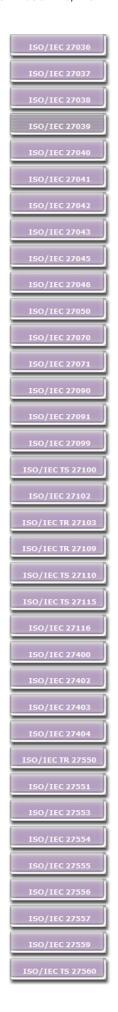
10



1 of 3 8/28/25, 21:31



respond to network security incidents as best they could;

- Automation tends to speed-up identification and response to attacks, particularly common types of attack that can be identified unambiguously through unique attack signatures;
- They give additional assurance to management that security issues on the networks and networked systems are being identified and mitigated.

The standard is, in effect, an ISPS implementation guide and advisory.

## Structure

Three main sections comprise the bulk of the standard's ~50 pages:

- Selection of IDPS various IDPS types, complementary tools etc. to consider (in some detail, expanded still further in the annex);
- · Deployment of IDPS;
- · IDPS operations.

## Status of the standard

The first edition was published in 2015, "revising and canceling" (i.e. replacing) ISO/IEC 18043:2006.

A technical corrigendum in 2016 corrected the title of the published standard, introducing "and prevention" that somehow got lost.

The standard was confirmed unchanged in 2020.

## Personal comments

I had hoped the standard would mention, in addition to the network security risks that they are meant to address, various information risks and issues associated with or introduced by the IDPS themselves, such as:

- They are technologically advanced and complex, making them difficult to configure, deploy and use effectively, hence there is a risk that they may be incorrectly configured, deployed or used in practice, with various consequences on the organisation and other systems. Furthermore, they probably introduce additional technical security vulnerabilities into the very networks and/or systems they are supposed to protect;
- They may adversely affect network traffic, restricting legitimate traffic and hence normal use of the network and systems, as well as hacking traffic;
- They are not 100% capable, meaning that certain types or modes of attack (particularly novel ones) may
  not be reliably identified and hence blocked, potentially creating a false sense of security (inappropriate
  assurance);
- They can only detect and react to available information, making them blind and deaf to attacks that bypass
  the networks and systems being monitored (including, for examples, social engineering and physical
  intrusion attacks):
- They usually require network bandwidth, processing and storage capacity for their own operations and record-keeping, and require hooks into the networks and systems being monitored and/or controlled, impinging upon normal use;
- They are complicated to configure and manage for best effect, requiring the involvement of competent security engineers who, potentially at least, may themselves be hackers;
- They require privileged access to network traffic, network devices and/or systems, and could potentially be misused as a vector or mechanism to compromise them.

However, it does not ...

< Previous standard ^ Up a level ^ Next standard >

2 of 3 8/28/25, 21:31



Copyright © 2025 <u>IsecT Ltd</u>. <u>Contact us</u> re Intellectual Property Rights

3 of 3 8/28/25, 21:31