Secure and Harden Splunk Enterprise

These are the steps that can be taken to secure and harden Splunk environments.

Securing Data Communication

Between Splunk components

SSL encryption of data communication between Splunk components (e.g. Search heads, indexers, deployment servers and forwarders) over port 8089 is implemented by default and the recommendation is to leave it enabled.

Communication from browsers to Splunk Web

SSL encryption of Splunk web user sessions. This would commonly be the search head, but could also be other components where Splunk web is running. You can either use self-signed certificates or implement your own SSL certificate. It would be considered best practice to implement on your search heads as a minimum.

Communication from forwarders to indexers

SSL encryption of the log data flowing from the Splunk forwarders to the Splunk indexers. If you have a mix of SSL enabled and non-SSL enabled forwarders, they will need to send to separate ports on the indexer (e.g. 9997 for non-SSL and 9998 for SSL). There may be some small performance impact at index time, depending on data volumes and the amount of indexers you have.

Securing Against Data Loss or Modification

Enable Indexer Acknowledgement

Used for ensuring delivery of data from the forwarder to the indexer. When enabled, the forwarder will resend any data not acknowledged as "received" by the indexer.Expect this to have some performance impact and introduce the possibility of event duplication. Also ensure the forwarder queue size is sufficient to cache data in the event that data cannot get to the indexers.

Enable Event and IT Data Block Signing

IT events, audit events and archives can be cryptographically signed to help detect any modification or tampering of the underlying data. Expect a fairly high indexing performance cost when implementing these features. Signing cannot currently be used in a clustered setup, nor is it supported for distributed search, so it's usefulness may be somewhat limited. The less secure Event Hashing feature can be leveraged when signing cannot be used.

Enable Event Hashing

Event hashing provides a lightweight way to detect if events have been tampered with between index time and search time. Event Hashes are not cryptograpically secure like IT data block signing. Individual event hashing is more resource intensive than data block signing and someone could tamper with an event if they obtain physical access to the back-end file system.

Securing Data Access

Integrate with existing Authentication and IDM controls

Integration of Splunk with existing identity management systems in your business (e.g. LDAP, SSO, 2-Factor/Radius), to meet company policies and requirements. There are many out of the box common integrations, such as LDAP. For others, some programming may be required.

Restrict Access using Roles

Implementation of roles within Splunk, to restrict access to only the data that users of those roles need. Implement when you need to restrict access to data in Splunk. Plan out your role-based access carefully. Think about all the individuals that will need access and design a role based approach that will scale and can be managed effectively.

Remove Inactive Users

Identify and remove all users that have not logged into Splunk for xx days, all users that may have changed roles and no longer require Splunk access and all users that have left the company.You can have Splunk alert on user activity and/or integrate Splunk with your Identity Management (IDM) systems within your company.

Anonymize / Mask Sensitive Data

Splunk is able to anonymize or mask sensitive data in events, such as credit card numbers or social security numbers, to prevent this data from being indexed and stored in Splunk. This is handled through the use of regex or sed scripts when the data hits Splunk. A better approach might be to see if you can configure logging such that sensitive data does not get into the logs in the first place, but this is not always possible.

Securing Other Areas

Stop Splunk Web when not in use

Splunk Web is typically enabled by default on many components such as indexers, search heads, deployment servers and even heavy forwarders. However, most of the time, it only really needs to be enabled on the search head. Stop Splunk web on components other than the search head. When you want to use the web front-end of a particular component, simply start it up.

Change the default username/password (*on the Forwarders too…*)

The default username/password for all Splunk components is admin/changeme. It goes without saying that a username and password that everyone knows is not terribly secure!

Any endpoints where Splunk is installed with the default username/password could potentially be open to malicious activity. If required, it is possible to script a password change via the deployment server to bulk change all Splunk forwarder passwords.

Implement appropriate firewall/port rules

Splunk uses a number of ports and directions for its various components.

It is best practice to only open up these ports/directions rather than allowing all directions and ports.

The following table lists the core firewall rules required by default Splunk configurations and the direction required. If you listen/send data on other ports, then you will need to implement those rules as well.

Component	TCP Port	Direction	What is the traffic?
Search Head	8000 8089	Inbound Both	Splunk Web Internal Splunk communication
Indexer	8000 8089 9997	Inbound Both Inbound	Splunk Web Internal Splunk communication Incoming Splunk TCP from forwarders
Deployment Server	8000 8089	Inbound Inbound	Splunk Web Internal Splunk communication
Forwarder	9997 8089 514 (maybe also UDP)	Outbound Outbound Inbound	Outgoing Splunk TCP Outgoing Splunk communication Inbound syslog data if set to receive

Avoid running Splunk as Root

It is not good security practice to run software as the root user and Splunk does not need to be run as root in production.When running as a non-root user, ensure the correct permissions are assigned to read log files, write to the

splunk directory, execute needed scripts and bind to appropriate network ports.

Do not use Splunk Free in a Production Environment

Splunk Free is a free version of Splunk that the 60 day Enterprise trial defaults to after the 60 days are up. However, the free version of Splunk is also free of any security. Splunk Free is not designed to be used in a production environment. The lack of security in the free version could, in theory, allow any machine readable file on the endpoint where Splunk Free is installed to be read.