Bandura Cyber GMC Release Notes

This document provides release notes for the Bandura Cyber Global Management Center (GMC).

The complete GMC User Manual can be retrieved from the Bandura Cyber Support Center, located here: <u>https://helpdesk.banduracyber.com/hc/en-us</u>.

RELEASE NOTES

Release: GMC Builds 62-66, July 2021

New Features:

Cyber Intelligence Marketplace

Cyber Intelligence Marketplace provides Bandura customers with even greater access to high-value multi-source cyber intelligence data from leading intelligence providers. Our Marketplace includes cyber intelligence from long-time partners, premium offerings from new partners, and an expanded partnership with DomainTools.

To access the Cyber Intelligence Marketplace in GMC, select Marketplace from the left-hand navigation menu. All available offerings will display:

🖶 BANDURA				Q @ 4 @ •
Dashboard >				
Policies				
🛱 Marketplace NEWL	BANESK Well-Fed Threat Intelligence	>	CYAX Cyjax Threat Intelligence Feed	8
Exception Lists			×4	0
▲ Threat Lists >		CINTEL471 Intel 471 Malv	CINTEL471 Intel 471 Malware Feed	ire Feed >
○ Denied Lists >	Patrol Malware Patrol Threat Intelligence Enterprise Feed	>	Ralware Malware Patrol Threat Intelligence Essentials Feed	>
Allowed Lists >		6		
◎ REACT >	proofpoint, Emerging Threats Intelligence Feeds	>		
Risk Adjustments >				

Out-of-the-box offerings, like DomainTools, are free to customers and display on this screen with no icon in the top-right corner. Premium offerings include a "\$" in the top-right corner of the listing.



To subscribe to an out-of-the-box feed:

- 1. Select the desired listing
- 2. Select the Subscribe button

🖶 BANDURA			Q @ 4 8 •
Dashboard >	Cyber Intelligence Marketplace		DOMAINTOOLS
⑦ Policies			
🛱 Marketplace 📊	The cost to add the DomainTools feed to your	DomainTools	
Exception Lists	subscription is:	Description	
▲ Threat Lists >	FREE!	boonprion	
○ Denied Lists >	Subscribe	One of the critical challenges for network defenders is identifying domains most likely to pose a threat at any giver their blocking and detection efforts. The Domain Hotlist consists of domains that have a DomainTools Risk Score o	n time, so that organizations can focus f 99 and higher. These domains are
Allowed Lists		both highly risky and currently active; in other words, operational. This list gives customers a relatively small, easy that they can use to track, monitor, and alert on active malicious domains on their network.	-to-manage, focused set of domains
		The Domain Hotlist provides protection from phishing, malware, and spam threats based on DomainTools Risk Sco	re machine learning classifiers and
▲ Risk Adjustments →		typically contains over 10 million malicious domains.	

3. Select the Enroll button



To subscribe to a premium feed:

- 1. Select the desired listing
- 2. Select the Purchase button

		Q @ 4	8 ~
Dashboard >	📜 Cyber Intelligence Mark	etplace	ware ol
⑦ Policies			
📜 Marketplace 📢	The cost to add the Malware Patrol Enterprise feed to your subscription is:	Malware Patrol Enterprise	
Exception Lists		Description	
A Threat Lists →	\$ PRICE	Description	
\odot Denied Lists \rightarrow	Purchase	Malware Patrol specializes in real-time threat intelligence that protects users and enterprises in over 175 countries against cyber attacks. The highly refined and continuously updated indicators identify compromised machines, botnets, command and control (C2) servers, phishing sites,	
\oplus Allowed Lists \rightarrow		malware/ransomware infections and other threats.	
• REACT >		Collecting and analyzing IoCs since 2005, Malware Patrol has developed an extensive network of global sensors, along with other proprietary data collection and identification mechanisms. Both automated and human analysis processes are used to verify and prioritize the data. The result is a vast	st
🛆 Risk Adjustments 🔿		database of unique and historically rich - "intelligent" - threat data.	
榕 Users		Malware Patrol's automated systems verify each indicator daily to ensure that its feeds contain only high confidence data. Feeds are updated hourly with newly found threats. Use these feeds to increase your visibility of active threats and to block malicious and unwanted traffic to/from your network.	rk.
😑 Command Logs		Malware Patrol has two subscription offerings available on the Bandura Threat Intelligence Data Marketolace.	
🙏 Assets			
□ Software →		Malware Patrol Essentials is an IPv4 Denied List that includes IPs associated with malware, ransomware, C2 servers, and Domain Generation Algorithm (DGA) infrastructure.	m
-b; System >		Malware Patrol Enterprise is both an IPv4 and Domain Denied List and includes an expanded set of indicators. The Malware Patrol Enterprise feed includes IP and domain indicators associated with malware, ransomware, C2 servers, DGA infrastructure, phishing, DNS over HTTPs (DOH) resolvers, and Tor exit nodes. The domain feed also includes domains associated with cryptominers.	,

- 3. On the Purchase modal, the following will display:
 - a. Annual Subscription Cost the one-year cost of the subscription, based on your account's total ThreatBlockr throughput
 - b. Pro-rated Amount the amount to be paid, based on your account's total ThreatBlockr throughput and the end date of your ThreatBlockr subscription(s)
 - c. Due Now the amount the account will be invoiced at the time of purchase
- 4. Select the hyperlink at the bottom of the modal to review the Terms and Conditions of the feed
- 5. Select the checkbox to verify you have read and agree to the Terms and Conditions
- 6. Select the Purchase button

📜 Marketplace Purchase	×				
Malware Patrol Enterprise Premium Feed Patrol					
PRICE					
Annual Subscription Cost \$ Annual					
Pro-rated amount to match your current ThreatBlockr subscription of 2 Gbps throughput with an end date of May 04, 2024	\$ Pro-rated				
Due Now	\$ Due Now				
PAYMENT					
Your account will be invoiced, based on the subscription term and amount shown above.					
I have read and agree to the Terms and Conditions	Cancel Purchase				

A modal will display providing further details about the subscription.



After successfully subscribing to a Marketplace offering, a blue check mark will display in the right corner of the listing on the main Marketplace page:

