

Study Guide

Introduction to Splunk

Created By: Tahir Ibrahim, Teaching Assistant

Module 1: Introduction

Lesson 1.1: Welcome

Skills Learned From This Lesson: Intro to Splunk

- Learning Objectives
 - Discuss Splunk products and use cases
 - Navigate the web console and run basic Splunk commands
 - Set up basic alerts, reports and dashboards based on simple searches
 - Install a practice environment and add data
 - Be aware of other important topics for further study
- Course Break Down
 - Module 1: Introduction Module
 - Module 2: Splunk products and resources
 - Module 3: Setting up Splunk
 - Module 4: Data
 - Module 5: Basic searches, Alerts, Reports and Dashboards
 - Module 6: Conclusion, review and other notes

Lesson 1.2: What is Splunk?

Skills Learned From This Lesson: Splunk, Using Splunk

- Splunk is a company specializing in data use and processing
 - 'Splunk turns machine data into answers'

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Splunk software aggregates, processes, analyzes and helps you use small to a massive amount of data. Its particularly helpful for turning unstructured data into usable information
- Splunk history
 - 2003 - Founded
 - 2012 - Went public
 - 2017 - Employees become some of the highest paid in the world
 - 2018 - Several major acquisitions including Phantom, VictorOps and KryptonCloud
- Splunk is good for organizing raw data
- Splunk takes data that's difficult to handle and makes it usable in a variety of ways
- Reporting, alerting, troubleshooting, threat hunting and making a business decision and so on

Lesson 1.3: Splunk and Your Career

Skills Learned From This Lesson: Splunk, Career, Certifications

- Average Salary
 - \$66,966 to \$149,142 per year
- Resume Items
 - Installed and maintained small Splunk enterprise environment
 - Created alerts, dashboards and reports from Splunk data
 - Onboarded new data sources for Splunk environment
- Splunk Certification Paths
 - Splunk core certified user
 - Free
 - Requires completion of online Splunk fundamentals 1 course
 - Splunk core certified power user
 - Splunk Fundamentals 1 & 2 required, plus exam
 - Splunk fundamentals 2 costs \$2000 USD
 - The exam costs \$125 USD
 - Splunk Enterprise Certified Admin
 - Previous courses and certifications required

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Splunk enterprise system administration course, Splunk enterprise data administration course, Certification exam
- Other Certifications
 - Splunk enterprise certified architect
 - Splunk certified developer
 - Splunk enterprise security certified admin
 - Splunk IT service intelligence certified admin
- Many different job possibilities, Splunk can be an added bonus to an existing skillset or a career itself.
- Certification paths exist and after the first certification it costs money

Module 2: Splunk Products, Resources and Certifications

Lesson 2.1: Splunk Products, Resources and Certifications

Skills Learned From This Lesson: Splunk, Introduction

- <https://www.splunk.com/>

Lesson 2.2: Splunk website

Skills Learned From This Lesson: Splunk, Training, Documentation

- Splunk website has a variety of resources that can be accessed
- <https://docs.splunk.com/Documentation>
 - Documentation area
- Installation manuals
- Q&As on the website
- Splunkbase has Apps that can be installed
- Splunk Training

Lesson 2.3: Splunk products

Skills Learned From This Lesson: Splunk, Products, knowledge

- Splunk core
 - Splunk Free - Max Daily Indexing Volume 500MB
 - Splunk Light - Max Daily Indexing Volume 20GB

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Splunk Enterprise - Max Daily Indexing Volume Unlimited
- Splunk Cloud - Max Daily Indexing Volume Unlimited
- Pricing is based on how much data is indexed on a daily basis
- Speciality Focuses
 - Splunk Enterprise Security (ES)
 - Splunk User Behaviour Analytics (UBA)
 - Splunk IT Service Intelligence
 - Splunk Insights for Infrastructure
 - Splunk Insights for AWS Cloud Monitoring
 - Splunk Insights for Ransomware
 - Splunk for Industrial IoT
- Splunk Enterprise
 - Investigate
 - Log aggregation
 - Rules, statistics, correlation
 - Ad Hoc searches & data pivot
 - Realm of known
- Splunk UBA
 - Detection
 - Risk behaviour detection
 - Entity profiling, scoring
 - Kill chain, graph analysis
 - Realm of unknown
- Other Products
 - Phantom
 - Automation tool, that sets off an automated chain of events
 - VictorOps
 - Manage on-call schedules and create notification either through push notification, phone calls or emails
- Splunk enterprise security is an addon to add on a Splunk platform to give additional tools
- Summary
 - Splunk platforms
 - Splunk Enterprise, Splunk Cloud, Splunk light, Splunk free

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Additional analytics, intelligence operationalization
 - Splunk insights, Splunk enterprise security..etc
- Other tools
 - Phantom, VictorOps

Module 3: Setting Up Splunk

Lesson 3.1: Setting Up Splunk

Skills Learned From This Lesson: Splunk, Setting up Splunk, Support

- Planning Your Environment
 - For a production environment, planning is needed!
 - If you're using an unusual setup, check Splunk's system requirements prior to installation (Link in Supplemental Resources)
 - If you're working with an old system, you may need an older version of Splunk
 - Try to match your test/practise environment to the environment you will work in
- <https://splunk-sizing.appspot.com/>
 - Plans for storage requirements, based on how much data
- <https://docs.splunk.com/Documentation/Splunk/7.3.1/Capacity/IntroductiontocapacityplanningforSplunkEnterprise>
 - Capacity planning manual, checks what requires are needed to set up
- <https://docs.splunk.com/Documentation/Splunk/7.3.1/Installation/Chooseyourplatform>
 - Installation Manual shows supported OSES and system requirements
- https://www.splunk.com/en_us/download.html
 - Splunk sandbox has a free 7-day trial

Lesson 3.2: Parts of Splunk

Skills Learned From This Lesson: Splunk, Data pipeline, How Splunk works

- Data Pipeline
 - Input
 - Splunk is getting data
 - Parsing
 - Data turning to events, Example, line breaks or data transformed based on certain rules

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Indexing
 - Taking the parsed events and putting them into an index for later use
 - Searching
 - Interaction between the search head and the indexers. The search head is responsible for search management, search management is where you would go to running a search and that search requests go into the indexer, then the results get sent back to the search head to view and work with
 - At the searching level, schedule searches, alerts and dashboards
 - UF (Universal Forwarder) Example, an agent set up on a windows server to collect Windows event logs
 - IDX - Parsing and Indexing, taking the data breaking it into events and organising it so the search heads can easily find
 - SH (Search Heads)
- UF ⇒ IDX ⇒ SH
 - Search Heads
 - Search management
 - Scheduled searches, alerts, dashboards
 - Distributes searches to indexers
 - Indexers
 - Receive, index, store data
 - Search data based on search requests from search heads
 - Index - noun: a data repository
 - Index - verb: Processing raw data
 - Indexer: Splunk instance that indexes data

An indexer indexes data and puts it into an index

- Forwarders
 - Sends data onward
 - Universal Forwarder
 - Light forwarder (deprecated)
 - Heavy forwarder

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Other server roles
 - Deployment server can help you manage forwarders, and set apps by groups..etc
- Distributed environments
 - “Horizontal scaling”
 - Separate out the pieces
- Deployment Scales
 - Very small office/department
 - <20GB
 - <100 forwarders
 - Large Enterprise
 - 300GB+
 - Up to 1000s of forwarders
- Clustering
 - Data replication
 - Availability
 - Fidelity
 - Recovery
- Review
 - Forwarders send data, indexers turn data into events and place them in indexes, search heads send search requests, display data
 - A large company will likely need a distributed environment
 - Clustering provides redundancy

Lesson 3.3: Installing Splunk on Linux

Skills Learned From This Lesson: Installation, Linux, Splunk

- https://www.splunk.com/en_us/download.html
- Choose Splunk Free, then click on Linux and download depending on your distribution
- Can also download using the command line using wget
- Once downloaded use the command line to uncompress it by doing to the directory of the downloaded file and type **tar xvzf [package name].tgz -C /opt**
- That will download to /opt/splunk/bin/splunk
- To start Splunk using the command line: **/opt/splunk/bin/splunk start**

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Enter a username and password and once configured it should show you the web address to open the web interface

Lesson 3.4: Installing Splunk on Windows

Skills Learned From This Lesson: Installation, Windows, Splunk

- https://www.splunk.com/en_us/download.html
- Choose Splunk Free
- Choose 32bit or 64 bit based on your OS
- Once downloaded execute the windows installer file and go through the options to configure the installation
- Once downloaded can access the interface on **localhost:8000** in a web browser
- Typing in the username and password to enter the interface

Lesson 3.5: Installing a Universal Forwarder

Skills Learned From This Lesson: Universal Forwarder, Splunk, Installation

- Review: UF
 - Universal Forwarder is a type of forwarder that..forwards data
 - Install on a machine that you wish to collect data from
 - There are other ways to get data into Splunk, but this is a popular method
- A Few Checks
 - Can host talk to Splunk server?
 - Splunk ports
 - What permissions are needed to access or retrieve the data you want to forward?
- Splunk Ports

Component	Purpose	Communicates on	Listens on
All Components	Management/REST API	N/A	TCP/8089
Search head/Indexer	Splunk Web access	Any	TCP/8000
Search head	App Key-Value Store	Any	TCP/8065, TCP/8191

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Indexer	Receiving data from forwarders	N/A	TCP/9997
Indexer cluster peer node/Search head cluster member	Cluster replication	N/A	TCP/9887
Index/Forwarder	Network input (Syslog)	N/A	UDP/514

- https://www.splunk.com/en_us/download/universal-forwarder.html
- Link to download Splunk Universal Forwarder

Module 4: Data

Lesson 4.1: Data

Skills Learned From This Lesson: Data, Splunk, Configurations

- This Module:
 - Using the web interface
 - Ways to get data into Splunk
 - Indexes and source types
 - Modifying input.conf to get data

Lesson 4.2: Web Interface Tour

Skills Learned From This Lesson: Data, Splunk, Configurations

- To check the status of Splunk to know if it is running or not type **/opt/splunk/bin/splunk status** in the command line
- To tell Splunk to automatically start up when the machine starts to type the following: **/opt/splunk/bin/splunk enable boot-start**
- To start Splunk type the following **/opt/splunk/bin/splunk start**
- Which will show the HTTP port number, hopefully, port:8000
- To enter into the web interface type the following in the URL **localhost:8000** then enter your credentials

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Once logged in the Apps are found on the left-hand side, Clicking on the Search & Reporting app, from here you can search for data
- To view internal data type the following in the search bar: **index=_internal** which can be saved as a report, Alert or an Event type.
- There are different options is visualise the data, The i button at the top is the health status of Splunk, Messages are a good place to check for any possible errors or issues
- For an overall view of the health status of Splunk, **Settings** → **Monitoring Consoles** an overview of usages and statuses
- **Settings** → **Searches, reports and alerts**, a report section for alerts, reports and saved searches
- **Settings** → **Access Controls** → **Users**, to add a new user
- **Settings** → **Access Controls** → **Roles**, to set new roles for the user

Lesson 4.3: Ways to Get Data

Skills Learned From This Lesson: Data, Splunk, Configurations

- This image shows you what Splunk can index



- There are many ways to get data
 - Monitor files and directories

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

- Upload data
- Run scripts and collect results
- TCP/UDP ports
- Syslog collection
- Collect events using WMI
- Connect to databases
- APIs
- And more
- Indexes
 - An indexer indexes data and puts it in an index
 - Data repository
 - Help with
 - Search efficiency
 - Separating policies
 - Access control
- Source types
 - Identify the structure of events
- Field extractions
 - Fields have name/value pairings
 - Jun 2 14:55:46 fire00 fire00: NetScreen device_id=fire00 [Root]system-notification-00257(traffic): start_time="2006-06-02 14:55:45# duration=0 policy_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust **action=Deny** sent=0 rcvd=0 src=192.168.2.1 dst=1.2.3.4 src_port=3036 dst_port=7001
 - action=Deny
 - action=Allow
- To upload a data file into Splunk, go to **Settings** → **Add Data** → **Upload**
- Once uploaded can select a source type on the left-hand side and customise it to your liking
- Once data is uploaded, the fields on the lefthand side can be customised by clicking on **+ Extract New Fields** link
- Click on a sample event to work with then select 'next' to select a method
 - Regular Expression
 - Splunk Enterprise will extract fields using a regular expression

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Delimiters
 - Will extract fields using a delimiter (such as commas, spaces or characters)
- Clicking next will give the option to write your own Regex (Regular Expression)
- Can select fields and customise it to the way you want it

Lesson 4.4: Inputs Monitoring

Skills Learned From This Lesson: Data Inputs, Splunk configurations, Splunk

- Configuration Files
 - Settings, authentication information, save searches, etc.
 - Ends in .conf
 - Written in stanzas (contains configuration parameters)
 - Splunk often needs to be restarted after changes
- Inputs.conf
 - The input.conf is found at: **\$SPLUNK_HOME/etc/system/local**
 - [monitor://<path>]
 - index=
 - source type =
- Configure receiving
 - On Splunk web interface
 - Server settings check
 - Listen on port 9997
- To set up Splunk to listen on port 9997
 - **Settings** → **Forwarding and receiving** → **configure receiving** → **New receiving port**, then enter the port you have listening on the universal forwarder
- To check what ports are listening type in the following command in terminal: **netstat -tulpn**

Module 5: Using Data

Lesson 5.1: Using Data

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

Skills Learned From This Lesson: Splunk, Handling data,

- In this module:
 - Searches
 - Alerts
 - Reports & Dashboards
 - Apps

Lesson 5.2: Searches

Skills Learned From This Lesson: Splunk, Handling data, Splunk Searches

- To get started login to the Splunk web interface and go to the search and reporting app

The screenshot displays the Splunk Search & Reporting interface. At the top, the navigation bar includes 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main search bar contains the query 'index=_internal' and shows '333 of 436 events matched'. A 'Time Range Picker' is set to '1 minute window'. Below the search bar, there are tabs for 'Events (333)', 'Patterns', 'Statistics', and 'Visualization'. A timeline visualization shows two green bars representing event counts. Below the timeline, a table of matching events is displayed. The table has columns for 'Time' and 'Event'. The first event is from 4/15/18 at 12:28:42.386 AM, and the second is from 4/15/18 at 12:28:42.385 AM. The event details include IP addresses, user agents, and source information.

i	Time	Event
>	4/15/18 12:28:42.386 AM	127.0.0.1 - [15/Apr/2018:00:28:42.386 -0700] "GET /en-US/splunkd/_raw/services/search/jobs/rt... eLine?offset=0&count=10000_1523768615245 HTTP/1.1" 200 10020 "-" "Mozilla/5.0 (Macintosh; Intel Mac... leWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36" - c8fc653b6f17e144e0ef0d7630f... host = Istewart-mbpr15.sv.splunk.com source = /Applications/Splunk/var/log/splunk/splunkd_u_access.log ... sourcetype = splunkd_u_access
>	4/15/18 12:28:42.385 AM	127.0.0.1 - admin [15/Apr/2018:00:28:42.385 -0700] "GET /en-US/splunkd/_raw/servicesNS/nobody/search... 523777291.67/events?output_mode=json&offset=-20&count=20&segmentation=full&max_lines=5&field_list=ho... cetype%2Cnetwork%2Cconcurrency%2Cduration%2CtimeDelta%2Cmailto%2Craw%2C_time%2C_audit%2C_decoration%... enttype_color%2Clinecount%2C_fulllinecount%2C_icon%2Ctag%2C_serial%2C_si&truncation_mode=abstract&... P/1.1" 200 117465 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, li... 5.0.3325.181 Safari/537.36" - c8fc653b6f17e144e0ef0d763064d542 15ms

- SPL: Search Processing Language
- Six categories of search commands:

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Distribute streaming
- Centralized streaming
- Transforming
- Generating
- Orchestrating
- Dataset processing
- Searching tips:
 - The more specific, the better
 - Limit searches by time, index, and other fields
- Fields:
 - Searchable name/value pairings
 - Field names are case sensitive
 - Field values are not case sensitive
 - You can use wildcards
 - Use quotation marks if there are spaces
- Username=Sarah is not the same as username=Sarah
- Username=sarah is the same as Username=SaRaH
- * ← is a wildcard and can be used in searches
 - Name=sa*
 - Results: Samantha, Sarah
- For spaces use quotation marks “ “
 - Name="Sarah Smith"
- Boolean operators:
 - AND
 - OR
 - NOT
 - Username=sarah AND Machine=host3
 - Username=sarah OR Machine=host3
 - Username=sarah NOT Machine=host3
 - Username=sarah Machine!=host3
- Transforming data:
 - Pipes: |
 - index=windows | stats count by host | sort -count
 - index=windows | table host | dedup host

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Search modes:
 - Fast mode
 - Smart mode
 - Verbose mode

Lesson 5.3: Alerts

Skills Learned From This Lesson: Splunk, Handling data, Splunk Alerts

- Alerts:
 - Use saved searches to look for events
 - Trigger when certain conditions are met
 - `index=firewall threatname=sql_injection | table src_ip dest_ip message`
 - Triggers an alert if an SQL injection is attempted
 - `index=authentication Machine=importantmachine action=failure`
 - Continuously runs and triggers alerts when there are more than 5 events triggered in the last 10 minutes
- Timing:
 - Scheduled
 - Cron expression
 - Real-time
 - Resource-greedy
 - Stagger saved searches
- Actions:
 - Send email
 - Webhook (to update a web resource)
 - Write results to csv
 - Add to triggered alerts
 - Others

Lesson 5.4: Reports and Dashboards

Skills Learned From This Lesson: Splunk, Handling data, Spunk Reports & Dashboards

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Reports
 - Saved searches
 - Pivot: Build tables and visualizations using multiple fields and metrics without writing searches
- Reports
 - Can be scheduled
 - Can have triggered actions
- Dashboards:
 - Help visualize data
 - Can be an interactive - form
 - Simple XML or HTML or Splunk interface
 - App use interface

Lesson 5.5: App Basics

Skills Learned From This Lesson: Splunk, Handling data, Splunk Apps

- Apps vs Add-ons
 - Apps: User interface
 - Add-ons: retrieve/work with data behind-the-scenes
- Apps:
 - Splunk built, vendor, built, user-built
 - Install in the test environment first
- Splunkbase: Site for apps and add-ons
 - <https://splunkbase.splunk.com/>
- Popular apps to look for:
 - Splunk Security Essentials
 - DBConnect - used to retrieve data from databases
 - Lookup File Editor - modify lookup tables from the web console
 - Vendor-specific apps
- Developer Life:
 - You can make an app
 - Splunk Certified Developer

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Module 6: Conclusion

Lesson 6.1: More to Learn

Skills Learned From This Lesson: Splunk, Continued Learning

- Splunk Fundamentals 1 is a free course hosted on the Splunk website
- Searching:
 - Lookup tables
 - Search macros
 - Summary indexing
 - Subsearches
 - CIM - Common Information Model
- Architecture:
 - Distributed environments
 - Clustered environments
 - Buckets
 - Load-balancing
 - Best practices
- Development:
 - Browse Splunkbase
 - Develop apps
- Troubleshooting, Management and other Topics:
 - btool
 - Job inspector
 - Crash logs
 - Project management

Lesson 6.2: Final Review

Skills Learned From This Lesson: Splunk, Review

- Module 1:
 - Splunk “Turns machine data into answers”
 - Lots of career opportunities
- Module 2:

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Resources
- Training
- Certifications
- Splunk Products:
 - Splunk enterprise
 - Splunk enterprise security
 - Splunk UBA
 - Phantom
 - VictorOps
 - Other
- Module 3:
 - Data pipeline
 - Parts of Splunk
 - Splunk installation
- Parts of Splunk:
 - Forwarders (UF)
 - Indexers (IDX)
 - Search headers (SH)
- Module 4:
 - Web interface
 - Adding data
 - Inputs.conf
- Many ways to get data:
 - Monitor files and directories
 - Upload data
 - Run scripts and collect results
 - TCP/UDP ports
 - Syslog collection
 - Collect events using WMI
 - Connect to databases
 - APIs
- Module 5:
 - Basic searches
 - Alerts

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Reports
- Dashboards
- Apps
- Make specific searches
- Stagger saved search times
- Example searches
- Module 6:
 - Lots of learning paths



Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.