IDS IPS Monitoring

☆ Edit Export ▾ ...

Allowed Intrusion Attempts

1,629

Blocked Intrusion Attempts

0

Critical Severity Alerts

5

High Severity Alerts

19

Medium Severity Alerts

1,605

Intrusion Signatures

alert.signature	count
ET POLICY RDP connection confirm	9
ET POLICY TLS possible TOR SSL traffic	4
ET POLICY Vulnerable Java Version 1.8.x Detected	12
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection	1547
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection	1
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 127	2
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 222	1
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 279	1
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 322	1
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 358	2
ET TROJAN DNS Reply Sinkhole - Anubis - 195.22.26.192/26	1
ET TROJAN OSX Backdoor Quimitchin DNS Lookup	4
SURICATA TLS invalid handshake message	22
SURICATA TLS invalid record/traffic	22