EDIT TYPES

TYPE	REGEX
IPv4	^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$
IPv6	(([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4
Fortinet ID	\d{7,}
MAC	^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$
Message	*
UTC	\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[1-2]\d
EPOCH	\d{10,}

SAVE

EDIT TYPES

TYPE	REGEX
IPv4	^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$
IPv6	(([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4
Fortinet ID	\d{7,}
MAC	^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$
Message	*
UTC	\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[1-2]\d
EPOCH	

SAVE

EDIT TYPES

TYPE	REGEX
IPv4	^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$
IPv6	(([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4
Fortinet ID	\d{7,}
MAC	^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$
Message	*
UTC	\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[1-2]\d

SAVE

LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

HOME

INPUT FORMAT

+ CREATE

RECENT

Fortinet East-Aus #2md2	5 minutes ago •••
Firepower 4112	5 minutes ago •••
Catalyst C3560CX-8PC	5 minutes ago •••
MS250-24P	5 minutes ago •••

OUTPUT FORMAT

+ CREATE

RECENT

Splunk Cyber Security Team	5 days ago •••
Elastic Security Team	20 days ago •••

NORMALISATION MAPPINGS

+ CREATE

RECENT

Firepower 4112	→	Splunk Cyber Security Team Alpha	5 minutes ago
Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha	30 minutes ago
Catalyst C3560CX-8PC	→	Splunk Cyber Security Team Alpha	4 hours ago
MS250-24P	→	Elastic Security Team - Dolan	1 day ago
Firepower 1150	→	Splunk Cyber Security Team Alpha	3 days ago
Firepower 1150	→	Splunk Cyber Security Team Alpha	5 days ago

INPUT FORMATS

Search

+ CREATE

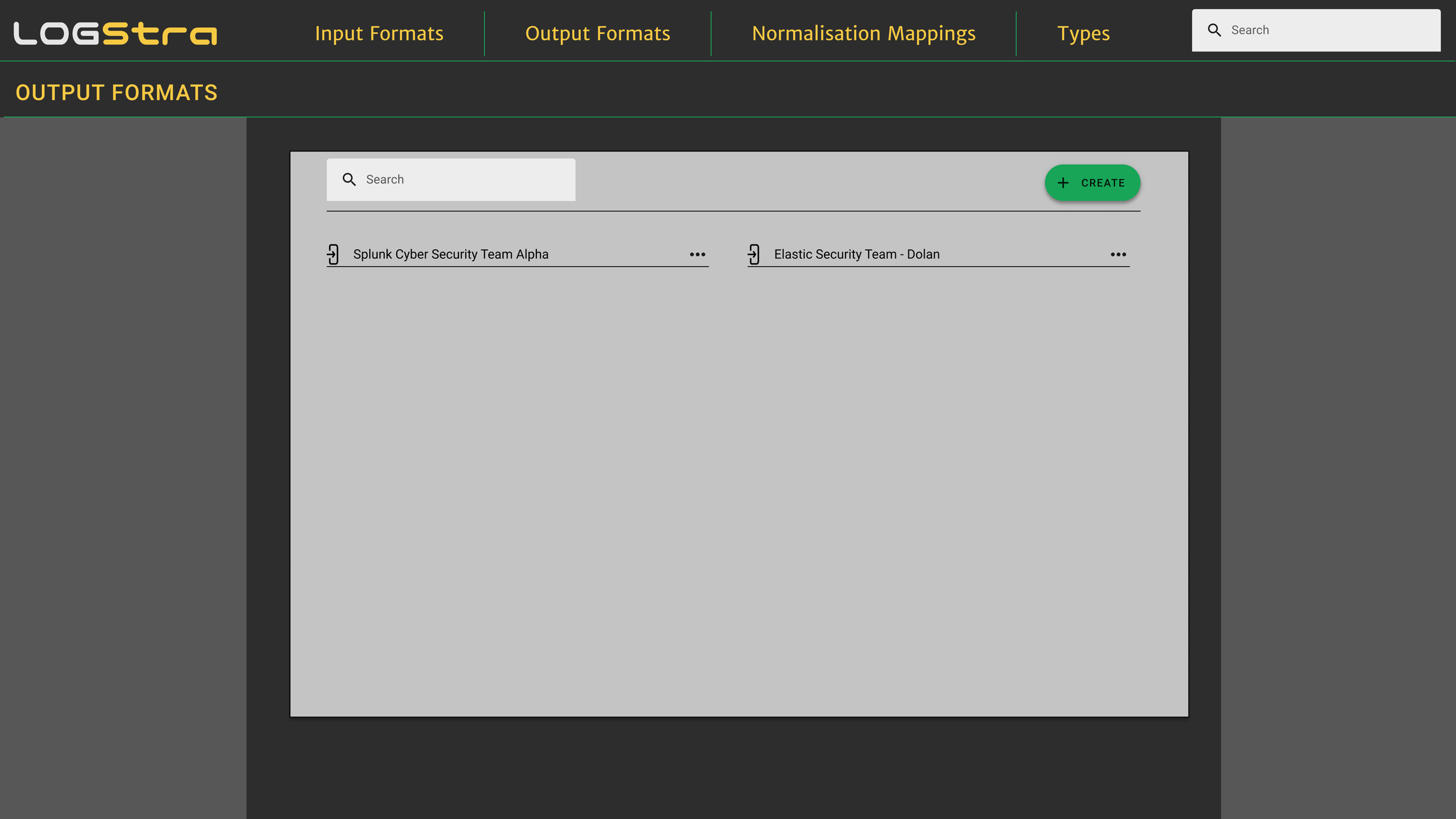
- Fortinet East-Aus #2md2
- Firepower 1150
- Firepower 4112
- Firepower 4145
- Catalyst C3560CX-12PC
- Catlayst C3560CX-8PC
- Catalyst 9500 100/40-G
- MS210-24
- MS210-24P
- MS250-24
- MS250-23P
- Nexus 9332D-GX2B
- Nexus 9332D-GX3B
- Nexus 9500 X9716-GX

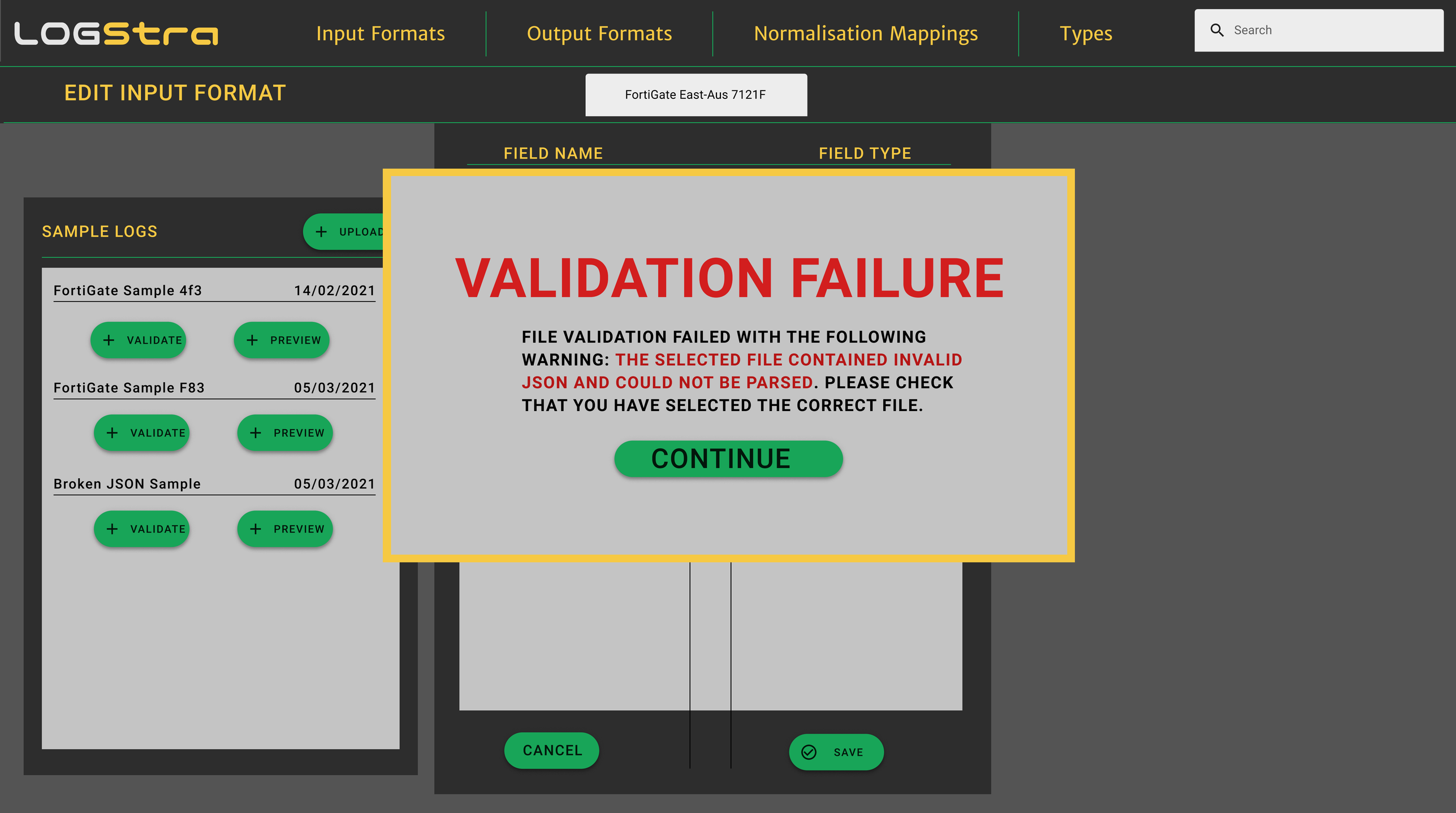
NORMALISATION MAPPINGS

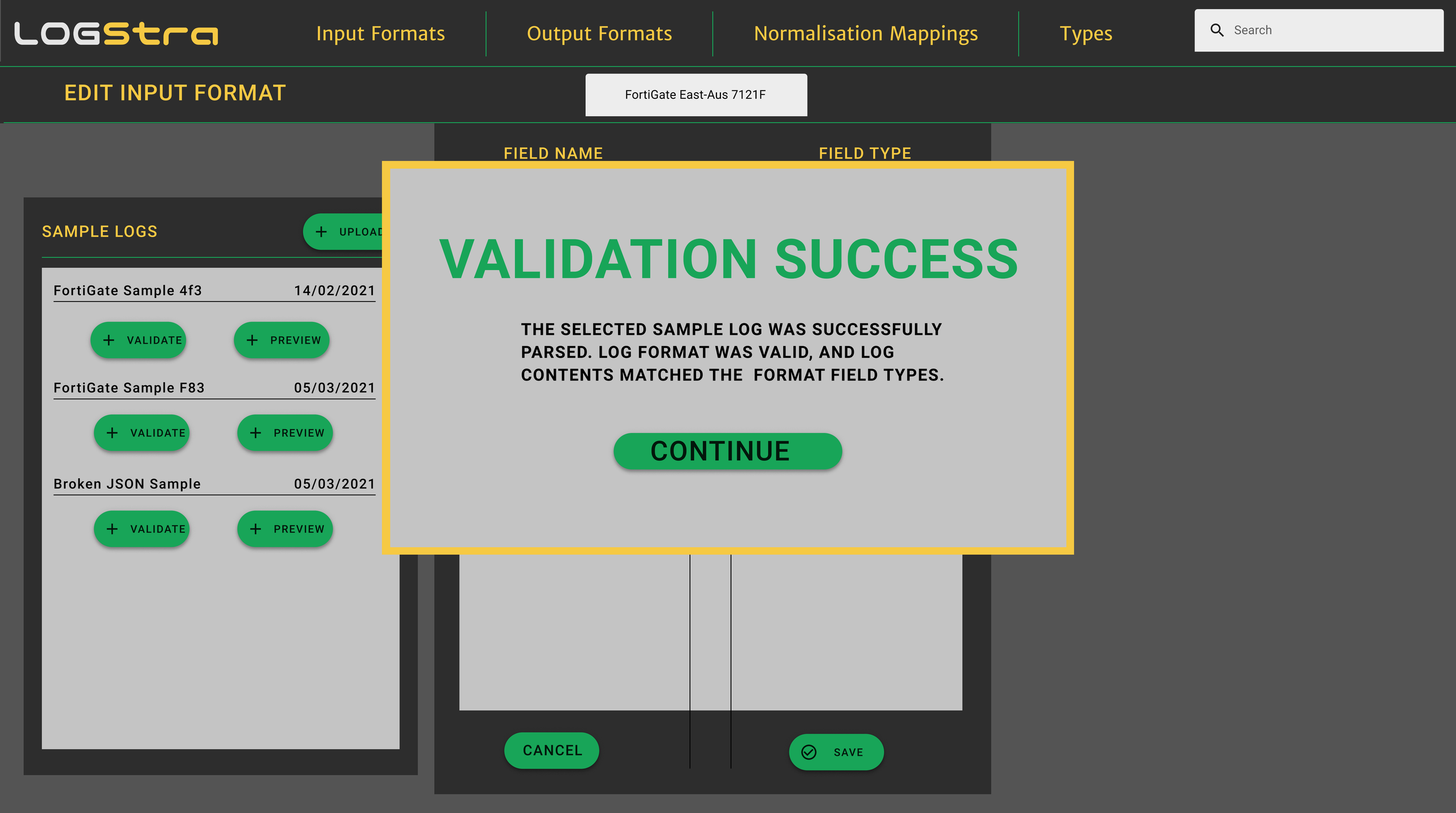
Search

+ CREATE

Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha
Firepower 1150	→	Splunk Cyber Security Team Alpha
Firepower 1140	→	Splunk Cyber Security Team Alpha
Firepower 4145	→	Splunk Cyber Security Team Alpha
Catalyst C3560CX-12PC	→	Splunk Cyber Security Team Alpha
Catalyst C3560CX-8PC	→	Elastic Security Team - Dolan
Catalyst 9500 100/40-G	→	Elastic Security Team - Dolan
MS210-24	→	Elastic Security Team - Dolan
MS250-24P	→	Elastic Security Team - Dolan
Nexus 9500 X9716-GX	→	Elastic Security Team - Dolan


LOGStra
Input Formats
Output Formats
Normalisation Mappings
Types
Search
OUTPUT FORMATS
Search
CREATE
Splunk Cyber Security Team Alpha
Elastic Security Team - Dolan


LOGStra
Input Formats
Output Formats
Normalisation Mappings
Types
Search
EDIT INPUT FORMAT
FortiGate East-Aus 7121F
FIELD NAME
FIELD TYPE
SAMPLE LOGS
+ UPLOAD
FortiGate Sample 4f3
14/02/2021
+ VALIDATE
+ PREVIEW
FortiGate Sample F83
05/03/2021
+ VALIDATE
+ PREVIEW
Broken JSON Sample
05/03/2021
+ VALIDATE
+ PREVIEW
VALIDATION FAILURE
FILE VALIDATION FAILED WITH THE FOLLOWING WARNING: THE SELECTED FILE CONTAINED INVALID JSON AND COULD NOT BE PARSED. PLEASE CHECK THAT YOU HAVE SELECTED THE CORRECT FILE.
CONTINUE
CANCEL
SAVE


LOGStra
Input Formats
Output Formats
Normalisation Mappings
Types
Search
EDIT INPUT FORMAT
FortiGate East-Aus 7121F
FIELD NAME
FIELD TYPE
SAMPLE LOGS
+ UPLOAD
FortiGate Sample 4f3
14/02/2021
+ VALIDATE
+ PREVIEW
FortiGate Sample F83
05/03/2021
+ VALIDATE
+ PREVIEW
Broken JSON Sample
05/03/2021
+ VALIDATE
+ PREVIEW
VALIDATION SUCCESS
THE SELECTED SAMPLE LOG WAS SUCCESSFULLY PARSED. LOG FORMAT WAS VALID, AND LOG CONTENTS MATCHED THE FORMAT FIELD TYPES.
CONTINUE
CANCEL
SAVE

CREATE MAPPING

SELECT INPUT FORMAT

Search

SELECT OUTPUT FORMAT

Search

Fortinet East-Aus #2md2	+ SELECT	Splunk Cyber Security Team Alpha	+ SELECT
Firepower 4112	+ SELECT	Splunk V1	+ SELECT
Catalyst C3560CX-8PC	+ SELECT	Splunk V3	+ SELECT
MS250-24P	+ SELECT	Elastic Security Team	+ SELECT

CREATE MAPPING FORTINET LOG V121 JAVA → SPLUNK V3

INPUT FIELDS		OUTPUT FIELDS
	→	Source_Destination
srcport (Suggested)	→	Source_Port
	→	Network_Log
	→	Type_Class
logid (Suggested)	→	id
time (Suggested)	→	eventTime

Save

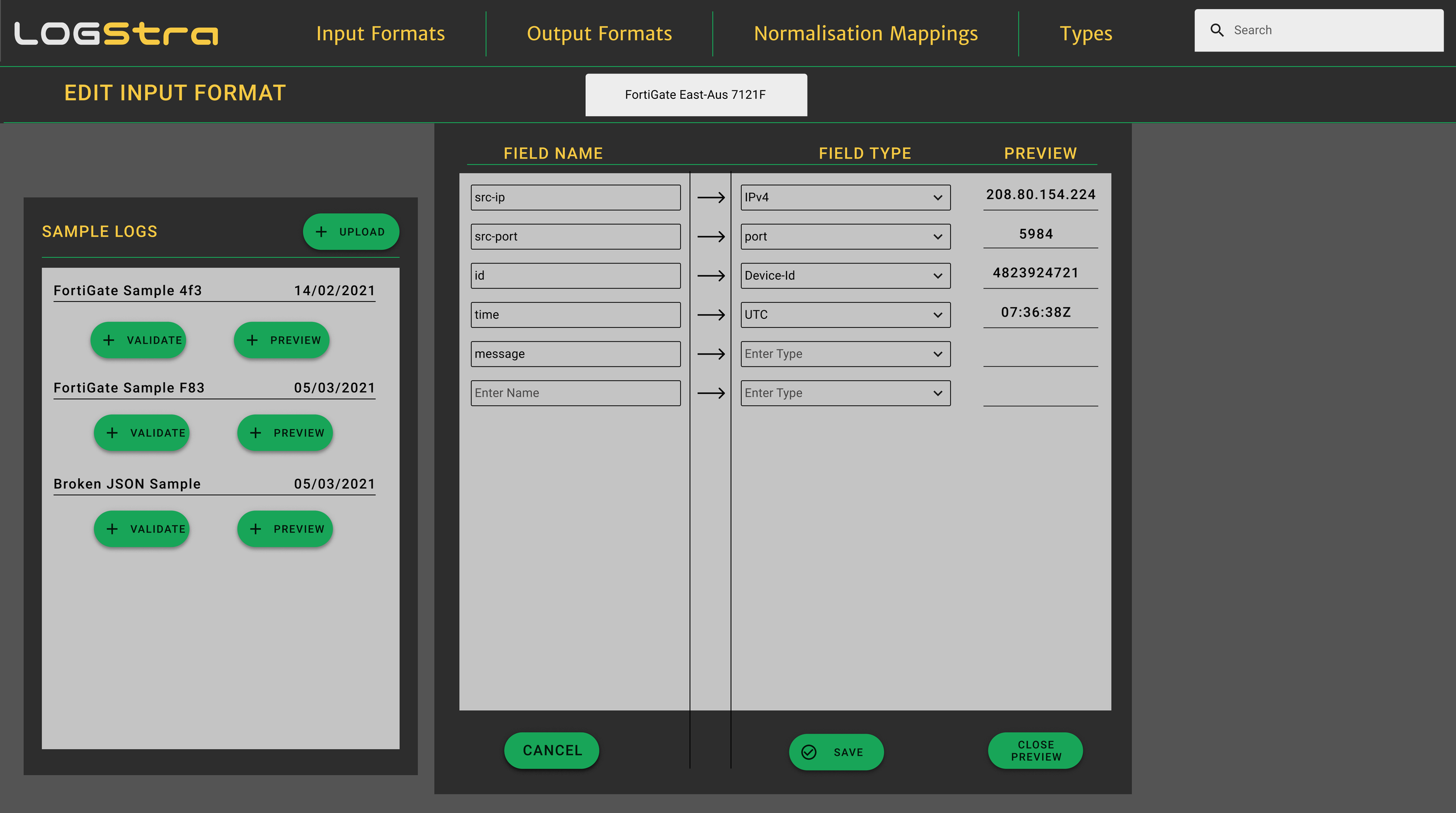
DELETE FORMAT

CONFIRM DELETE

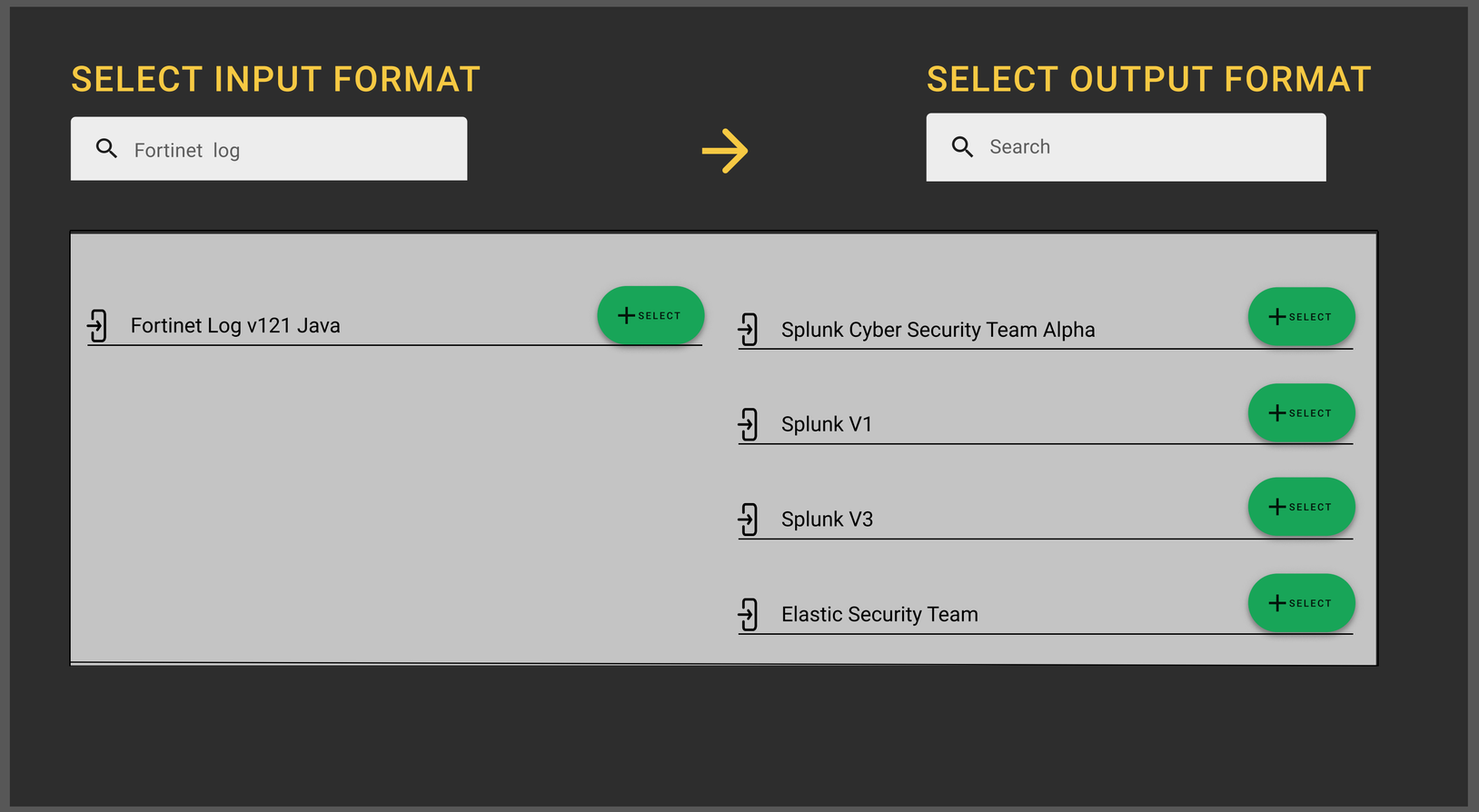
ARE YOU SURE YOU WANT TO DELETE THE FORMAT FORTINET EAST-AUS #2MD2? DELETED FORMATS CANNOT BE RECOVERED.

DELETE

CANCEL


LOGStra
Input Formats
Output Formats
Normalisation Mappings
Types
Search
EDIT INPUT FORMAT
FortiGate East-Aus 7121F
SAMPLE LOGS
+ UPLOAD
FortiGate Sample 4f3 14/02/2021
+ VALIDATE
+ PREVIEW
FortiGate Sample F83 05/03/2021
+ VALIDATE
+ PREVIEW
Broken JSON Sample 05/03/2021
+ VALIDATE
+ PREVIEW
FIELD NAME
FIELD TYPE
PREVIEW
src-ip → IPv4 208.80.154.224
src-port → port 5984
id → Device-Id 4823924721
time → UTC 07:36:38Z
message → Enter Type
Enter Name → Enter Type
CANCEL
SAVE
CLOSE PREVIEW

CREATE MAPPING



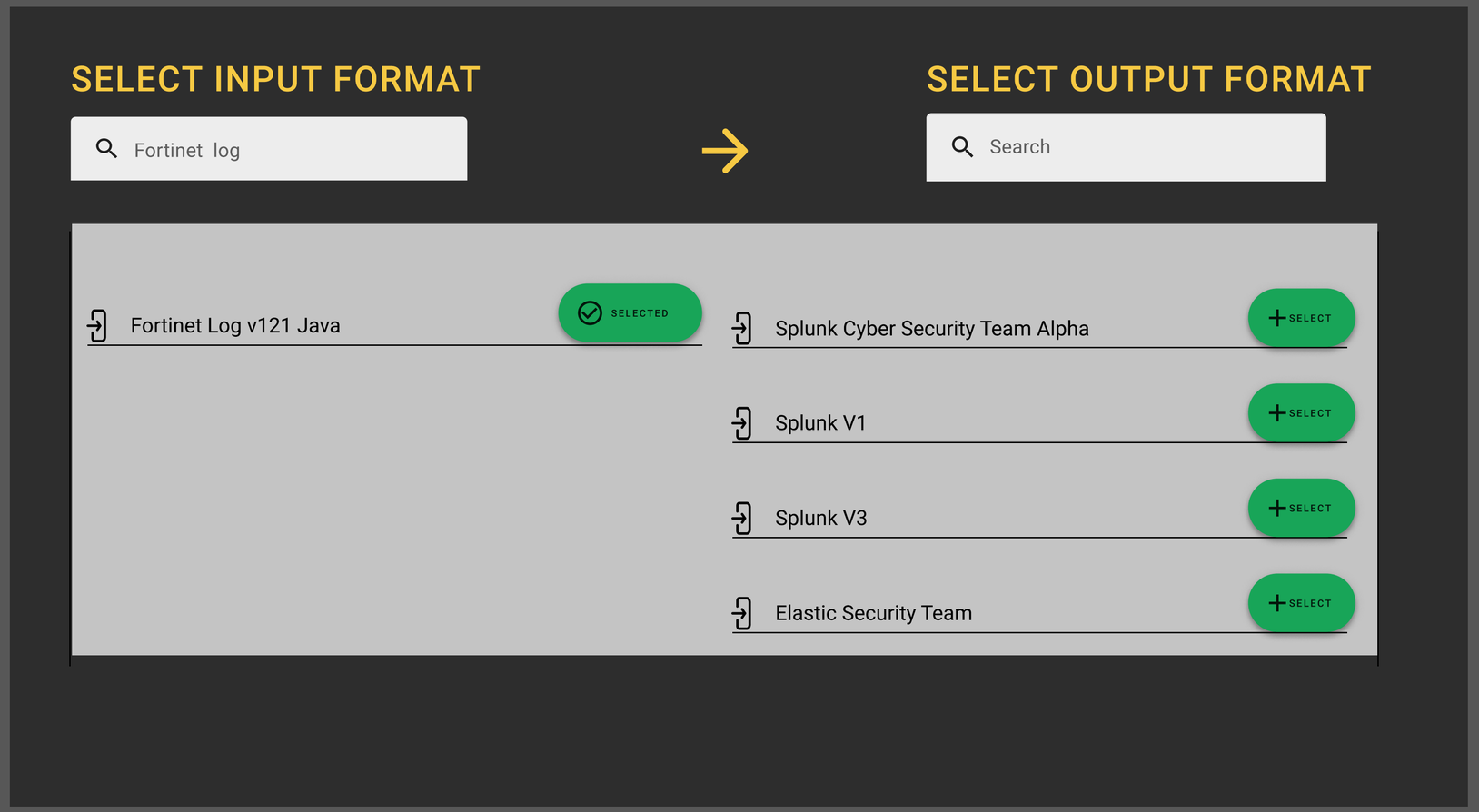
CREATE MAPPING

FORTINET LOG V121 JAVA → SPLUNK V3

INPUT FIELDS		OUTPUT FIELDS
src_ip	→	Source_Destination
srcport (Suggested)	→	Source_Port
	→	Network_Log
	→	Type_Class
logid (Suggested)	→	id
time (Suggested)	→	eventTime

Save

CREATE MAPPING **FORTINET LOG V121 JAVA** →

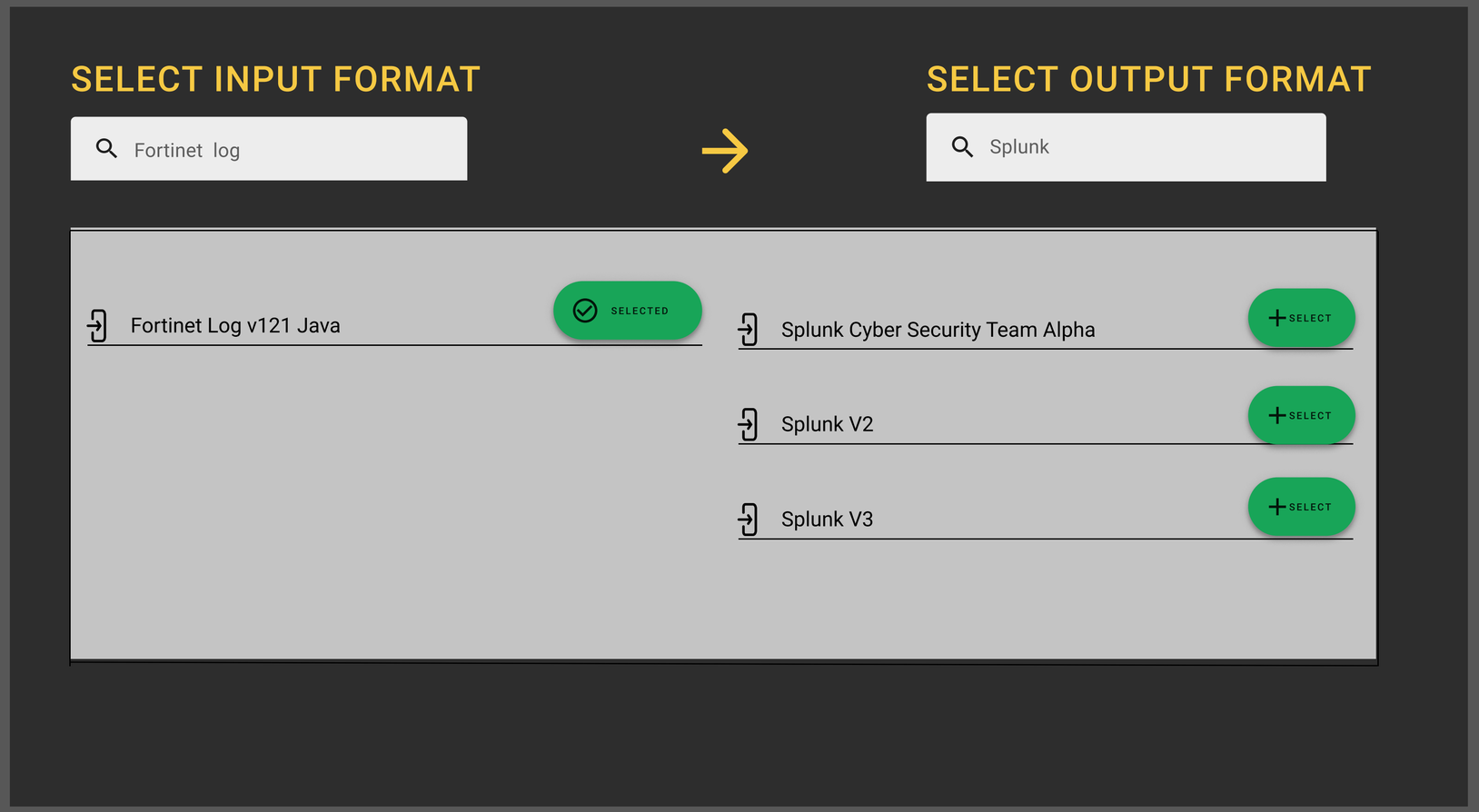


CREATE MAPPING FORTINET LOG V121 JAVA → SPLUNK V3

INPUT FIELDS		OUTPUT FIELDS
src_ip	→	Source_Destination
srcport (Suggested)	→	Source_Port
level	→	Network_Log
	→	Type_Class
logid (Suggested)	→	id
time (Suggested)	→	eventTime

Save

CREATE MAPPING **FORTINET LOG V121 JAVA** →



LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

CREATE MAPPING

FORTINET LOG V121 JAVA → SPLUNK V3

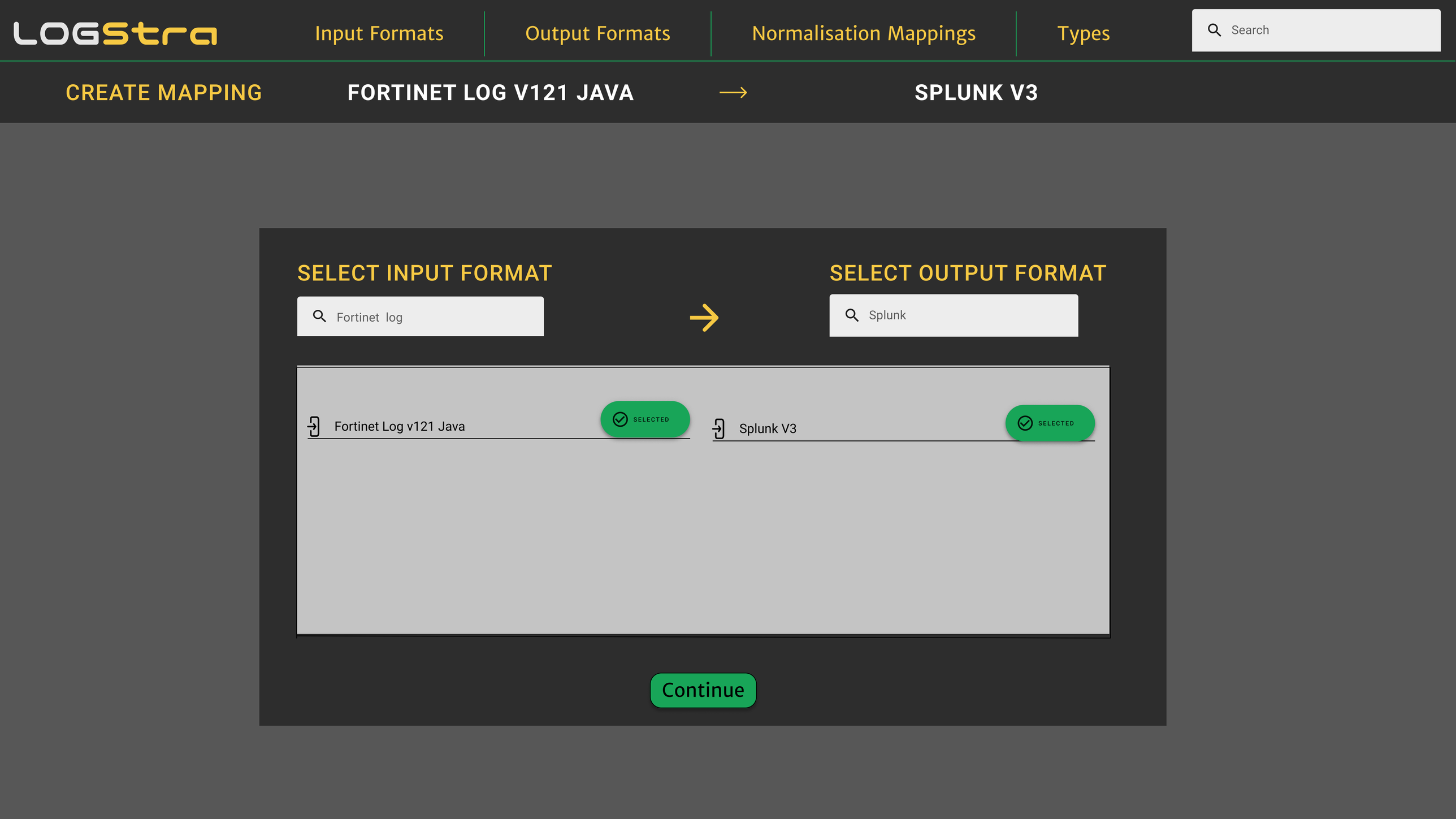
INPUT FIELDS		OUTPUT FIELDS
src_ip	→	Source_Destination
srcport (Suggested)	→	Source_Port
level	→	Network_Log
subtype 1	→	Type_Class
logid (Suggested)	→	id
time (Suggested)	→	eventTime

Save

NORMALISATION MAPPING FORTINET LOG V121 JAVA → SPLUNK V3

SAVE

INPUT FIELDS		OUTPUT FIELDS
srcip	→	Source_Destination
srcport	→	Source_Port
level	→	Network_Log
subtype	→	Type_Class
logid	→	id
time	→	eventTime


LOGStra
Input Formats
Output Formats
Normalisation Mappings
Types
Search
CREATE MAPPING
FORTINET LOG V121 JAVA
SPLUNK V3
SELECT INPUT FORMAT
Fortinet log
SELECT OUTPUT FORMAT
Splunk
Fortinet Log v121 Java
SELECTED
Splunk V3
SELECTED
Continue

NORMALISATION MAPPING FORTINET LOG V121 JAVA → SPLUNK V3

SAVE

INPUT FIELDS		OUTPUT FIELDS
dstip	→	Source_Destination
srcport	→	Source_Port
level	→	Network_Log
subtype	→	Type_Class
logid	→	id
time	→	eventTime