Name: BlueCat App for splunk
Version: 0.02
Release Date: 02 November 2017
Authors: Muhammad Heidir(mheidir@bluecatnetworks.com), Timothy Noel(tnoel@bluecatnetworks.com)

NOTE
This software is not officially released or supplied by BlueCat Networks

THANKS
To all those involved in the testing and verification.
Albert Sim for supporting this project

CHANGELOG
2/Nov/2017

- v0.2 - Covered most of BlueCat DNS related queries, rpz, rate limit, warning DNS Tunneling setup interface is working and settings are retrieved by python script for detection and mitigation action Dashboard edit has been disabled to avoid tampering End user does not have to meddle with any Splunk configuration Sourcetypes are defined for almost all DNS related syslog messages Preconfigured dashboard based on sourcetypes defined for DNS ALERT is not working at this point in time, not created yet BLOCK is working based on the settings set in the Splunk App Separate tabs for DNS Analytics, Security Threats and Search

28/Sep/2017

- v0.1 - Initial release. Works as it should but with extreme limitation

INSTALL

1. Create an empty Response Policy in BlueCat Address Manager
2. Create a Response Policy Zone under a specified View
3. Add RPZ Deployment Roles for the specified BlueCat DNS/DHCP Server
4. Create an API User Account in BlueCat Address Manager
5. Click on the Server to be deployed, and add a DNS Raw Option
6. Add the following rate-limit statement:

```
rate-limit {
   responses-per-second 5;
   window 5;
};
```

7. Perform Server Deployment to configure BlueCat DNS/DHCP Server
8. [OPTIONAL] - To gain more visibility into DNS Analytics, it recommended to
   (a) Turn on querylogging via CLI
   (b) Login to BlueCat DNS/DHCP Server as "admin"

```
>configure querylogging
>enable
```

9. Launch Splunk
10. Install BlueCat App as you would with any other Splunk App by accessing through

Manage Apps

11. Setup BlueCat App for the first time supplying the following information:
    BAM IP Address:
    BAM API Username:
    BAM API Password:

    Configuration Name:
    Response Policy Name:
    BlueCat DNS/DHCP Server Name:

    Length of Query:
    Number of Count to identify as Tunnel:

    Enable or Disable Alert:
    Enable or Disable automatic Block:

12. Done!

LICENSE

BUG REPORTING

Please email directly to the authors to submit bug report