NIST SP 800-53 identification and authentication

You need to monitor user and service identification and authentication mechanisms using zero trust security principles. These actions will help with compliance to NIST SP 800-53 rev5.

Required data

- Data normalized to the following Common Information Model:
  - Authentication

To optimize the searches shown below, you should specify an index and a time range.

Remote authentication activity by geolocation

To see the locations your users or processes are logging in from, run the following search.

```
| tstats count FROM datamodel=Authentication BY Authentication.src
| where (NOT cidrmatch("10.0.0.0/8",Authentication.src)) AND (NOT cidrmatch("172.16.0.0/12",Authentication.src)) AND (NOT cidrmatch("192.168.0.0/16",Authentication.src))
| iplocation Authentication.src
| search (Country!="null")
| geostats sum(count) BY Country globallimit=200
```

Trends in authentication attempts

To see the total number of times the top most frequently authenticating users logged in to your system, run the following search. You can change the limit value to more than 20 if needed.

```
| tstats count FROM datamodel=Authentication WHERE (Authentication.user="*") BY _time Authentication.action Authentication.src Authentication.dest Authentication.user
| where (NOT cidrmatch("10.0.0.0/8",Authentication.src)) AND (NOT cidrmatch("172.16.0.0/12",Authentication.src)) AND (NOT cidrmatch("192.168.0.0/16",Authentication.src))
| eval Time=strftime(_time,"%m/%d/%y %H:%M:%S")
| timechart sum(Attempt) BY User useother=f limit=20
| fillnull value=0
```

Table of authentication activity per user

To see basic data about everyone who has logged into your system, run the following search. You can change the
value to more than 10 seconds if needed.

| tstats count FROM datamodel=Authentication WHERE (Authentication.action="*") AND (Authentication.
user="*") BY _time Authentication.action Authentication.src Authentication.dest Authentication.user span=10s
| where (NOT cidrmatch ("10.0.0.0/8",Authentication.src)) AND (NOT cidrmatch ("172.16.0.0/12",Authentication.
src)) AND (NOT cidrmatch ("192.168.0.0/16",Authentication.src))
| rename Authentication.user AS User Authentication.src AS Source, Authentication.dest AS Destination,
Authentication.action AS "Login Action" count AS Attempts
| eval Time=strftime(_time,"%m/%d/%y %H:%M:%S")
| table Time User, Destination, "Login Action" Attempts
| sort -Time

Next steps

After running these access controls and taking appropriate action, you may want to look into other NIST SP 800-53 rev5 controls:

- Access control
- Audit and accountability
- Identification and authentication
- Incident response
- Risk assessment
- System and information integrity