FLIR Cyber Hardening Guide

09/2018

FLIR Cyber Hardening Guide

Overview

This document is meant to serve as a general guide for securing IP-connected FLIR security hardware, such as cameras, encoders, radars, and similar devices. Some settings or features described may not be available on all products or firmware revisions.

Cyber security is an evolving process and typically depends on variables specific to a site, installation environment, or use case, making it impossible to develop a universal set of recommendations or procedures. FLIR does not guarantee the following the recommendations outlined in this document will render a system “safe” from cyber-attacks, though it will provide a minimum of increased cyber hardening relative to a default installation.

Note that FLIR currently ships many products in a default configuration that makes initial setup easier, such as using default accounts and passwords, but which also makes the products unsuitable for connection to an openly accessible network without some amount of cyber security hardening applied. It is FLIR’s expectation that these defaults will be changed to settings and values appropriate to the installation environment and application of the product. Changing these settings is the responsibility of the installer or end-user.

Those unfamiliar with the features and settings outlined in this document should refer to the manuals for the specific products being administered under these guidelines for additional details on how to implement the suggested settings, or potential operational impacts from doing so.

FLIR Cyber Hardening Guide

Update Firmware

FLIR regularly updates product firmware to add new features or correct any issues reported. Each FLIR Security product page on FLIR.com includes a “support” tab where users can be located firmware updates. All devices should be updated to latest available firmware as a matter of best practice and to ensure that all known issues have been resolved.

Reset to defaults

It is best to start any hardening process with equipment in a known state. Resetting your product to factory defaults will wipe out any stored user accounts or settings that may not have been documented or known to those implementing the cyber security processes. Note that resetting a unit in a production environment to its defaults will likely result in the unit being inaccessible until proper settings required for operation can be successfully restored.

Secure User Accounts

Managing access to devices is one of the core requirements for minimizing cyber-attacks and breaches. Devices will generally have an “admin” account from which a user can take full control of features and settings, as well as restore defaults. The admin account should have a strong password, using a combination of letters, numerals, and symbols to minimize the chances it can be guessed or cracked.

If your organization has policies for strong password formats, they should be followed as part of setting the admin account. If you do not have a strong password policy, FLIR recommends an account password with a minimum of 10 characters that uses at least two uppercase, lowercase, numeric and symbolic characters. The password should be highly random (eg: Hq&9Nb41m%) and not follow a guessable substation pattern (eg: C0mp@ny1).

Use of the admin account should be strictly limited to individuals who need to make changes to device settings. The admin account should not be used to connect to a video management system (VMS) or other software platforms. It should also not be used for the general viewing of video or for regular operations usage.

For products that support individual user accounts, such accounts should be created with appropriately limited permissions for each person or service that will log in to the device. This enables easier administration when account privileges need either to be escalated or revoked over the course of operation. For products with limited user accounts (eg: Admin / Expert / User), the account with the lowest privilege level necessary for a given use should be selected for that application. All accounts should have strong passwords as outlined above that are updated on a regular basis to prevent accidental disclosure or unauthorized use.

Secure Network Architecture

In most applications, the security devices will be managed and accessed through a software package, such as a VMS. This enables the use of a network architecture that segments the security devices from production networks, making them much more difficult to access directly by a hacker, while not impairing their intended use.

In other words, the security devices should be on a different network than the corporate network and separated from external/internet/remote access. By doing so, the devices are effectively invisible to external hackers and unreachable by various software probes or analyzers that may be looking for exploitable devices.

While the segmented network provides strong protection against outside attacks, it does not make devices immune to attack. Insider threats are still a possibility, as well as hackers gaining access to the server running the VMS application, which itself may be externally accessible and able to be used to launch attacks against the inside devices. Still, this approach provides significant protection from outside attacks. It offers additional benefits by keeping the network traffic from the security devices separate from the corporate LANs. This should be implemented whenever practical.

Secure Network Access

Even with the secure network architecture outlined above, at least some servers or work stations will need access to the devices. Access should be restricted to the smallest possible set of servers and/or IP addresses possible to facilitate full functionality of the system.

Utilize IP Whitelists or Allowed IPs settings to limit the device to only accept network connections from the specific servers/IPs that will be used for administration, video storage, or streaming access. If remote access to devices is required, FLIR recommends the use of a VPN server, preferably with a two-factor authentication scheme that both validates and authorizes remote users onto the network from which the security devices are accessible.

If a VPN is not practical, an acceptable alternative can involve remote desktop services that enable remote access to an internal PC. As a given, such services should be selected based on their history of security. In addition, a dedicated machine with minimal pre-installed software should be used as the remote connection host. Do not enable remote desktop connectivity directly to critical servers or workstations.

FLIR does not recommend placing any security hardware directly on “open” or “port-forwarded” networks that enable unfiltered remote connections. Doing so exposes devices directly to random connection attempts, IoT logging services (such as Shodan), and other connections that would

generally be considered undesirable for a security network. This increases the risk of exploit, or of denial of service attacks directed at a device, rendering it potentially inoperable.

Disable Unused Services

FLIR has designed many of its security devices to be extremely versatile and to fulfill several customer requirements for different applications. While this makes the devices very flexible, it can also create additional security weaknesses, as it increases the number of potential attack points. Any unused features or services not being utilized in your environment—such as FTP, SSH, SNMP, or SAMBA—should be disabled to prevent these services from being utilized as potential attack points.

Time/Date Settings

Having all time clocks across devices and servers synchronized makes investigations of potential attacks or other issues easier, given that all devices use a consistent time base. Configuring devices to receive time/date data from an NTP server will help ensure time clock accuracy across all components of the security infrastructure.

Use Internal Servers When Possible

DNS and NTP servers are two of the most commonly utilized external services in security networks. DNS provides name resolution, allowing a hostname like "www.flir.com" to be resolved to an actual IP address to connect to the server. NTP provides time/date information.

It is common practice to rely on external servers, such as Google's "8.8.8.8" DNS server or pool.ntp.org, for NTP data. However, at times, hackers have managed to hijack or redirect data requests on external servers, potentially allowing them to direct traffic to their own servers with spoofed sites that harvest data, such as usernames and passwords. Running these services on an internal server that is properly protected and secured can help reduce the chances of attack via 3rd party services. Setting up and maintaining your own DNS or NTP servers is outside the scope of this document, though resources and guidelines are readily available on the internet for doing so.

Keep Firmware Updated

The cyber security hardening process starts with using latest available firmware. Maintaining up-to-date firmware is an ongoing requirement to ensure that any vulnerabilities that may have been discovered are properly addressed. Check for updated firmware regularly and patch affected devices as appropriate.

Check Log Files

Periodically check log files from security devices, VMSs, firewalls/VPNs, and related components of the security network for signs of attack or intrusion. In many cases attack attempts can be noticed before access is gained, and appropriate actions can be taken to keep attackers out of your network. If attackers hack gained access, log file review may help determine which devices have been affected and need to be addressed as part of a remediation plan.

Penetration Testing

Regular attempts to “hack” your own network should be carried out, in a coordinated fashion, to ensure that devices are truly secured and only accessible via expected paths. Additionally, outside cyber security firms can be hired to attack and audit your infrastructure, utilizing the same tools and methods that hackers would commonly undertake to gain access to devices or servers.

In some cases, these penetration tests can include testers pretending to be from the IT Department or Corporate headquarters and requesting passwords, or various forms of equipment access, from random employees associated with the security infrastructure.