Ahana System and Solutions

**Ticket ID:2198718**

**Ticket Name: Ahana Firewall Communication From Blacklisted IP**

**Recommended Actions**

**Observation:**

We have observed an alert **" Ahana Firewall Communication From Blacklisted IP ",**

Please find the below details.

**Alert Details:**

Source Address: 162.142.125.222

Destination Address: 192.168.19.59

104.206.128.14 was found in our database!

Confidence of Abuse is 100%

ISP: GDNP LLC

Usage Type: Data Center/Web Hosting/Transit

Hostname(s): 14-128.206.104.serverhubrdns.in-addr.arpa

Domain Name: gdnplus.com

Country: United States of America

City: Las Vegas, Nevada

**Investigation:**

1. We have observed communication from the source address "162.142.125.222" towards destination Address "192.168.19.59" on port "8004", where we are observed device action as "Ahana Firewall" at the time "2022/06/14 06:39:14 UTC".
2. The IP "162.142.125.222" Belongs to the country " United States of America " (ISP: GDNP LLC.) found as BLACKLISTED in AbuseIPDB and previously involved in Brute-force, SSH, Hacking, Web app attack, Portscan, etc

Please find the attached artifacts for your reference.