SALES BRIEFING: THREAT INTELLIGENCE

SKURIO

A NEW REQUIREMENT FOR ISO 27001 CERTIFICATION

Not for direct distribution to your customers or prospects

ISO 27001 IS CHANGING

ISO 27001 will be updated in October 2022 and becomes ISO 27001:2022, and threat intelligence will be a new mandatory requirement. Although organisations will generally be given 2 years to comply with the updated requirements, this is a massive opportunity for Skurio and its channel partners right now. Start talking to your customers about this change to position yourself as a trusted advisor for threat intelligence.

WHAT IS ISO 27001?

ISO 27001 is an international standard that sets out the Information Security Management Systems (ISMS) specification. It allows organisations to establish, implement, operate, monitor, review, maintain, and improve ISMS.

WHAT IS ISO 27002?

ISO 27002 provides details of the security controls that an organisation needs to comply with for ISO 27001 certification. The updated ISO 27002:2022 was released in February, and includes details of the new threat intelligence requirements, which will be incorporated into the ISO27001:2022 update later this year.

WHAT IS THREAT INTELLIGENCE?

The purpose of threat intelligence is to provide awareness of the organisation's threat environment so that the appropriate mitigation actions can be taken.

As an activity, intelligence needs to perform three functions. Firstly, information relating to security threats needs to be obtained. Secondly, this information must be processed (collated, evaluated, analysed, integrated, and interpreted) to form intelligence. Lastly, intelligence needs to be disseminated to those who need it.

Organisations can use this information to prepare for, identify, prevent, and recover from cyber-attacks. Read our Cyber Threat Intelligence (CTI) blog for more detailed information.

WHO NEEDS THREAT INTELLIGENCE?

No matter how big or small, every organisation that uses a computer system (everyone!) can benefit from using threat intelligence – even if it's something simple like monitoring the Dark Web for compromised credentials, or detecting typosquatted domains impersonating your brand.
From top to bottom of the IT chain, the positive impact of threat intelligence can be felt at every level. Knowing they're using their budget strategically and effectively is comforting for the senior management team. Knowing their bases are covered and regularly reviewed helps IT Managers and supervisors sleep at night. Finally, IT technicians and engineers have less on their plates and can get on with their work on the ground.

> "Tell me what you know...tell me what you don't know...tell me what you think – always distinguish which is which."
>
> General Colin Powell, USA Chairman of the Joint Chief of Staff, 1989-1993.

SALES BRIEFING: THREAT INTELLIGENCE
A REQUIREMENT FOR ISO 27001 CERTIFICATION

SKURIO

THE SKURIO CTI PLATFORM

Skurio wants to make threat intelligence accessible to everyone, no matter the IT budget. So, we are the perfect solution to address this new requirement, along with support from Skurio's analyst team. Skurio's CTI platform provides an IT team with a near real-time threat intelligence solution tailored for their business that curates information and data from multiple sources. We also offer in-app "ask an analyst" capabilities if you're not sure what to do next.

Our platform combines our extensive experience with data pulled from the surface, deep, and Dark Web, making threat intelligence more straightforward for businesses. Powerful search tools, analysis, and reporting capabilities give access to intelligence enriched with context immediately. Data visualisation and clear, actionable insights allow for faster research, leading to more rapid protection.

WHAT SHOULD THREAT INTELLIGENCE LOOK LIKE?

Relevant	Why has it been produced, and is it relevant to the organisation?
Insightful	Develop an understanding of the threat landscape.
Contextual	Who, what, where, why, when, how.
Actionable	Enhance the decision-making process.

THREAT INTELLIGENCE ACTIVITIES

Activities should include:

»	**Objectives**	ISO 27001 compliance, identify threats, mitigate threats, enhance the decision-making process.
»	**Identify Sources**	- Consider processing assets. Each has strengths and weaknesses - Review your requirements and objectives to determine sources - A collection plan may be needed and documented as evidence
»	**Processing Information**	1. Collate information for comparison 2. Evaluate reliability & accuracy of the information 3. Analysis & integration of information and intelligence 4. Interpret information and intelligence 5. Integrate information to produce intelligence product
»	**Analysing Information**	What does the information / intelligence mean?
»	**Communicating & Sharing**	- Apply basic principles: Brevity, Clarity & Relevance - An Intelligence product will have 3 elements: 1. Context: Description of source reporting. Statement of facts 2. Analyst comment: Facts or additional information which adds more detail to the source content 3. Analyst assessment: the interpretation, evaluation and assessment of the source content. Consider the evaluation of threat capabilities / limitations along with the likely Course of Action.

A threat intelligence solution will include the elements above along with analyst recommendations.