/Documentation/Splunk/latest/Data/UseHECusingconffiles#Global_settings
- https://wiki.splunk.com/images/f/fb/SplunkTrustApril-SSLipperySlopeRevisited.pdf
- https://www.duanewaddle.com/splunk-pass4symmkey-for-deployment-client-deployment-server/
- https://github.com/splunk/docker-swarm-splunk-hf
- https://downloads.cisecurity.org/download-issues/benchmarks
- https://galaxy.ansible.com/search?deprecated=false&keywords=cis%20benchmarks&order_by=-relevance&page=1
- https://opensource.com/article/18/3/ansible-patch-systems

Operating System Checklist

Security Control	Implemented?
System hardened against CIS benchmarks|other hardening standards	
splunk installed as non-privileged user	
IPTABLES|ufw|firewalld configured	
SSH access restricted	
SSH access controlled via LDAP|ZeroTrust	
All SSH keys rotated periodically	
Kernel patched and up-to-date	
All packages patched and up-to-date	
Vulnerability scan regularly completed and results remediated	

Splunk Checklist (All Roles)

Security Control	**Implemented?**
Operating System Checklist evaluated	
Splunk installed as non-privileged user	
FACLs configured to allow splunk user to read /var/log	
Monitor stanza configured and enabled for /var/log in inputs.conf	
Splunk _internal and _audit logs forwarded to indexers in outputs.conf *applies to all roles except indexers	
Splunk admin password changed	
Latest version of Splunk installed	
AD|LDAP|SSO used in authentication.conf	
Splunk admin role access limited	
Default splunk certificates changed	
Splunk enable boot-start	
splunk.secret standardized	
All Splunk-related credentials stored in a secret manager	
If Splunk version less than 7.0.0, insecure encryption algorithms disabled	

Universal Forwarder Checklist

Security Control	Implemented?
Splunk Checklist (All Roles) evaluated	
UF configured as a DS client	
REST listener port disabled in server.conf	
pass4SymmKey configured for DS authentication	

Heavy Forwarder Checklist

Security Control	Implemented?
Splunk Checklist (All Roles) evaluated	
Universal Forwarder Checklist evaluated	
Unnecessary Splunk services evaluated and disabled (REST, Splunkd, Web, KV store)	
If Splunk web enabled, enableSplunkWebSSL=true in web.conf	
If Splunk web enabled, new CSR generated, signed, installed, and configured in web.conf	

Deployment Server Checklist

Security Control	Implemented?
Splunk Checklist (All Roles) evaluated	
If Internet facing, WAF configured in front of DS	
If Internet facing, non-standard splunkd port configured for mgmtHostPort in web.conf	
pass4SymmKey client authentication enabled and restmap.conf configured	
If Splunk web enabled, TLS enabled	
If Splunk web enabled, new certificate generated, signed, and installed	

Indexer Checklist

Security Control	Implemented?
Splunk Checklist (All Roles) evaluated	
Data integrity control enabled in indexes.conf	
Indexer acknowledgement enabled for Splunk2Splunk	
Indexer acknowledgement enabled for HTTP Event Collector (HEC)	
If using indexer clustering, pass4SymmKey configured	
Splunk web disabled	
acceptFrom configured in inputs.conf	
Dedicated volume used for $SPLUNK_DB and owned by splunk user	
enableSSL = true configured in inputs.conf in the http stanza	

Search Head Checklist

Security Control	Implemented?
Splunk Checklist (All Roles) evaluated	
enable_memory_tracker enabled and configured in limits.conf	
srchMaxTime configured for each role (and default stanza) in authorize.conf	
excludeReplicatedLookupSize configured in distsearch.conf	
If Splunk web enabled, enableSplunkWebSSL=true in web.conf	
If Splunk web enabled, new certificate generated, signed, installed, and configured in web.conf	
Number of users in the splunk admin role limited to true admins	
SSO enabled and configured (if available)	
Multi-factor authentication (MFA) enabled for Splunk Web access	
Token-based authentication in use for REST API access	
If SSO unavailable, Splunk users authenticated via AD|LDAP	
Reasonable search concurrency quotas configured for each role (and default stanza) in authorize.conf	
Reasonable disk quotas configured for each role(and default stanza) in authorize.conf	
If SHC, replication ports locked down to only SHC members	
If SHC, pass4SymmKey configured	
If SHC, load balancer logs forwarded to Splunk	