Bandura Cyber ThreatBlockr 2.0 Cumulative Release Notes

ThreatBlockr 2.0 is still the same core software as TIG OS 2.0. We're simply giving our devices and their control software a new name: ThreatBlockr (yes, without the 'e'). The new appliance naming makes it easier for us to talk about what we do. And what is it that we do? We block threats at scale, with consistent latency all the way to line rates irrespective of packet size and irrespective of the number of threat indicators employed.

Bandura Cyber ThreatBlockr 2.0 (previously named TIG OS version 2.0)

This document provides cumulative release notes and upgrade path information for the Bandura Cyber ThreatBlockr 2.0.

Upgrade Requirements

The table below lists the Bandura Cyber hardware part numbers that are compatible with ThreatBlockr 2.0 software, as tested with build 32 and later. Each of these can end in C (copper), F (standard reach multi-mode fiber), or S (long reach single-mode fiber):

Bandura Cyber Part Number
Lanner PW-ESE-BS1-05
Supermicro PW-ESE-ES1-05
Dell PW-ESE-MS1-04
Intel PW-ESE-XS2-01 * certain models only - consult Bandura Cyber Support
Dell PW-ESE-XS2-02
Dell PW-ESE-XS2-03
Dell PW-ESE-XS2-04
Dell PW-ESE-XS2-05
Dell PW-ESE-ZS2-04
Dell PW-ESE-ZS2-05

NOTE: Upgrading compatible hardware from TIG OS to ThreatBlockr 2.0 will require a physical reimaging of the device. Due to hardware requirements, some legacy Bandura Cyber devices will not support ThreatBlockr 2.0. If you are currently running a legacy version and would like to upgrade to ThreatBlockr 2.0, please contact support@banduracyber.com or your sales representative to determine upgrade options for your device.

For upgradeable devices, please note that *it is not possible to remotely upgrade from TIG OS to ThreatBlockr 2.0 via remote software download*. For compatible devices, users will need to physically upgrade their devices

onsite via a USB installation process. To initiate this process, please contact Bandura Cyber support or your sales representative, listed below.

Documentation

For more information see the ThreatBlockr User Manual, located in the Bandura Support Center, located here: https://helpdesk.banduracyber.com/hc/en-us

If you have any questions about these updates, would like to initiate the upgrade path for your compatible legacy device, or have questions regarding your legacy device, please contact the Bandura Support team at **support@banduracyber.com** or by calling +**1-855-765-4925**.

RELEASE NOTES

Release: ThreatBlockr 2.0 Build 75

File Date: 4 March 2021

Purpose of the Release

This release is an important update that adds new features while fixing several defects. Some of the defects were discovered by customers - you know who you are, and we thank you!

Important security updates are included in this release, including remediation for the highly publicized Linux vulnerability CVE-2021-3165, as well as a new set of updates to DPDK. There was also a **critical** fix in our own software stack this release, relating to an out-of-bounds condition on ASN indexes which was exacerbated after February 19, 2021 with new ASN mappings that came online. **This is critical - devices without this fix will continue to use the ASN and country registration information as of February 19, 2021, and will not be able to receive updated ASN information from our central GMC management platform until this software release is installed. As such, we urge all of our customers in the strongest of terms to upgrade to this release as soon as possible.**

New and Improved

- **New 'Description' Field for Syslog Export Configurations (DEV-1449)**
  - Our customers that use our syslog export capability (and if you're not, you should!) may or not be aware that you can export the logs to as many external sources as you'd like. When you've got more than one, it can be difficult to know which is which. To improve the user experience, you can now add an optional free-form text description to your syslog export configurations, so that you can more easily identify what you're connecting to at a quick glance.
- **Dell+Silicom Hardware Now Support Hardcoded Speed and Duplex Settings (DEV-1776)**
  - We now support software-configurable hardcoding of speed and duplex for our Dell server + Silicom card solutions. This can be a useful workaround for customers with very old networking or firewall equipment that don't support auto-negotiation standards.

    - No, this feature is not available on our lower-end equipment, due to hardware limitations on the lower-end equipment. For those devices, auto-negotiation is typically required.
- **Completion of Certificate Management Subsystems for UI Security (DEV-1939, DEV-2061)**
    - We had never finished the certificate management subsystem, which meant that customers had to utilize browser features to accept security exceptions in order to connect to the device UI 'securely'. We have now completed this work, and we believe it now has comprehensive support for importing a certificate created from a certificate signing request (CSR), plus also support for full PKCS12 certificate chains, including intermediate certificates.
    - This means that customers that want to sign access to their devices with a recognized CA should now be able to do so.
- **Using a Common Access Dialog Framework in the Device UI (DEV-2011)**
    - We consolidated some of our access dialog stuff in the device UI for a more consistent user experience across the various views.
- **Intelligent Policy Assignment for Resource Group Imports (DEV-2065)**
    - When importing resource groups, we now check to see if a matching policy exists in GMC, and if we find one, we automatically apply it. This is a fantastic time-saver when importing information during device configuration.
- **Reduction in Download Image Sizes (DEV-2068)**
    - We underwent a series of internal build system optimizations and in so doing were able to greatly reduce the total size of our download images, both for on-premise and cloud deployments. This will result in more rapid system updates.
- **Cloud Deployment Assistance (DEV-2070)**
    - We added some extra error checking when logging in to a ThreatBlockr Cloud deployment to make sure the system was spun up properly. If we detect an anomaly, we point the user at our comprehensive cloud deployment documentation so that they can address any issues in their AWS environment to ensure a proper deployment architecture. For reference, our cloud deployment documentation is fully available to the public, and can be found at the following link in AWS S3:
    - https://threatblockr-marketplace.s3.amazonaws.com/Bandura+Cyber+ThreatBlockr+Cloud+in+AWS.pdf
- **DPDK 19.11.6 LTS (DEV-2072)**
    - We now ship with DPDK 19.11.6 LTS, which includes recent performance improvements and fixes for DPDK.
- **New Domain Resolution Logs Export (DEV-2085)**
    - By popular demand, we have an **exciting new log export** now that contains DNS resolution details for A and CNAME responses! There is no device UI view for this - it is only available if you export the logs via our RFC-compliant syslog export mechanism after updating your device configuration's *Logging* > *External Syslog* configuration appropriately. Additionally, we've updated our comprehensive syslog export documentation with detailed formatting for this feature, which you can get from our Customer Success site or by contacting our Customer Success team.
    - The new exported detail can be very useful information to assist with detailed logs analysis and correlation with other available details, such as when exporting our

detailed logs to powerful external SIEM tools, or even simple ultra-low-cost syslog-ng sinks where you're simply storing the data for analysis downstream as simple text files (which is what we do ourselves!).

- **Internal Improvements to Better Track Feed Synchronization (DEV-2087)**
    - We've been blind to some recent feed synchronization issues (often resulting from customer-side networking considerations), and these improvements will help our Success team when working with customers to troubleshoot such issues.
- **Add More Info to the System Information UI Panel (DEV-2093, DEV-2102, DEV-2108, DEV-2113)**
    - When available, we now include the system uptime and certain serial number information in the System Information panel in the device UI.
- **Improve Audit Logs Relating to License Removals and Additions (DEV-2094)**
    - We now have customers contemplating moving infrastructure to the AWS cloud, and we support the ability of a customer to remove a license from one unit and attach it to another. However, we weren't being very verbose about this in the Audit Logs, which was causing some confusion, and so we've extended the Audit Logs to have more meaningful information included when license swapping is undertaken.

Defect Fix Description(s)

- **A 'bus error' Caused by Use of a Domain Name in Syslog Export Configs (DEV-1961)**
    - A 'bus error' message is kind of a catch-all error message in some system components, and we had a customer run into one. We tracked it down to the use of a domain name in a syslog export configuration, which wasn't properly supported. We have updated the configuration handlers to properly support the use of DNS names in the syslog export configuration, so customers that would prefer to use them instead of numeric IPs can do so now.
- **A 422 Error is Reported in the SNMP Dialog (DEV-2010)**
    - We fixed this minor error. Note that the internal error was an extra PUT operation after a POST, where the PUT caused the 422, but the desired operation actually succeeded.
- **Missing Risk Threshold Categories on Device-Side UI Display (DEV-2031)**
    - The device UI was missing recently added Risk Threshold categories. This is now fixed.
- **Importing a Configuration Block Doesn't Show Up in the Audit Log (DEV-2071)**
    - When assisting a customer with an upgrade, we noticed that importing a configuration didn't get audited properly in our logs. We've fixed this.
- **Minor Internal Fixes (DEV-2077)**
    - We fixed a few other internal non-customer impacting things in this cycle as well, such as some internal marketing-related naming changes in some of our cloud-based stuff.
- **Source and Destination Port Information Now Appear in our Domain Logs (DEV-2084)**
    - In our ongoing efforts to make our exportable device logs (via our Syslog Export features) better and better, we have added source port and destination port information to our Domain Logs.
- **Warning/Error Banner Fixes in the Device UI (DEV-2089, DEV-2095)**
    - At the top of the device UI we embed a small banner area where we can display warning/error messages that may be meaningful to the user, such as when there is a device licensing problem or when GMC connectivity is sporadic. There were a set of

defects relating to the timely display (and clearing) of such information that we have now addressed.

- **Double Quotes in ASN Names (DEV-2091)**
  - We've stripped double quotes appearing in ASN names. Our system handles this condition properly, but it could cause problems in downstream systems attempting to parse the syslog export data. We noticed a nefarious Ukrainian service attempting to use this scheme, which could conceivably be used as an attack vector against poorly constructed syslog parsers in use in various SIEM or SIEM-like tools.
- **Loose State Handling (LSH) Algorithm Collision (DEV-2096)**
  - We've revamped our loose state handling algorithms to be more deterministic. There was an edge case where a non-deterministic decision could have resulted when resource group matches occurred which has been addressed. Additionally, we are now applying LSH algorithms only to TCP traffic. For UDP traffic, packet direction trumps in LSH determination.
- **Internal Routines Now Requery License Settings (DEV-2097)**
  - A license migration error, most often seen when performing a legacy device upgrade to our newest software, could have caused some internal processes to use the wrong license. We have been internally working around this problem manually in our production database. This is now fixed.
- **Mitigate CVE-2021-3156 (DEV-2105)**
  - **Because of the critical nature of this defect in the underlying Linux architecture, we recommend, in the strongest possible terms, that customers upgrade immediately to this build.** CVE-2021-3156 is a critical defect that impacts most worldwide infrastructure leveraging open source Linux over the past decade. The defect was a least-privilege escalation bug with a standard variant of the popular sudo tool, which ships as a stock part of most Linux distributions, including Ubuntu 18.04 LTS Server which our system is currently based on. On an impacted Linux system, this defect would allow any logged in shell user to potentially gain root access. We have fixed the defect - as has most of the world at this point, if they're smart. If you have other Linux-based systems in your infrastructure, we strongly recommend that you update them (and/or work with your vendors to do so) as soon as humanly possible.
- **Domain Lookups for Block and Allow Determination Should be Case-Insensitive (DEV-2109)**
  - **Because of the critical nature of this defect, which we have discovered exists in all previously released versions of our software, we STRONGLY advise all customers to update immediately.**
  - We found that a malicious actor could conceivably bypass our domain protection by using mixed-case domain names. We have corrected this, and now all domain name checks are properly performed in case-insensitive fashion.
- **NTP Servers Not Being Recognized (DEV-2111)**
  - Build 68 introduced a defect where configured NTP servers were being ignored. This is now fixed. Please note that you may see a pair of 'red' error-level messages relating to the ntpd system daemon show up in the internal system logs early in the startup sequence on first-boot after installing this release. That is normal, and they can be safely ignored.

- **Metadata Healthcheck Information Timestamps Incorrect (DEV-2112)**
    - The metadata health check information that is occasionally sent back to our centralized GMC platform was being timestamped as local timezone, but should have been UTC. It is now UTC as required by our backend metadata logic.
- **Internal Process Cleanup Fixes (DEV-2114)**
    - As part of an internal review, we identified a few processes that were not cleanly exiting on various abort conditions. These are now fixed, and standardized.
- **Miscellaneous Internal Fixes (DEV-2115, DEV-2116, DEV-2120, DEV-2124, DEV-2126, DEV-2128, DEV-2129)**
    - Various internal, non-customer impacting fixes were made. This included serial number propagation, multiple startup failure logging fixes/improvements, internal hanging transaction cleaning, internal build system modifications, and some minor systemd follow-up work stemming from our previous Build 68 release.
- **Extension Support for License Expiration (DEV-2117)**
    - An internal ordering problem which precluded license extensions from working is now fixed. A workaround did exist for this problem, but involved a system reboot. Once this code is installed, that workaround is no longer required for a license to be extended after expiration occurs.
- **Deleting a Resource Group Displaying Incorrect Error Messages (DEV-2118)**
    - An issue with resource group deletion on the device that could have resulted in erroneous error messages being generated was fixed. However, even though the messages could be displayed, the resource group was still correctly removed.
- **Extend the Total Number of Supported ASNs (DEV-2130, DEV-2132)**
    - The internal device ASN limits were reached, and we have extended them in this release. **This is critical - devices without this fix will continue to use the ASN and country registration information as of February 19, 2021, and will not be able to receive updated ASN information from our central GMC management platform until this software release is installed. As such, we urge all of our customers in the strongest of terms to upgrade to this release as soon as possible.**

Release: ThreatBlockr 2.0 Build 68

File Date: 23 December 2020

Purpose of the Release

This release is an important update that adds new features while fixing several defects. Some of the defects were discovered by customers - you know who you are, and we thank you! Critical new additions in this release include the migration from Python 2 to Python 3, as well as the migration from DPDK 18.11 to 19.11. Because of these important changes, **we strongly recommend that all customers upgrade to this release as soon as possible**. We say that because community support for Python 2 is drying up, which means that unpatched Python 2 and related library security holes become a real concern over time. Similarly, community support for DPDK 18.11 has ended, with long term support guidance now attached to DPDK 19.11.

New and Improved

- **Support our new Dual Rate (1G and 10G) Capable Hardware Coming in 2021 (DEV-1937, DEV-2024)**
    - We'll soon be shipping new hardware that will be able to be configured in software for either 1G or 10G operation. This will provide a nice software upgrade path for current 1G customers when they need to migrate to 10G downstream, without requiring hardware upgrades, as long as the medium choice (copper or fiber) is consistent.
- **Internal Logs Wrap Predictions (DEV-1966)**
    - A message is now displayed on our internal logs screen(s) that gives the user an idea of how long it will take the internal logs to wrap given recent usage patterns. We also note the importance of using our RFC-compliant syslog export feature for long term logs storage.
- **DPDK 19.11.5 LTS (DEV-2041)**
    - We now ship with DPDK 19.11.5 LTS, which includes recent improvements and fixes for DPDK. Note that the prior LTS version of DPDK, 18.11.8, is no longer under active support by the community, **so we consider it imperative to upgrade to this release to ensure timely support for any future DPDK security fixes and performance improvements.**
- **Python 2 to Python 3 Migration (DEV-1825)**
    - This was a critical change that was needed given that Python 2 is now, for all intents and purposes, a dead language, and the community support for it is rapidly drying up. We have therefore migrated all internal subsystems that utilized Python 2 to Python 3. Because of this, **we strongly recommend that all customers upgrade to this release as soon as possible.** We say that because community support for Python 2 is drying up, which means that unpatched Python 2 and related library security holes become a real concern over time.
- **Ability to Move Licenses (DEV-2039)**
    - This is a key new feature that allows users to more easily move licenses between systems. This has a variety of uses, but the main use case driver was for customers with on-premise ThreatBlockr 2.0 devices that are migrating infrastructure to the cloud. This feature now allows them to seamlessly turn down service for one of their on-premise devices and transfer the license for use at another location, to include the cloud.
- **ThreatBlockr Cloud on AWS Feature Merges (Various)**
    - This release, and all subsequent releases, marry our cloud and on-premise technology, which means that the same build versions can be applied to both your on-premise ThreatBlockr 2.0 devices as well as any ThreatBlockr Cloud installations that you've deployed in AWS.
        - Our current ThreatBlockr Cloud and associated ThreatBlockr Anywhere offerings exclusively deploy via AWS Marketplace with a bring-your-own-license (BYOL) model, allowing you to protect your AWS-native cloud infrastructure with the same ThreatBlockr technology that our customers rely on for their on-premise infrastructure.
        - For questions about deploying us on AWS, please contact our Customer

Success team.
    - In 2021, we'll be rolling out support for Microsoft Azure and Google Cloud Platform. Our current projections have us finishing up this work no later than the end of June 2021.
- **Other minor internal improvements (DEV-1828, DEV-2000, DEV-2040)**
    - A variety of minor internal improvements were also made. These included:
        - some internal database logging changes for more efficient troubleshooting,
        - a migration to systemd for improved system bring-up and management, and,
        - an increase to our threat intelligence filter sizes.

Defect Fix Description(s)

- **Updated Bypass Control for Lanner Set-Top Boxes (DEV-1797)**
    - We have updated the control software that we use for bypass control, and are now operating it as a kernel module to eliminate any possibility of bypass driver contention. We had not explicitly seen any directly attributable adverse effects in the wild, but this was a prudent change made out of an abundance of caution.
- **Domain Log Searches Failing When Using IP Source or Destination Filters (DEV-2062)**
    - We've fixed a problem with domain log searches in our internal logs. Prior to this fix, using the IP source or destination filters when searching the domain logs would produce incorrect results. This has been fixed. A big "Thank You!" goes out to the customer that identified this problem for us.
- **Configuration Import Defects (DEV-2063, DEV-2064, DEV-2067)**
    - There were three defects identified by one of our customers that were found when they were attempting to export and re-import device configuration data:
        - First, resource imports were not properly considering resource direction which caused an invalid error message to be generated.
        - Second, the 'check all' import box wasn't working properly. There was a workaround to manually check each box individually, but with this fix the 'check all' function works as intended.
        - Third, imported service groups were erroneously reported as being managed by GMC, which is not yet possible (although that is a feature we'll be working on in 2021). Both of these have been fixed and we thank the customer who identified them for pointing them out to us!
- **Special Characters Precluded Default ASN Data From Loading Properly (DEV-2069)**
    - This was a minor issue that we discovered internally when doing some routine testing. When a device is first installed (typically at one of our box-build partners), prior to being configured for connection to GMC, there is a default ASN list that exists in the installation. That list was not loading properly due to special character handling. This has now been fixed. Note that this defect is not believed to impact any customer, since once customers are properly bolted to GMC, the GMC-provided lists override the default lists, and the GMC lists do not exhibit this issue.
- **Automatic Software Update Could Result in a Defunct Process (DEV-2073)**
    - This is a minor internal issue, but we noticed the possibility of a defunct process resulting from the automated software update mechanism. This is now fixed.
- **Integer Math Overflow Error (DEV-2075)**

- We fixed an internal logs wrap prediction messaging problem relating to an integer overflow math defect that could cause a UI error message to pop up.

Release: ThreatBlockr 2.0 Build 59

File Date: 3 December 2020

Purpose of the Release

This release fixes four defects, two of which were found internally, and two of which we found when troubleshooting directly with one of our customers. To that customer - you know who you are - thank you for helping us get to the bottom of these issues!

New and Improved

- **N/A**

Defect Fix Description(s)

- **Data Validation on an Internal File (DEV-2037)**
  - An internal data validation issue existed for a specific set of informational data. We don't believe that there was any possibility of impacting customer use, but we fixed it anyway out of abundance of caution.
- **List Tag Inconsistency On Removal (DEV-2042)**
  - We discovered an internal condition where removal of entries from a list did indeed properly remove from the database, but they could still erroneously be tabulated in logs as still existing in the source it was removed from. This is now fixed.
- **DNS Proxy Failing for Sizes > 512 Bytes (DEV-2056)**
  - An internal buffering problem occurred for certain DNS requests larger than about 512 bytes, causing the request (and/or the reply) to not be propagated. This is now fixed.
- **Software Watchdog Timer Race Condition Caused a List to Hang (DEV-2057)**
  - An internal timing problem with a specific software watchdog as it relates to list management could result in the list being hung, which kept it from populating, although the system would otherwise proclaim everything was fine. It wasn't. This is now fixed.

Release: ThreatBlockr 2.0 Build 58

File Date: 19 November 2020

Purpose of the Release

This release fixes a few minor defects. If you're already on build 57 (the prior release to this one), there's no explicit need to install this update unless you are impacted by one of the defects documented below.

If you are currently on build 57 and want to upgrade to this new build 58, note that this is the first time you'll be able to use our cool automated software update feature from the GMC Assets page, since the automated update feature requires a minimum installed build of 57 to function. Give it a try!

New and Improved

- **N/A**

Defect Fix Description(s)

- **CPU Clobbering By an Internal Process (DEV-2038)**
  - During routine internal testing, we noticed an internal process that was not properly giving up CPU resources, which caused a CPU core to spin needlessly. This did not in any way impact system performance, but it did unnecessarily consume system resources. This is now fixed.
- **New User Creation (DEV-2043 and DEV-2044)**
  - Our new user creation routines on ThreatBlockr 2.0 devices had two defects. The first defect was that we weren't properly enforcing the password rules for required character groups, which caused confusion on initial password entry when adding a new user. The second defect was that after creating a new user, the system didn't actually create it. A workaround to coax it into creating it was to go back to the users list and edit the new user's credentials to re-enter the password. Both of these defects are now fixed.
  - We'd like to thank one of our (potential!) customers/partners for discovering these two defects and letting us know about them! You know who you are! Thank you!

Release: ThreatBlockr 2.0 Build 57

File Date: 29 October 2020

Purpose of the Release

This release fixed a couple of minor bugs, provides ThreatBlockr rebranding, and adds an exciting new feature to simplify and automate the software download process moving forward.

New and Improved

- **Automated software download support (DEV-1684)**
  - We're excited to release our new automated software download scheme. Our users still have 100% control over the download process, and we've left the old manual mechanism in place, but this exciting new feature allows our users to, at their discretion, perform an automated or scheduled download (or, when applicable, even reverting). This means you'll no longer have to manually download our full secure images only to turn around and manually upload them to your Bandura devices
- **ThreatBlockr Rebranding (DEV-2032, 2033, 2034, 2035, 2036)**
  - We've rebranded our threat intelligence firewall devices. They are now referred to as ThreatBlockr devices. As part of this rebranding effort, our TIG OS 2.0 software is now

referred to as ThreatBlockr 2.0. Why did we go through the hassle of changing the device name? Well, this name just makes more sense. We had been calling ourselves a Threat Intelligence Firewall of late, but that caused some confusion amongst both our existing customers and new customers. To simplify things, we thought it might be a good idea to refer to the device more simply by what it does. And what it does is block threats, in real time, with no added latency irrespective of the line rate and irrespective of the number of active threat indicators. And so, the name ThreatBlockr is born!

Defect Fix Description(s)

- **Database connection slot problem (DEV-1958)**
  - We had seen this problem at two separate customer sites over the past several months, and in both cases it was cleared by a system reboot. We were finally able to internally reproduce this issue and we tracked it down and have now fixed the root cause issue to this extremely rare problem.
- **Internal buffer size problem (DEV-2027, partial)**
  - We noticed a buffer size problem with an internal DPDK buffer that we went ahead and fixed. We hadn't seen any issues either internally or in customer environments related to this, but regardless, it is now corrected.

Release: **TIG OS 2.0 Build 51**

File Date: 9 October 2020

Purpose of the Release

This is a minor release adding a specific software build number for one of our box-build partners. There is no need for end users to install this release (but it doesn't hurt if you do).

New and Improved

- **Adjusted software build configuration number (DEV-2029)**
  - We added a new internal configuration (extends on DEV-1938) software model for some new COTS hardware being used by one of our box-build partners.

Defect Fix Description(s)

- **Initial box-build installs not properly starting list update services (DEV-2030)**
  - We introduced a problem recently when adjusting some of our list naming conventions which kept list services from properly starting on the device for brand new installs shipping from our box-build partners. The issue had no bearing on previously installed customer equipment. Regardless, this is now fixed.

Release: **TIG OS 2.0 Build 49**

File Date: 25 September 2020

Purpose of the Release

This is a minor release adding a specific customer requested feature relating to SNMP support. If you don't need SNMP support for bridge pair monitoring, then there's really no need for you to install this release.

New and Improved

- **SNMP monitoring of bridging interfaces (DEV-2016)**
  - We now have the hooks in place to leverage SNMP for monitoring our DPDK-managed bridging interfaces. We had a customer ask us for this since they were used to leveraging SNMP on our legacy software to monitor their bridge pairs, and wanted to be able to do the same on our newer TIG OS 2.0 software.
- **Other minor internal improvements (DEV-1938)**
  - We added a new internal configuration for some future stuff we have planned.

Defect Fix Description(s)

- **Minor fix to catch an error and create a missing directory (DEV-2023)**
  - A very minor internal error is now handled properly. It was causing no real issue since the defaults that were used on fallback were correct, but regardless, it is now fixed.
- **Corrected a loose state handling configuration problem on an initial box build (DEV-2025)**
  - This one impacted our hardware build partners/integrators, but does not impact our end customers. We missed an initial box-build configuration step related to the loose state handling feature we added in build 48. This means our build partners will be shipping new systems with build 49.

Release: TIG OS 2.0 Build 48

File Date: 16 September 2020

Purpose of the Release

This is an exciting release, as it finalizes our planned work and improvements for our already exciting syslog export features. Several new features while fixing several important defects, including two serious defects, one of which is a security vulnerability - **and thus it is our strong recommendation that all customers upgrade to this release as soon as possible**.

New and Improved

- **Final planned round of major syslog export improvements (DEV-1974, 1981, 1984, 1996, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2015)**
  - With this release, we have finished our last planned major round of feature extensions

and improvements to our already-powerful syslog export features. We have streamlined the key value pairs, so you may need to update your parsers if you were pulling out connection information from our exported packet logs related to denied lists, allowed lists, and threat lists, especially.
    - Furthermore, with this release, we have fully documented our user-facing official RFC-compliant syslog export format as “version 1”. For a detailed descriptive document, feel free to reach out to our Customer Success team. Of course, we will continue to have minor improvements to our syslog export features over time, but we’re really excited since this release contains the last big-ticket items that we had planned.
    - For one of these items, we’d like to explicitly thank the good folks at Gravwell, who pointed out that we really ought to consider publishing the RFC-compliant APP-NAME field to uniquely identify our application. Consider it done! Gravwell is a preferred partner of ours for analysis and visualization of our awesome syslog export detail, and we highly recommend you check them out at https://gravwell.io. We also recently partnered with Gravwell to create a built-in “Bandura Cyber Kit” that customers can download directly from the Gravwell ecosystem for out-of-the-box queries and dashboards against our powerful syslog exports.
- **Add loose state handling detail to internal logs and syslog exports (DEV-1802)**
    - We now publish our loose state handling (LSH) connection direction determination data for cases where we were unable to “see” the initial SYN or SYN/ACK packets. Generally, our loose state handler operates by performing high-port-number analysis in real-time. When we leverage LSH (which is rare as usually we can definitively determine the direction), we now show these occurrences with small UI elements on the Internal Logs page. Additionally, when leveraging loose state handling, we also export a new key-value pair “lsh=true” in the associated syslog export, which can be parsed if desired in connected SIEM tools.
- **Minor improvements to our administration and recovery menus (DEV-1834, 1873, 1965, 1991)**
    - These include better software version visibility, a CLI shutdown option, DHCP configuration, and more.
- **Other minor internal improvements (DEV-1823, 1894, 1994)**
    - These are a variety of internal features, wording changes, and behind-the-scenes improvements to performance, towards our perpetual goal of always improving the overall customer experience.

Defect Fix Description(s)

- **Allow only TLS 1.2 for secure connections (DEV-2009)**
    - **<u>We consider this a significant security vulnerability and strongly recommend that all customers upgrade to this release as soon as possible.</u>**
    - We would like to thank one of our customers (you know who you are!) for pointing this out to us; after an independent vulnerability scan, they found that in addition to properly allowing TLS 1.2, we were erroneously allowing TLS 1.0, TLS 1.1, and SSLv3 by default. This is bad since TLS 1.0, TLS 1.1 and SSLv3 all have known security vulnerabilities that can result in insecure communications when exploited by a clever attacker. This is now fixed, and we now only allow TLS 1.2 for secure communications

channels.

- **Historic session purging was broken, potentially causing UI login lockout (DEV-2022)**
  - **<u>We consider this to be a significant defect and strongly recommend that all customers upgrade to this release as soon as possible.</u>**
  - This particular problem was discovered internally, and has not been witnessed in the field yet, but it could show up, so we thought it best to get it fixed as soon as possible. There was an internal database contention problem keeping historical session logs from being properly cleared, which, in the worst case, could have resulted in access by either API or the UI being denied. This has been fixed.
- **Corrected a potential stale-data condition in system log exports (DEV-2014)**
  - A minor internal condition existed where a structure was not being cleaned, which could have resulted in stale data being output in some system log export scenarios. This was discovered internally, and has not yet been witnessed in the field. Regardless, it has been fixed.
- **The threat category roll-up information sent to GMC needed to be more intuitive (DEV-2017)**
  - You could argue that this is a feature improvement, but it caused enough questions amongst our customers that we decided to classify this as a defect. We had gotten ahead of ourselves a bit with all of the cool attribution that TIG OS 2.0 has in place, and we over-complicated some of the metrics, which caused some confusion. This is in comparison to our legacy TIG OS software which was very limited in its ability to do attribution, but more intuitively mapped to our GMC security posture dashboards. With this fix, we made sure that the data being rolled up to GMC was as intuitive as it used to be, without sacrificing our ability to do detailed attribution in our awesome syslog exports. What does this mean? Basically, it means that the “Allowed by Category” and “Denied by Category” GMC dashboard graphs will no longer show excessive data/counts. They are now intuitive in that the “Allowed by Category” graph means a category was found but allowed through because its score was below a configured threshold. And “Denied by Category” means a category was found to be associated with a connection that was denied (for any reason). We apologize for getting ahead of ourselves and over-complicating this statistic - and a huge shout out to one of our best customers (you know who you are!) for helping us get our heads around the best way to “solve” this nagging concern!

Release: TIG OS 2.0 Build 42

File Date: 10 August 2020

Purpose of the Release

This release is a hotfix release for two specific problems. One was discovered internally, and one was brought to our attention by a customer. We also included a key improvement to an existing feature that will have great value in an upcoming update to our GMC SaaS application.

New and Improved

- **Include Bypass Information in all Healthcheck Data (DEV-1989)**
    - We recently revamped our GMC backend and frontend architecture ahead of some exciting new features that are coming soon. One of these features includes the ability to show more detailed information about a company's devices at the GMC level, to include information about whether a given system is in bypass mode or not. We had some of this information being transmitted between the TI Firewall and GMC already, but this feature provides the data ubiquitously.

Defect Fix Description(s)

- **Intermittent Device Synchronization Problem with GMC Manual IPv4 Lists (DEV-1987)**
    - We ran into a rather nasty intermittent device synchronization problem, reported by one of our customers. A sincere "Thank you!" goes out to that customer for reporting the problem to us and working with us on resolution! You know who you are!
    - We were able to identify a workaround, but it was not an especially easy to apply workaround. Thankfully, we've been able to isolate the issue, and this fix should remedy it. Since it manifests intermittently, we believe that other customers may run into this problem sporadically. Since it is extremely important that manually added IPv4 list entries (such as, for example, to add a false positive IP to an existing manually crafted allowed list) take effect properly every time, all the time, we decided it was important to push this release immediately out-of-band as a hotfix.
    - **We consider this a serious defect and we urge all customers on a prior build to update to this build as soon as they can, and especially if they run into problems adding IPv4 addresses to manually crafted allowed and denied lists.**
- **TCP Reset Packet Handling Fix (DEV-1993)**
    - Our TCP Reset packet handler on drops is a fairly typical and recommended approach for notifying a protected system of an outbound TCP connection that was blocked. There was a defect in the handling that could cause the controlling process to fail on non-TCP traffic. Our internal software watchdogs were able to detect this and fix things behind the scenes, but we removed the possibility of this happening in the future with this update, thereby ensuring performant and accurate TCP Reset generation.

Release: **TIG OS 2.0 Build 40**

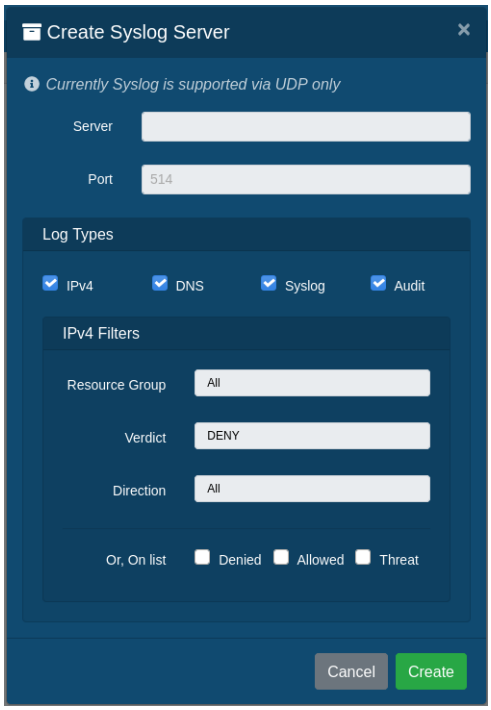
File Date: 31 July 2020

Purpose of the Release

This release continues our trend of significant improvements to our syslog export engines, adds a few other nifty features, as well as addresses a few minor defects.

New and Improved

- **Logs Clearing (DEV-1661)**
    - Our in-memory device logs are always cleared on reboot, but now they can be cleared on-demand at runtime with no impact to network and security performance. This can be very useful when doing security triage in real-time.
- **Jumbo Frame Support (DEV-1895)**
    - We now support jumbo frames in our enterprise-caliber Dell R340-based 1G-X and 10G-X systems, which we outfit with special bypass NIC cards leveraging robust Intel chipsets. No extra configuration is required, as our software stack natively configures the hardware for maximum jumbo frame support, up to the capabilities of the specific chipset. Generally, for our 1Gbps systems, the maximum jumbo ethernet (including header and CRC) frame size supported is 9234 bytes. For our 10Gbps systems (which leverage different Intel chipsets), the maximum jumbo ethernet (including header and CRC) frame size supported is 15872 bytes. Note that these frame sizes are subject to change, depending on a variety of hardware and software factors.
- **Logs Export Filtering Extensions (DEV-1907)**
    - Our syslog export capabilities continue to be extended and are now even more powerful. We can now incorporate things showing up on any defined list type, yielding the boolean export expression: `(Resource Group && Verdict && Direction) || Denied || Allowed || Threat`:



    - For example, you could choose to send just the information about connections that were blocked across all of your resource groups in both directions, but also additionally send any logs that appeared on any combination of allowed, denied, and threat lists. That can be really interesting ways to reduce your third-party SIEM costs since it limits the amount of data ingested by a SIEM to just the things you care about. In the above example, we cared about blocks plus anything that might have been on a known list. That can be a great way to utilize a SIEM tool of your choosing to centrally triage what is being blocked and allowed across the things you care about.

- **Allowed and Denied Lists Naming Convention in the UI (DEV-1963)**
    - In the same way we've recently changed our naming conventions in our Global Management Center (GMC) UI with respect to renaming Blacklists and Whitelists to Denied Lists and Allowed Lists, respectively, we've done the same thing on our devices.
- **Allowed and Denied Lists Naming Convention in Syslog Export (DEV-1964)**
    - We've also updated to the new allowed and denied list naming convention in our syslog export data. Previous quantities `blacklists_…` and `whitelists_…` are now `deniedlists_…` and `allowedlists_…`, respectively.
- **URL Updates (DEV-1976, 1977, 1978)**
    - With the recent major updates to our cloud-based GMC SaaS, we updated several of the internal URLs in the device to map to the newest, most up-to-date URLs.

Defect Fix Description(s)

- **Internal Logs View Display Errors on Time-Based Searches (DEV-1969, 1972)**
    - A customer-reported defect resulting in an error when searching the internal logs directly on the device with certain date constructs has been fixed. While fixing this, we also extended the functionality a bit, with pagination now possible on either side of the resulting position in the logs.
- **Other minor internal fixes and improvements (DEV-1918, 1970, 1975, 1979)**
    - A variety of minor internal fixes and improvements were also made.

Release: TIG OS 2.0 Build 38

File Date: 13 July 2020

Purpose of the Release

This is a fast-follow to our MVP (Minimum Viable Product) build 37 release of TIG OS 2.0 which was our very first release supporting a single 10Gbps bridge pair on new Bandura Cyber 10G-capable products.

New and Improved

- **Line-Rate Small Packet and Burst Performance (DEV-1967)**
    - We had already blown away our MVP projection by being able to support 150,000 connections per second at 256 byte packets. But now, we're able to proudly claim that we can support line rates at 10Gbps even at the smallest 64 byte packet sizes, with minimum measurable impact to latency, thanks to our patented filtering architecture!
    - This improvement also really helps with some loss that could conceivably occur at very high transient burst rates, especially on lightly loaded 10G fiber circuits.

Defect Fix Description(s)

- **Other minor internal fixes (DEV-1968)**
    - A minimal impact memory reference error resulting in memory being read that wasn't

needed was addressed.

Release: TIG OS 2.0 Build 37

File Date: 30 June 2020

Purpose of the Release

This is our MVP (Minimum Viable Product) release of TIG OS 2.0 supporting a single 10Gbps bridge pair on new Bandura Cyber 10G-capable products that are now generally available. If you'd like to inquire about purchasing a 10G-capable Bandura Cyber product, please contact your Bandura Cyber sales representative. Like all Bandura Cyber TIG OS 2.0 releases, this release is cumulative and also supports our non-10G equipment. This release also fixes a few recently discovered defects.

New and Improved

- **10Gbps Device Support (DEV-1483, DEV-1926, DEV-1947, DEV-1948, DEV-1952, DEV-1953, DEV-1954, DEV-1956)**
  - We are excited to release our first official 10Gbps threat intelligence firewall product. For information about ordering our 10G-capable device, please contact your Bandura Cyber sales representative.
  - Our 10Gbps MVP release target was to be able to support 100,000 connections per second with average packet sizes of 256 bytes, to truly stress the system -- that is to say, we didn't skate by with simplistic "large packet" testing. Instead, we stressed the system with lots of small packets so as to better represent highly stressful real-world environments. We're happy to report that our MVP release not only met the 100,000 connections goal at 256 byte packets, but our tests demonstrate that our MVP release can handle 150,000 connections per second with 256 byte sized packets without adverse packet loss.
- **Syslog Export Defaults (DEV-1940)**
  - To avoid data deluge, by default our syslog export function will export information about packets that have been blocked. If your specific SIEM or other syslog target can handle information about all allowed and denied packets, you can still of course select everything for export in the syslog export configuration screen.
- **General Internal Performance Improvements (DEV-1946, DEV-1951, DEV-1960, others)**
  - This includes better CPU and memory management and isolation, compiler optimization updates, plus better queue management, especially useful for TCP-related activity at very high connection rates.
- **Removed Extraneous Script Restart Alert (DEV-1957)**
  - We removed some misleading, extraneous script restart alerts that were showing up erroneously in the logs.

Defect Fix Description(s)

- **REACT Stats Propagation to GMC (DEV-1945)**

    - A problem with the propagation of REACT meta-statistics from TIG OS 2.0 to GMC has been addressed.
- **Policy Evaluation Edge Case (DEV-1962)**
    - An edge case with policy evaluation resulting in improper direction assignment is now addressed.

Release: TIG OS 2.0 Build 34

File Date: 12 June 2020

Purpose of the Release

This release adds some minor feature improvements including the latest DPDK 18.11.8 LTS build, which is responsible for packet performance improvements and several security fixes. This release also fixes a few recently discovered defects.

New and Improved

- **DPDK 18.11.8 (DEV-1903)**
    - We now ship with DPDK 18.11.8, which includes the latest set of improvements and fixes for DPDK to include security fixes for recently announced security vulnerabilities CVE-2020-10722, CVE-2020-10723, and CVE-2020-10724.
- **Proper Logout Endpoint Cleanup (DEV-1935)**
    - A proper auth/logout endpoint now exists in TIG OS 2.0. Previous logout attempts did indeed log the user out, but internal active session lists were not immediately being cleaned up. With this improvement, the active session lists are now able to be cleaned up immediately.
- **Removed Internal/Extraneous License Detail (DEV-1936)**
    - We removed some misleading, extraneous internal licensing information present in a specific UI screen after receiving several support calls where it had sparked confusion.

Defect Fix Description(s)

- **Memory Error (DEV-1930)**
    - A possible buffer overflow error in an internal library used by an internal registration tool was fixed.
- **Tombstone Policies (DEV-1934)**
    - A set of related problems existed which could cause policies that had been removed from GMC to not be fully removed from associated devices, resulting in a tombstone effect where policies were still being loaded and evaluated internally in the device even though they were not truly marked as being in-use. This has now been fixed.
- **UI Session Timeout (DEV-1943)**
    - The UI session timeout feature was not functioning properly. It now properly logs out after the session timer expires.
- **Other minor internal fixes (DEV-1941, DEV-1942)**

Release: TIG OS 2.0 Build 32

File Date: 22 May 2020

Purpose of the Release

This release provides exciting new features, the highlight being support for Domain Attribution. The release also addresses several important defects.

New and Improved

- **Domain Attribution (DEV-1893)**
  - Our TIG OS 2.0 packet logs have always supported full attribution, and now our domain logs do too!
- **95/5 Tracking (DEV-1656)**
  - We've added new industry-standard 95/5 bandwidth utilization tracking features, which enables us to provide more downstream billing configuration options to better meet diverse customer needs over time.
- **Alerts for Bypass Engagement (DEV-1752)**
  - Alerts are now generated if the bypass circuit is engaged, for any reason. This is an important alert since traffic is always passed-through on circuits placed in bypass mode, bypassing the internal Bandura Cyber protection engines.
- **Hardware Support for some of our X-Series Legacy Devices (DEV-1924, DEV-1925)**
  - We're happy to report that we've been able to certify our TIG OS 2.0 software on some of our older X-series hardware.

Defect Fix Description(s)

- **Disk Full Condition Due to Database Activity (DEV-1921)**
  - We internally identified a set of conditions that could result in the root disk partition becoming full due to runaway database activity. This has been fixed.
- **Remove Extraneous Connection Error Message for DHCP Admin Access (DEV-1906)**
  - An incorrect GMC connection error message was being reported on TIG OS 2.0 devices for an internal condition surrounding DHCP admin port connections. The scenario was not actually an error, and the internally generated error message has been removed.
- **Other minor internal fixes (DEV-1871, DEV-1928)**

Release: TIG OS 2.0 Build 30

File Date: 9 April 2020

Purpose of the Release

This release provides exciting new features relating to our syslog export capability. The release also addresses several important defects.

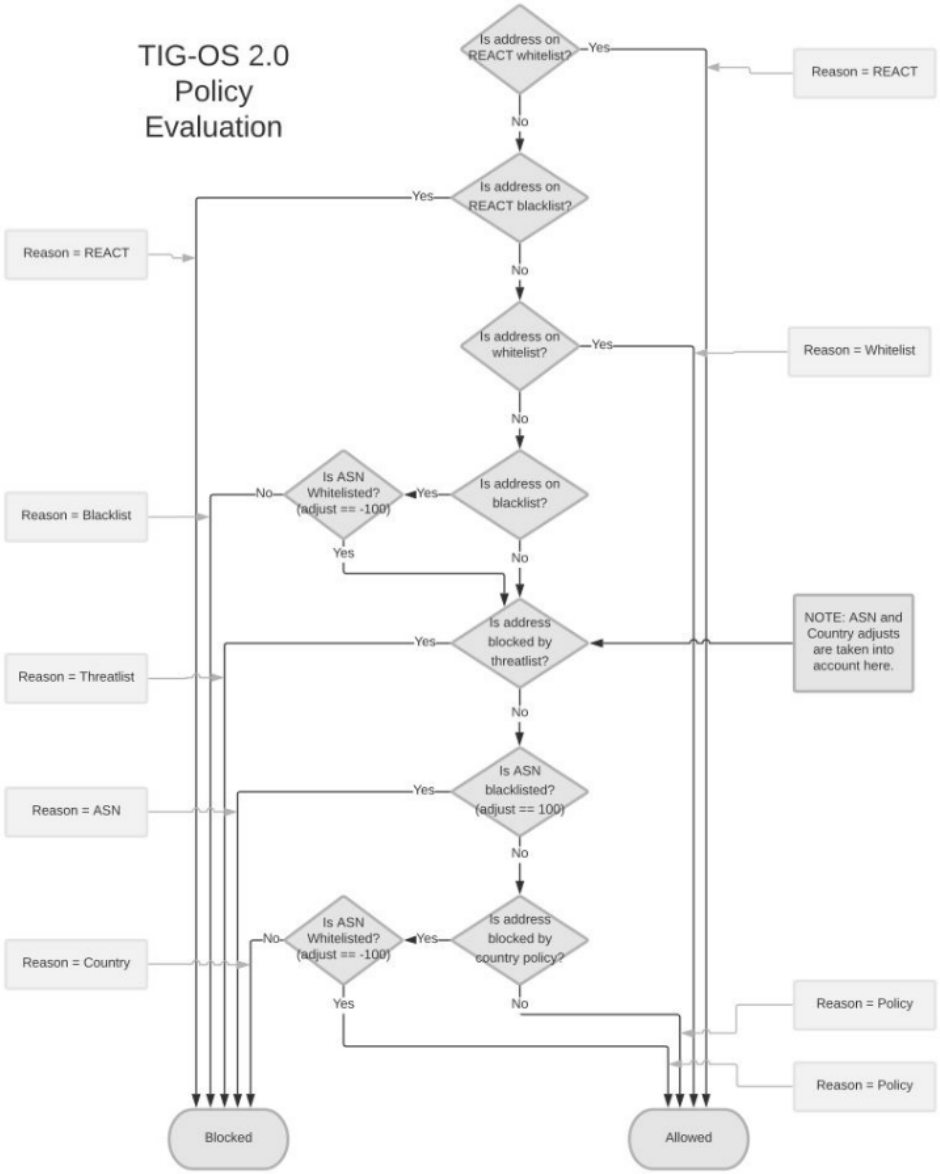
New and Improved

- **External Syslog Connection New Features and Improvements**
  - Although most tools don't specifically care about syslog export formats, our export headers are now fully compliant with RFC 5424. We've verified compatibility with syslog-ng, Gravwell, and Splunk.
  - When configuring the connection to an external syslog server, we now support individual selectors for packet logs, DNS logs, internal system message, and audit logs.
  - Packet logs can now be filtered by a configurable combination of Resource Group, Verdict and Direction, allowing end users to send only the data of interest to their external syslog servers, which can greatly reduce system cost when the target system (such as Splunk and others) charge users based on the amount of data that is ingested.
  - The syslog export data now supports all possible combinations of multiple list and multiple category outputs, with header name changes to include `whitelist -> whitelists`, `blacklist -> blacklists`, `threatlist -> threatlists`, and `category` is removed and has been separated into `matched_categories` and `denied_categories`.
  - Threat list categories are now output to the syslog export channel(s) as `matched_categories` and `denied_categories`. The `matched_categories` will be populated whenever a threat list category match is detected regardless of score, and it will also appear in the `denied_categories` list if its relevant category score was above the risk threshold setting for the associated policy.
  - The TIG's hostname is now output to all syslog export types, appearing between the standard syslog timestamp field and the log type name. This can allow users (or SIEMs or other systems) to pull such information directly from the log stream as opposed to being forced to use metadata attached by third-party external syslog server or other software.

Defect Fix Description(s)

- **Policy Change Impact to Already-Established Connections (DEV-1882)**
  - Previously, if a suitable policy change was made, an already-established connection that should begin to be denied by virtue of the policy change was still being allowed. This is now fixed.
- **Buffer overrun (DEV-1884)**
  - A potential internal buffer overrun condition resulting from filter size errors has been corrected. This could have resulted in anomalous blocking behavior in rare situations where GMC-supplied filters were incorrectly oversized. This addresses the problem in a more consistent fashion than the rapid hotfix that was originally supplied in Build 25.
- **Whitelists not properly applied to packet analysis in some scenarios (DEV-1897)**
  - A possible problem with whitelist vs blacklist determination for some packets has been addressed. With this fix, REACT blacklists are a higher priority than standard whitelists, which is the desired behavior. We've updated the customer-facing documentation to

match the corrected policy. Purely for reference, the current policy evaluation as of build 30 is as follows:



Release: TIG OS 2.0 Build 25

File Date: 5 March 2020

Purpose of the Release

This release serves as a hotfix to address a single, critical defect that was internally discovered by the Bandura Cyber team after the release of Build 24.

Due to the critical nature of this defect, Bandura Cyber strongly recommends that all current users running TIG OS 2.0 Build 24 immediately upgrade to Build 25 after first rebooting their device.

Defect Fix Description(s)

The identified defect caused the TIG to behave erratically and not follow its configured policy settings when receiving certain oversized filters. The result was incorrect traffic allowed/denied patterns which can erroneously impact your network and your network's security.

Normally, a reboot is not required prior to a Bandura Cyber software update, but the specific defect in Build 24 could have resulted in internal memory corruption, and therefore it is safest to first reboot a system that is currently running Build 24 before updating the software to Build 25. To reboot your device, log into the TIG's local web administration GUI from your favorite browser, select System > Reboot on the left-hand navigation pane, and then click the OK button in the modal that appears. After a few minutes the system will finish rebooting and you can then safely follow the standard Bandura Cyber software update procedure.

Release: **TIG OS 2.0 Build 24**

File Date: 20 February 2020

Purpose of the Release

Bandura Cyber is pleased to announce the release of the Bandura Cyber Threat Intelligence Gateway (TIG) OS 2.0. This release includes significant improvements to our Threat Intelligence Gateway (TIG) as listed below.

New and Improved

Bandura Cyber TIG-OS 2.0 new features Include:

- **Significant Performance Improvements** - TIG OS 2.0 can now support over 150M unique IP and domain indicators. This upgrade in performance offers unprecedented protection from a broad range of today's IP and domain threats.
- **Threat Feed Source Attribution** - Our on-device logs now associate IPs and domains with specific threat intelligence feeds and lists. This enhanced context improves visibility into specific threats, the ability to investigate threats, and most importantly, provides a mechanism to measure ROI and efficacy (i.e. false positives) for specific threat intelligence sources.
- **Improved Blacklisting & Whitelisting** – Our REACT functionality now has the ability to provide both whitelists and blacklists. Blacklist policies are now configured based on specific resource groups which provide mode granular policy management and enforcement capabilities.
- **Enhanced Visibility and Policy Control –** Through the use of expanded resource groups for global policy information, as well as JSON-based configuration import functionality, users can identify changes and quickly configure multiple TIG deployments across their network.
- **Usability Improvements –** A snappier and more responsive interface, improved IP lookups, and "context at a click" with intuitive icons throughout.
- **New threat feeds and whitelists –** New, out-of-box Feodo threat feed that tracks botnet C&Cs associated with Emotet (Heodo) and Dridex. A new IPv4 whitelist that helps mitigate false positives and provide richer contextual information about connection information. A new, curated, GitHub whitelist available for all users to easily configure and enable.