

ICS 35.020
CCS L70

YD

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

YD/T 6830-2026

**Cyber security situational awareness - Requirements for
security incident detection**

网络安全态势感知 安全事件检测要求

(English Translation)

Issued on: April 15, 2026

Implemented on: August 1, 2026

Issued by: Ministry of Industry and Information Technology

Table of Contents

- Foreword
- 1 Scope
- 2 Normative references
- 3 Terms and definitions

Foreword

YD/T 6830-2026 is a recommended industry standard of the People's Republic of China in the Telecom sector, approved and issued by the Ministry of Industry and Information Technology on 15 April 2026, with effect from 1 August 2026.

It is administered by the China Communications Standards Association.

Classification: ICS 35.020; CCS L70.

1 Scope

YD/T 6830-2026 specifies technical requirements for the detection of network security incidents within network security situational awareness. These include technical requirements for single-step attack detection and for multi-step attack detection. A single-step attack is one isolated hostile action, while a multi-step attack is a sequence of related actions, and the document treats the detection of each. It applies to network security situational awareness products and to business applications that detect single-step and multi-step network security attack events.

The standard is voluntary (code with /T). Product developers, operators of security monitoring services and test laboratories are the intended users. It was approved by the Ministry of Industry and Information Technology, issued on 15 April 2026 and takes effect on 1 August 2026. It is a new standard and belongs to the same series as the overall architecture and data processing documents on situational awareness.