

Adding short data load to Protect / Risk

| | |
|---------------------------------------------------------------|----------|
| Preparing the PingOne Protect Data Loader | 1 |
| Reference: How do I get brew? | 2 |
| Modifying PingOne Protect Policy To Override Decisions | 2 |
| Appendix 1: PingOne instance variables | 3 |
| Appendix 2: Sample Verbose Run With Bad Actors Enabled | 3 |

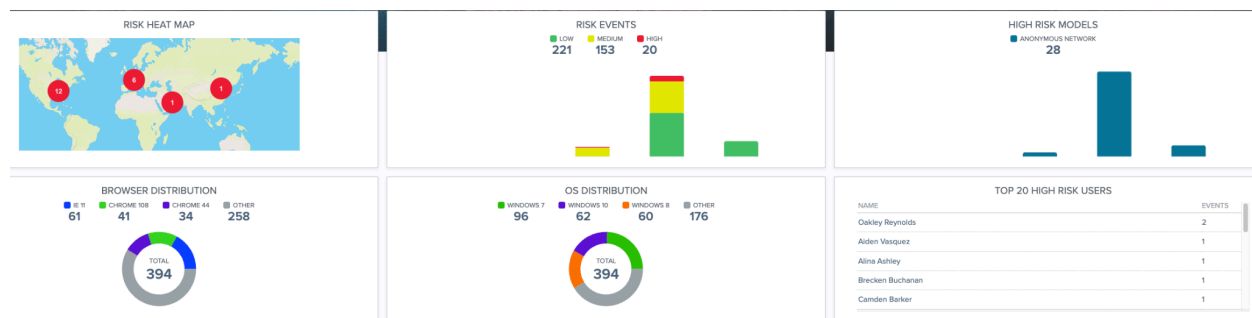
Preparing the PingOne Protect Data Loader

The PingOne Protect Data Loader is available on GIT at:

<https://github.com/malewars/pingone-synthetic-risk-loader>

This is purely for demonstration purposes.

The source file includes a few hundred ip addresses, mail domains, fictitious user applications, and almost all the known Brower agents so we can load a reasonable amount of variety into the PingOne Protect Dash Board to look something like the following:



Step 1: Clone the GIT (<https://github.com/malewars/pingone-synthetic-risk-loader>)

Step 2: Update the variables file; the following values are needed from PingOne:

Worker Client
Worker Client Secret
Environment ID
Risk Policy ID

Also, update the variables with how many samples to load and if Bad Actors should be included.

Example:

myclient="CLIENTID-001"

client_secret="CLIENT-SECRET-0011-1111-1111"

```
RISKPOLICYID="RISKPOLICY-001-001"
ENVID="ENVID-001-0001-001"
BADACTIONS="YES"
RUNS=1
DEBUG="NO"
```

- Step 3: Your local machine needs to have the following installed using Brew or with the OS
- Jot - a command to issue random numbers in a range
 - Python - a working Python 3 with base64, requests, sys (command: **brew update; brew install python3**)
 - Curl - a command to make HTTP requests; suggested to use the one with Brew as the default Mac OS X curl is limited (command: **brew install curl**)
 - Gawk - Installed via Brew (command: **brew install gawk**)
- Step 4: Open a terminal and run the script - Showing below a quiet run, see Appendix for a verbose run output.

Reference: How do I get brew?

Open a terminal window and run this command:

```
/bin/bash -c "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Modifying PingOne Protect Policy To Override Decisions

Open PingOne

Two ways to override loading decisions to distribute load into charts.

- 1) Modify the Weights to force medium and high decisions to be low, medium, or high.
Open Risk Policies > Threat Protection > Risk Policies
Click Pencil to edit the Default Risk Policy
Click Scores : If we need to force low - change High to be 99 and Medium as 98 (be sure to restore values later)
- 2) Add a custom predictor to force decisions
Add new Custom Predictor > Click Threat > Predictor +
Name it Custom > InduceRisk
Attribute: \${event.country}
Fallback: Low
Risk Mapping: List
Low: Add "LabLow"
Medium: Add "LabMed"

High: Add “LabHigh” and click save.

Screenshot:



Open Risk Policies > Threat Protection > Risk Policies

Click Pencil to edit the Default Risk Policy

Add Override Rule:

Click Induce Risk: Score High > Low; Medium > Low




Run a short feed to see if results are now received as Low.



 InduceRisk > Edit 



Attribute Mapping *

Fallback Predictor Decision Value

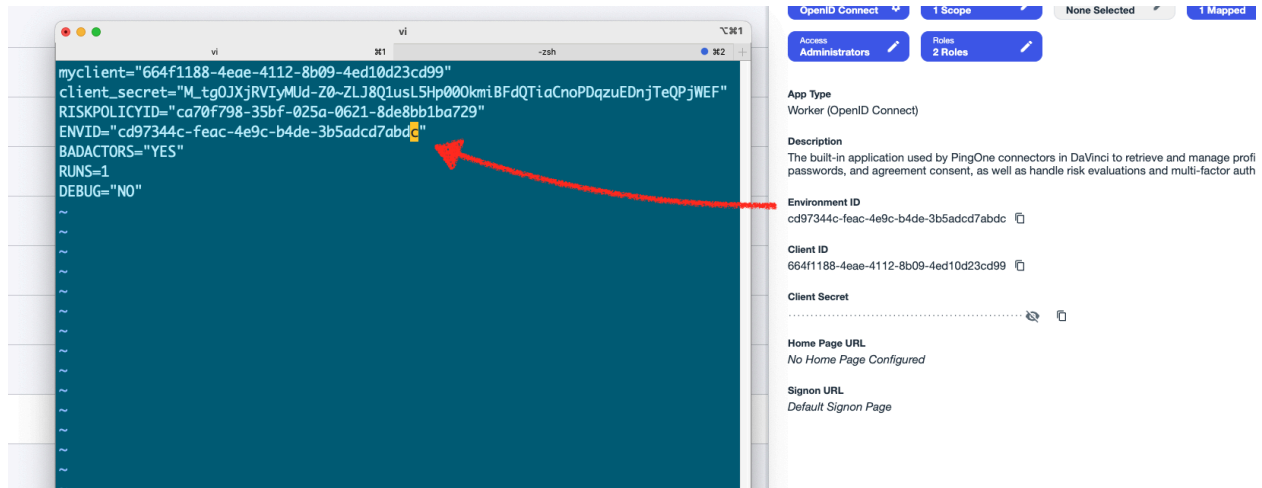
Risk Level Mapping
☐ Range ☐ IP Ranges ☒ List Item

Low 
  
[+ Add List Item](#)

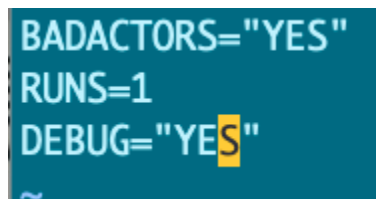
Medium 
 
[+ Add List Item](#)

High 
 
[+ Add List Item](#)

Appendix 1: PingOne instance variables



Appendix 2: Sample Verbose Run With Bad Actors Enabled



./sendrandom.sh

We are loading number 1

Name is Jamir Donovan and source app is Web App Two domain is web.de

Emails is Jamir.Donovan@web.de and Client browser: Mozilla/5.0 (iPad; CPU OS 8_1_2 like

Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B440

Safari/600.1.4 and their ip is 194.72.48.87

--

{

"_links" : {

"self" : {

"href" :

"https://api.pingone.com/v1/environments/cd97344c-feac-4e9c-b4de-3b5adcd7abdc/riskEvaluations/39d64390-11ff-405f-9fd9-0746b03eb275"

},

```
"environment" : {
  "href" : "https://api.pingone.com/v1/environments/cd97344c-feac-4e9c-b4de-3b5adcd7abdc"
},
"event" : {
  "href" :
"https://api.pingone.com/v1/environments/cd97344c-feac-4e9c-b4de-3b5adcd7abdc/riskEvaluati
ons/39d64390-11ff-405f-9fd9-0746b03eb275/event"
}
},
"id" : "39d64390-11ff-405f-9fd9-0746b03eb275",
"environment" : {
  "id" : "cd97344c-feac-4e9c-b4de-3b5adcd7abdc"
},
"createdAt" : "2024-02-14T14:54:10.610Z",
"updatedAt" : "2024-02-14T14:54:10.610Z",
"event" : {
  "completionStatus" : "IN_PROGRESS",
  "targetResource" : {
    "id" : "15fa85c0742a8be144a703f6b14b2888",
    "name" : "RiskMFAScoring"
  },
  "ip" : "194.72.48.87",
  "flow" : {
    "type" : "AUTHENTICATION"
  },
  "session" : {
    "id" : "002b1094-9676-42c3-9f4f-56ef112c6918"
  },
  "user" : {
    "id" : "Jamir.Donovan@web.de",
    "name" : "Jamir Donovan",
    "type" : "EXTERNAL",
    "groups" : [ {
      "name" : "seasonal"
    }, {
      "name" : "yellow"
    } ]
  },
  "sharingType" : "SHARED",
  "browser" : {
    "userAgent" : "Mozilla/5.0 (iPad; CPU OS 8_1_2 like Mac OS X) AppleWebKit/600.1.4
(KHTML, like Gecko) Version/8.0 Mobile/12B440 Safari/600.1.4",
    "webglVendorAndRenderer" : "Intel Inc.~Intel Iris Pro OpenGL Engine",
    "hasLiedLanguages" : false,
```

```
"touchSupport" : [ "0", "false", "false" ],
"timezone" : "New York/US",
"localStorage" : true,
"cpuClass" : "not available",
"hasLiedOs" : false,
"language" : "en",
"indexedDb" : true,
"deviceMemory" : 8,
"hasLiedBrowser" : false,
"platform" : "macOS Sierra",
"hasLiedResolution" : false,
"hardwareConcurrency" : 8,
"addBehaviour" : null,
"availableScreenResolution" : [ 877, 1380 ],
"timezoneOffset" : -5.0,
"fonts" : [ "Arial", "Comic Sans MS", "Courier", "Courier New", "Helvetica" ],
"sessionStorage" : true,
"colorDepth" : 24,
"audio" : "124.04345808873768",
"screenResolution" : [ 900, 1440 ],
"openDatabase" : true,
"adBlock" : false
},
"origin" : "Web App Two"
},
"riskPolicySet" : {
  "id" : "ca70f798-35bf-025a-0621-8de8bb1ba729",
  "name" : "Default Risk Policy"
},
"result" : {
  "level" : "LOW",
  "score" : 0.0,
  "source" : "AGGREGATED_SCORES",
  "type" : "VALUE"
},
"details" : {
  "ipAddressReputation" : {
    "score" : 0,
    "domain" : {
      "asn" : 2856,
      "sld" : "bt",
      "tld" : "net",
      "organization" : "ftip003172872 malvern instruments ltd",
      "isp" : "british telecommunications plc"
```

```
,
  "level" : "LOW"
},
"anonymousNetworkDetected" : false,
"country" : "united kingdom",
"device" : {
  "os" : {
    "name" : "iOS"
  },
  "browser" : {
    "name" : "Mobile Safari"
  }
},
"state" : "worcestershire",
"city" : "malvern",
"impossibleTravel" : false,
"ipVelocityByUser" : {
  "level" : "LOW",
  "threshold" : {
    "source" : "MIN_NOT_REACHED"
  },
  "velocity" : {
    "distinctCount" : 1,
    "during" : 3600
  },
  "type" : "VELOCITY"
},
"userLocationAnomaly" : {
  "reason" : "Not enough information to assess risk score",
  "status" : "IN_TRAINING_PERIOD",
  "type" : "USER_LOCATION_ANOMALY"
},
"userVelocityByIp" : {
  "level" : "LOW",
  "threshold" : {
    "source" : "MIN_NOT_REACHED"
  },
  "velocity" : {
    "distinctCount" : 1,
    "during" : 3600
  },
  "type" : "VELOCITY"
},
"geoVelocity" : {
```

```
"level" : "LOW",
"type" : "GEO_VELOCITY"
},
"newDevice" : {
  "reason" : "This device cannot be identified",
  "status" : "MISSING_DEVICE_IDENTIFIER",
  "type" : "DEVICE"
},
"ipRisk" : {
  "level" : "LOW",
  "type" : "IP_REPUTATION"
},
"userBasedRiskBehavior" : {
  "reason" : "Not enough information to assess risk score",
  "status" : "IN_TRAINING_PERIOD",
  "type" : "USER_RISK_BEHAVIOR"
},
"anonymousNetwork" : {
  "level" : "LOW",
  "type" : "ANONYMOUS_NETWORK"
}
}
}Name is Moses Li and source app is Risk Test App domain is mail.ru
Emails is Moses.Li@mail.ru and Client browser: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36 and their ip is
220.125.91.208
```