Infoblox

Best Practices for Combination Feeds

Combination Feeds. Infoblox has a large and robust offering of threat intelligence feeds, which allow users to tailor their security to their individual needs. The large number of options may be somewhat overwhelming for some customers. In an effort to simplify the process for these users, Infoblox created “combination feeds” to group sets of threat intelligence feeds in order to reduce the number of choices and make the process more intuitive. As no two users have the same requirements, we narrowed these selections to a small number of “sets" of intelligence feeds. Which set to choose depends on the sensitivity your environment has to protection of potential threats as compared to the sensitivity your environment has to blocking potentially benign sites.

Aside from simplifying the choice from 20+ individual feeds to a single set, there are other benefits to these feeds as well. These feeds will continue to be curated over time. As new feeds that qualify for inclusion are introduced, these new classes of indicators will be added automatically and not require a major change to your policy rules. Similarly, as some feeds are deprecated, they can be removed from the combination feed automatically, also not requiring maintenance of your policy rules. As these feeds are enhanced and maintained, users will be updated to know any substantive changes to their contents.

Infoblox provides four sets of combination feeds:

- “**Low**” blocks the fewest number of threats but also minimizes the potential of blocking benign sites. Examples of these environments may be universities, service providers and public wifi access points.
- “**Medium**” is an ideal balance between detection while minimizing the potential for positives. We designed the “Medium” set to be appropriate for most enterprise organizations. If you are unsure which set to use, “Medium” is probably the best fit for your organization
- “**High**” was designed for environments where security is the most important factor. These feeds are most appropriate for environments where communication is well understood and security of the devices is critical. Examples of environments where “High” is most appropriate include server farms, networks with IoT devices or Point-of-Sale terminals. It is inappropriate for networks where users typically surf the web or check their email
- **“Extreme”** was created to provide the greatest degree of security, but these sets are not recommended for most users as the potential for positives is much higher than normal. Use this feed at your own risk.

Each set includes two separate feeds, which should be deployed together and without any other set:

- **Block** - This file should be deployed with the policy action of “Block” and should be one of the first actions in the policy list, possibly following a global allow list.
- **Log -** This file should be deployed with the policy action of “Allow” (preferably with log) and should be one of the last actions in the policy list.

© Infoblox Inc. All rights reserved |

For example, this is what a minimal policy should look like if the “Medium” set best describes your organization

Order	Object	Action
1	Custom List: Global Allow List	Allow - No log
2	RPZ: ib-med-block	Block - Default Redirect
3	RPZ: ib-med-log	Allow - with Log

Table 1: Example organization of policy flow

Contents of Combination Feeds Combination feeds, as the name would suggest, are combinations of other existing feeds. If you deploy either the Low, Medium, High or Extreme combination feed set, these feeds are already combinations of one or more of the following existing feeds:

- AntiMalware
- AntiMalware_IP
- Base Hostnames
- Bogon
- Cryptocurrency hostnames and domains
- DoH Public Hostnames
- DoH Public IPs
- Exploit Kit IPs
- Extended Base & anti-malware Hostnames
- Extended Exploit Kits IPs
- Extended malware IPs
- Extended Ransomware IPs
- Extended TOR Exit Node IPs
- Malware DGA hostnames
- Malware IPs
- Ransomware
- SURBL Fresh domains
- SURBL Multi domains
- SURBL Multi Lite domains
- TOR Exit Node IPs

Table 2: Threat Feeds used by Combination Feeds

© Infoblox Inc. All rights reserved | End of Support, CDC-Based Threat Insight

This means that if you use one of the combination feed sets, you should not:

A. Use it in combination with any other set. In other words, do not deploy Low and Medium or High together. Each is completely self contained, and deploying them together will almost certainly not provide the results you are looking for.
B. Use it in combination with any of the other above feeds, as these feeds are already reelected in the contents of the combination feed, so deploying them together will at minimum cause your NIOS appliance to expend more resources than necessary, and may also result in undesired actions if there are conflicting policies.

Best Practice Summary

1. Choose the set of feeds that best describes your organization: Low, Medium or High. If in doubt, most organizations are best served with Medium.
2. Deploy the set of feeds together. For example, if "**Medium**" best describes your organization, deploy both *ib-med-block* and *ib-med-log* together.
3. Do not deploy a set of threat intelligence with any other set. In other words, do not deploy Medium together with High. Choose one set, and deploy them together and without any other set.
4. Do not deploy a set with any feeds listed in ***Table 2***. These feeds are already reflected in the combination feeds, so using them together may cause duplication, redundancy or potentially conflict.
5. Deploy blocking feeds as close to the first policy action as possible (potentially after a global allow list).
6. Deploy logging feeds after all blocking feeds so as to not accidentally allow an indicator that another feed wanted to block

What to do if you have already deployed a combination feed?

If you have already deployed a combination feed, please review the best practices recommendation above and try to make sure that you have followed the guidelines described above. Specifically:

- If you have deployed two or more sets of combination feeds, **remove the lower sets** as these are already reflected in the higher sets. For example, if you have deployed all three (Low, Medium and High), remove Low and Medium because the indicators in these sets are already reflected in High.
- If you have deployed one of the sets along with any of the feeds reflected in Table 2, **remove those feeds** from the policy actions list as they are already reflected in your selected policy group.

© Infoblox Inc. All rights reserved | End of Support, CDC-Based Threat Insight

Supplemental #1: The following shows the current contents of each of the combination feeds.

Feeds	Extreme Block	Extreme Log	High Block	High Log	Med Block	Med Log	Low Block	Low Log
AntiMalware	✔		✔			✔		✔
AntiMalware_IP	✔		✔			✔		
Base Hostnames	✔		✔		✔		✔	
Bogon	✔		✔		✔			✔
Cryptocurrency hostnames and domains	✔		✔			✔		✔
DoH Public Hostnames	✔		✔			✔		✔
DoH Public IPs		✔		✔		✔	✔	✔
Extended Base & anti-malware Hostnames	✔		✔		✔		✔	
Extended malware IPs	✔			✔		✔		✔
Extended Ransomware IPs	✔			✔		✔		✔
Extended TOR Exit Node IPs	✔		✔			✔		✔
Malware DGA hostnames	✔		✔		✔		✔	
Malware IPs	✔			✔		✔		✔
Ransomware	✔		✔		✔		✔	

© Infoblox Inc. All rights reserved |