WHAT'S NEW IN ISO27001:2022
THREAT INTELLIGENCE

ISO 27001:2022 is the latest version of the international standard that provides a framework for Information Security Management Systems (ISMS). It's designed to help organisations manage and protect their sensitive information effectively, requiring organisations who wish to remain compliant to adhere to the new requirements by October 2025.

Among these requirements are enhancements such as data leak prevention, web filtering, ensuring business continuity for ICT systems, bolstering physical security monitoring, overseeing configuration changes and fostering secure coding practices. Annex A of ISO 27001 contains a set of controls that organisations can implement to address these requirements.

Of particular interest is the emphasis on threat intelligence outlined in Annex A, Control 5.7. This may pose a unique challenge for organisations lacking established protocols for the gathering and analysis of threat-related information.

Control 5.7 - Threat Intelligence

Control 5.7 of Annex A focuses on threat intelligence, which is crucial for identifying and mitigating cybersecurity threats. Here's a breakdown of what this control entails:

- **Structured Approach**: Organisations must adopt a structured approach to both collecting and analysing threat intelligence. This means having processes in place to gather relevant information about potential threats to their systems and data.

- **Understanding Threat Actors**: It involves understanding who the potential threat actors are – whether they are hackers, cybercriminals, or even insiders with malicious intent. By knowing the adversaries, organisations can better anticipate their motives and tactics.

- **Threat Models**: Organisations need to apply threat models to their systems. These models help identify vulnerabilities and potential attack vectors, allowing for proactive risk mitigation.

- **Vulnerability Identification:** Control 5.7 requires organisations to identify vulnerabilities in their systems. This involves conducting regular assessments and audits to pinpoint weaknesses that could be exploited by threat actors.
.
- **Exploits Analysis**: Organisations must analyze potential exploits that could be used against identified vulnerabilities. This involves understanding the techniques and tools that threat actors may employ to breach systems.

In summary, ISO 27001:2022 Annex A, Control 5.7 introduces the importance of adopting a structured approach to threat intelligence. By understanding potential threats, vulnerabilities and exploits, organisations can better protect their information assets and mitigate cybersecurity risks effectively.

COMPLIANT THREAT INTELLIGENCE SERVICE

Talanos cybersecurity

Threat intelligence platforms are expensive and interestly, hold different sets of data about organisations which is why Talanos purchase feeds from several vendors, providing a cost effective service to organisations. Consolidating data from multiple sources, Talanos analyse tens of thousands of records to create and triage incidents, determining their impact and priority to create actionable intelligence.

If an incident is determined to be a true positive, the team will then work to neutralise the threat on behalf of the organisation. Finally, with the incident contained, the threat intelligence and raw data are passed to the organisation detailing the findings along with steps taken to resolve the incident and any additional recommendations based on observed issues and indicators.

Organisations looking to rapidly satisfy their ISO27001 threat intelligence requirements can rely on Talanos' meticulous documentation, policies and procedures to evidence their compliance.

TALANOS DARK WEB & DEEP WEB THREAT INTELLIGENCE

RISK ASSESS LEAKED CREDENTIALS

Triaging whether the data presents a real risk or is an active indicator of compromise is part of the analysis performed by the Talanos intelligence team. Impacts are quantified and if necessary, the team will run incident response.

DETECT & TAKEDOWN SPOOFED DOMAINS

Typosquatting domains and spoofed websites are registered all the time. Talanos will detect when material that infringes your copyright and trademarks are published and proactively takedown the domains and pages before they become a threat.

IDENTIFY INFECTED MACHINES

Metadata attached to breached data provides a wealth of information on how the data was collected and where it could be subsequently used. Talanos analyses this data to determine a number of insights such as if endpoints have been infected with malware or whether MFA has been effectively rolled out.

DETECT INBOUND & OUTBOUND TOR TRAFFIC

Although there might be a legitimate reason why an end-user would connect to your public facing website from the "Dark Web", it is highly suspect if your infrastructure connects outbound to a Tor network. Talanos monitor these network behaviours to proactively detect emerging threats.

Andrew Gibbens
Head of UK Sales

andrew.gibbens@taloscs.com
+44 (0)1291 343012
+44 (0)7980 275480
www.talanos.co.uk

CYBER ESSENTIALS CERTIFIED PLUS

National Cyber Security Centre INDUSTRY 100

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 8289 ISO 9001 QUALITY MANAGEMENT

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 8289 ISO 27001 INFORMATION SECURITY MANAGEMENT