AXIS Camera Station Pro

System hardening guide

Introduction

A one-size-fits-all, fool-proof feature that could make any security system and site 100% cybersecure. As appealing as those words sound, no such feature exists — or is likely to exist anytime soon. Instead, one needs to examine the risk posed by threats and vulnerabilities unique to their organization and, when the risk is deemed unacceptable, implement controls to mitigate that risk. Well-defined policies and procedures ensure consistent communication and application of those controls throughout an organization and form the basis of a mature cybersecurity program.

A recommended approach is to work according to standardized IT security risk management frameworks such as ISO 27001, NIST CSF or others. While this task may be daunting for smaller organizations, defining a basic set of information security policies and supporting processes is far better than having nothing at all. If your organization is getting started on a journey to cyber maturity and have limited resources at your disposal, we recommend investigating the *Center for Internet Safety (CIS) Critical Security Controls Version 8*. CIS provides a list of 18 security control activities organized into three implementation groups to help organizations develop and mature their cybersecurity program.

Security breaches occur in many organizations because the company has not established clear policies, rules and procedures that govern the usage of and access rights for their own employees. Is your organization working with policies and processes for video management operations? If not, it is time you start defining them.

Purpose

This document outlines a number of cybersecurity policies and procedures useful to support secure deployment and maintenance of systems. While not directly mapped to a cybersecurity framework, we do draw primarily from CIS Security Controls v8 with a particular focus on the following Control activities:

- *Control 1: Inventory and Control of Enterprise Assets*
- *Control 2: Inventory and Control of Software Assets*
- *Control 3: Data Protection*
- *Control 4: Secure Configuration of Enterprise Assets and Software*
- *Control 5: Account Management*
- *Control 6: Access Control Management*
- *Control 7: Continuous Vulnerability Management*
- *Control 10: Malware Defenses*

Our recommendations focus on assisting installers, integrators, and end-users to mitigate common risks when deploying and managing systems.

Prerequisites

It is assumed that the recommendations and procedures defined and described in the *AXIS OS Hardening Guide* are understood and followed. Also, this document refers to several common user roles that interact with a video system. Please map these user roles to match your own user and role classifications. An individual user may have multiple roles, depending on the organization.

Defined roles:

- **System Installer**: installs, sets up, repairs, upgrades, and downgrades systems
- **Network Administrator**: maintains the network infrastructure, end node connectivity, network servers and resources, as well as network protection
- **Video System Administrator**: defines and manages the video system to secure its usage, performance, and user privileges

Introduction

- **Video System Maintainer**: monitors, adjusts, and troubleshoots components to secure system performance on behalf of the Video System Administrator
- **Users**: individuals who use client to access live and recorded video and are typically responsible for an organization's physical protection.

System security policies

Physical security

Physical protection policy

Servers, devices, network equipment and cables are physical objects that can be interfered with, sabotaged, or stolen. The host running server software and important network equipment (routers, switches, etc.) should be placed in an environment with physically and logically restricted access. Cameras and other connected devices should be mounted in hard-to-reach places and feature vandal-resistant models or casings. Attention should be made to protect the cables in walls or conduits, as these increase risks of tampering and sabotage.

Recommended policies and procedures
Define an individual or organizational unit that is responsible for visually auditing the physical protection for VMS servers, network hardware, connected devices, and cabling at defined intervals. It is essential to maintain an accurate inventory of all servers and devices, including their location.

Software management

Third party application software policy

As is installed in a standard Windows environment, it can be tempting to utilize that environment for software applications not related to video management. Installing other 3rd party applications opens the possibility of introducing malware into the environment which could lead to system downtime or provide a back door for an attacker to enter the organization's network.

Recommended policies and procedures
Do not run anything other than server software and trusted third-party integrations on the host hardware. If the physical hardware should be utilized for other purposes, it is recommended to use multiple virtual server instances and run the server software in one virtual machine and the third-party non-VMS related software in another virtual machine. Information on running in a virtual environment can be found *here*.

It is recommended that you deploy anti-virus software on all servers and computers that connect to server. If mobile devices are deployed, this includes ensuring that the devices have the latest operating systems and patches (though not directly anti-virus) installed. When you do virus scanning, do not scan directories and subdirectories that contain recording databases. Scanning for viruses on these directories can impact system performance.

Account management

General account policy

Administrator-level rights are sometimes granted to normal users for the sake of convenience. In many organizations, it is unclear who is responsible for reviewing account privileges and monitoring employee access to systems.

Recommended policies and procedures
We recommend that organizations follow the principle of least privilege when defining system accounts. This means that user access privileges are limited to only the resources needed to perform their specific work tasks. It is also advisable to periodically audit the account privileges of system users to guard against "privilege creep".

administrator account policy

A common mistake when deploying in a Windows environment is that a single administrator account is defined for the Windows host. Over time, the password may be shared within the organization with the risk of unauthorized individuals gaining administrator privileges to the Windows environment. This can easily result in numerous unwanted user applications or malware installed on that server.

Recommended policies and procedures
The Windows machine hosting server should have at least one administrator privileged account and one user privileged account.

Neither of these accounts should be the same as the default Administrator account for Windows. The default Administrator account should be disabled after creating the administrator and user privileged accounts. After deployment, the administrator account password should only be known and used by **Network Administrator(s)**. The user privileged account should be used by the **Video System Administrator** if/when they need to login to the server. It should be noted that even if the above two roles are carried out by the same individual, having separate Network and Video System Administrator accounts is still recommended for auditing purposes. To support other roles as defined previously, further non-privileged user accounts should be created for each individual **User** who will log into the system.

If the host running is placed in a Windows Active Directory domain environment, administrator and user accounts can be created in the context of the domain or an employee's existing domain account can be used to authenticate to host. This can simplify account management as no additional accounts need to be created and maintained. This also opens the possibility of using Group Policy Management to enforce password complexity, certificate deployment, and other security features available in domain environments.

user account policy

User accounts are assigned to specific roles in , which in turn determines the specific rights each user has in the system, such as what views and video they are privileged to access. If multiple individuals share a single user account, there is an increased risk of a password being shared with others in the organization. Sharing accounts will also make auditing of who accessed what camera/video at what time practically impossible.

Recommended policies and procedures

We recommend that you use **Kerberos** to authenticate client users, see *Authenticate using Kerberos on page 5*.

If possible, use Microsoft Active Directory for easy user and group management. It is also recommended to verify that the relevant security groups have been defined for all user roles before setting up the system.

Active Directory will also provide:

- A password policy that requires users to change their password regularly
- Brute force protection, so that the Windows AD account is blocked after several failed authentication attempts, in line with the organization password policy
- Role-based permissions, so access controls can be applied across the domain

If one must use local Windows accounts, it is recommended that a unique account be created for each user of the system and that they be given access to only the entities in the system necessary for carrying out their responsibilities. Utilizing groups for users can help simplify the assignment of permissions if there are multiple users with identical permissions.

Authenticate using Kerberos

uses Integrated Windows authentication to authenticate the users of the client. uses the Microsoft Negotiate protocol (SPNEGO) which means that Kerberos is the preferred and default authentication protocol. The Negotiate protocol attempts to use Kerberos and uses NTLM as fallback.

To use Kerberos, you must register Service Principal Names (SPN) in Active Directory using the following command:

```
setspn -s ACSService/{HOST} {ACCOUNT_NAME}
```

HOST – The hostname of the server running server.

ACCOUNT_NAME – The name of the computer (computer account) that runs server.

For Kerberos to work properly, we recommend that you register both short hostname and FQDN for the target server.

Example:

```
setspn -s ACSService/CompanyServer CompanyServerAccount setspn -s
ACSService/CompanyServer.domain.local CompanyServerAccount
```

See *Setspn on microsoft.com* for more information.

Device account policy

The accounts in Axis devices are primarily computer/client accounts. **Users** should never be allowed to access the device directly. The only client that should access devices during normal operation is server. A common strategy is for all devices to have the same password. This introduces additional risks but can also simplify password management so one must assess their own risk tolerance. supports assigning unique passwords to each device through its management interface.

A common mistake is that devices are added to with a single account shared by multiple roles. At some point, when a **Video System Maintainer** needs to use a browser to adjust something, the device's master account (root) password is disclosed. Within months, most people in the organization will know the password for all devices and have administrator privileges to the system.

Recommended policies and procedures
The device should have at least two administrator accounts: a unique one created for device administrators and the default root account for adding devices to server. Temporary access, such as a when a **Video System Maintainer** accesses a device using a web browser, should be managed through the use of temporary accounts.

AXIS Device Manager should be used as the primary tool for managing device accounts and passwords. A version of AXIS Device Manager is built directly into and is available in the Management tab. The device's root password should only be used by AXIS Device Manager and , and it should only be known to those who use AXIS Device Manager or as a tool to manage devices.

Use to provision a temporary account when someone in a maintainer role needs to use a web browser to access (a) device(s) for troubleshooting or maintenance. Select the device(s) and create a new account, preferably with operator privileges, that the maintainer may use. Once the task is complete, remove the temporary account.

System maintenance

Windows host patching policy

server and clients run on top of a Windows environment. It is important that these systems are kept up to date to ensure that the systems hosting software do not have open vulnerabilities that can be exploited to gain unauthorized access to the video management system.

Recommended policies and procedures
For all systems, whether running on Axis NVR or custom hardware, it is recommended to turn off Automatic Update. Windows updates have in the past caused instability in the underlying Windows OS, so it is recommended that available updates are tested on select machines to ensure stability of the system before being pushed out to all host systems running . However, a balance between security and stability needs to be reached as leaving the Windows system un-patched for too long can introduce risk to the overall environment. Based on the exposure level of the customer's system to external threats, a time frame for ensuring that systems receive the latest updates should be outlined in the patching policy.

software update policy

In most cases, using the latest software release for will ensure you utilize security patches for all newly discovered vulnerabilities. Leaving the system unpatched for a longer period will increase the risk of an adversary exploiting the vulnerabilities and possibly compromising the system.

Recommended policies and procedures
It is important to define a patching policy with regular assessments of deployed software versions for ensuring that is up to date. The patching policy should also identify who is responsible for managing the work associated with updating both the server and client software. For , the most recent release can be found on *www.axis.com*. requires the latest .NET libraries so care must be taken to align the Windows patching policy to policy.

Device firmware update policy

Running devices with up-to-date firmware versions mitigates most common risks, as the latest firmware versions will include patches for known vulnerabilities that attackers may try to exploit. Axis provides a long-term support (LTS) release for device firmware that includes security patches and bug fixes but feature additions are limited to ensure the long-term stability of the platform. For more information on Axis' strategy around firmware development, see the *Axis firmware management* whitepaper.

Recommended policies and procedures
For hardware devices, the policy should state that all firmware be kept up to date. Processes can leverage the built-in firmware

update feature in , or AXIS Device Manager Extend, to identify if new firmware versions are available for Axis devices. A scheduled time should be defined, usually outside of business hours, to deploy all firmware upgrades for all cameras. / AXIS Device Manager Extend can also verify if the firmware updates were accepted. If the system has specific integrations that could be affected by updating, consider standardizing on an LTS firmware track.

Network security

Remote access policy

Devices and services exposed to the Internet increase the risk of external adversaries probing or exploiting known vulnerabilities. Cameras exposed to the Internet, for instance by small organizations that need remote video access, become easy victims if weak passwords are used or a new critical vulnerability is discovered. Remote access to the Windows environment should be tightly controlled or avoided if possible. While the Windows environment may have internet connectivity as a matter of convenience for updating systems, utilizing remote desktop services like Windows Remote Desktop, TeamViewer, and AnyDesk introduce paths to gain access to your system if not managed correctly.

Recommended policies and procedures
Never expose a camera's IP address/port in a way that makes it accessible directly from the Internet. If remote video access is required, use Axis Secure Remote Access. uses a cloud-based remote access server to facilitate encrypted remote access to the system via client or the AXIS Camera Station mobile application. Apart from being responsible for connection management for remote and mobile users, the remote access server plays an important role in protecting integrity when used by remote users. More information on Axis Secure Remote Access can be found *here*. Axis supplies officially branded mobile applications for both Android and Apple iOS. The AXIS Camera Station mobile app should only be downloaded from official sources, the Google Play Store and Apple App Store respectively.

When it comes to remote desktop access to the Windows environment, it is not recommended to provide this type of access to a system running . However, if required, extreme care must be taken to ensure that the remote desktop application of choice is secure, and access is only provided to those individuals that require it. Implementing additional layers of controls such as multifactor authentication (MFA) is encouraged. Logging and subsequent auditing of remote connection attempts is highly recommended to track who and at what times the Windows environment is being accessed remotely.

Local network exposure policy

Reducing local network exposure can help mitigate many common threats by reducing the attack surface. There are many ways to reduce network exposure, including physical network segmentation (separate network hardware and cables), logical network segmentation via virtual LANs (VLAN) and IP filtering. Axis cameras support an IP filter (IP tables) so that the device only responds to connection requests made from explicitly allowed IP addresses.

Recommended policies and procedures
AXIS Camera Station S22 NVRs are hardware servers with dual network ports. One of the ports creates a segmented network for cameras and the other connects to the primary network (domain) to serve video clients. The server acts as a bridge and a firewall to the camera network, preventing clients from accessing cameras directly. This reduces the likelihood of threats from adversaries on the primary network.

If server and cameras are all placed on the primary network, it is recommended to configure the camera's IP filter, limiting access to only the servers hosting , AXIS Device Manager, and additional maintenance clients.

Network encryption policy

Network traffic that is transferred over insecure networks should always be encrypted. The Internet is classified as an insecure network. A local network may also be classified as insecure and network traffic should therefore also be encrypted. What policy to apply to video traffic on the network depends how video is classified and the risk of adversaries having network access to the video system. It is recommended to assume that the network has already been compromised. Larger organizations will normally have a policy that defines how the network is classified.

Recommended policies and procedures

The traffic between the video client and server should use encryption. The traffic between server and cameras should be encrypted depending on the infrastructure. Axis cameras come with a self-signed certificate and HTTPS enabled by default. If there is a risk of network spoofing, like when a malicious computer attempts to impersonate a camera, a private key infrastructure (PKI) with CA-signed certificates should be used. has a built-in local Certificate Authority (CA) that can cost-efficiently manage the signing and distribution of server certificates for Axis devices.

TLS versions

We recommend disabling TLS versions 1.1 and 1.0. The AXIS Camera Station installer offers to assist during the installation or upgrade.

HTTPS ciphers

supports and uses TLS cipher suites to encrypt HTTPS connections securely. The specific cipher suite depends on the client that connects to or the service contacted, and negotiates it according to the TLS protocol. We recommend configuring Windows not to use the TLS 1.2 cipher suites listed *in RFC 7540*. The ability to disable a cipher suite depends on the devices and cameras used together with . If a device or camera requires a specific cipher suite, it might not be possible to disable the weak cipher suite.

Data management

Video classification

Live and recorded video should be classified. Video may be classified as public, private, restricted or any other classes defined by organizational policies. In many cases, video is regulated by law and regional regulations as well as internal IT policies, so it is the system owner's responsibility to be aware of the laws and regulations that apply to their video data.

Recommended policies and procedures
Classify live video, recorded video, and audio in accordance with organizational data classification policies. Configure user access privileges and hardening of the system according to the sensitivity of the video and audio data. If not required, audio may be disabled on a device level.

Additional security controls

Depending on the maturity level and risk tolerance of your organization, there are several additional security controls from CIS Controls v8 we recommend implementing to help reduce cybersecurity risks in day-to-day operations.

Additional CIS Controls:

Control 8: Audit Log Management
Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Control 14: Implement a Security Awareness and Training Program
Understand the skills and behaviors of your workforce members. Train the workforce on how to identify different forms of attacks.

Control 17: Incident Response and Management
Utilize written incident response plans with clearly defined phases of incident handling/management and personnel roles, as well as how to report a security incident to relevant authorities and third parties.

System hardening guide
AXIS Camera Station Pro

Ver. M1.7
Date: April 2024
Part no. T10203603