WHITEPAPER

Attivo NETWORKS®

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM AND THE ISO/IEC 27000 FAMILY OF STANDARDS

INTRODUCTION

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27000 family of standards helps organizations keep information assets secure. Using this family of standards helps an organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to the organization by third parties. ISO/IEC 27001 provides requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's information security requirements. ISO/IEC 27002 helps organizations to keep secure both their information assets and those of their customers. It offers organizations a wide selection of security controls, together with accompanying implementation guidance. It brings these controls together as a code of practice based on the controls that different many organizations commonly applied. Updated in 2013, ISO/IEC 27001 and 27002 are used together to help organizations secure both their information assets and those of their customers. More information about the standards are located at https://www.iso.org/isoiec-27001-information-security.html.

Deception technology is well-known for providing in-network threat detection, but less familiar is its ability to meet or support the guidance set forth by the ISO/IEC 27000 Family of Standards. Attivo Networks evaluated its capabilities in relation to ISO/IEC 27001 and 27002 and found that its ThreatDefend Platform provides extensive capabilities that meet the guidance set forth in the standard while supporting controls requirements to support the stated policy objectives.

ISO/IEC 27001 AND 27002

Most organizations have several information security controls. However, without an ISMS, controls can be somewhat disorganized and disjointed, often having been implemented as point solutions to specific situations or simply as a matter of convention. Business continuity planning and physical security may be managed quite independently of IT or information security. Meanwhile, Human Resources practices may make little reference to the need for defining and assigning information security roles and responsibilities throughout the organization. Note that ISO/IEC 27001 is designed to cover much more than just IT.

ISO/IEC 27001 requires that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

The certification auditor determines what controls will be tested as part of certification to ISO/IEC 27001 and can include any controls that the organization has deemed to be within the scope of the ISMS. The auditor can require testing to any depth necessary to assess whether the control has been implemented and that it is operating effectively.

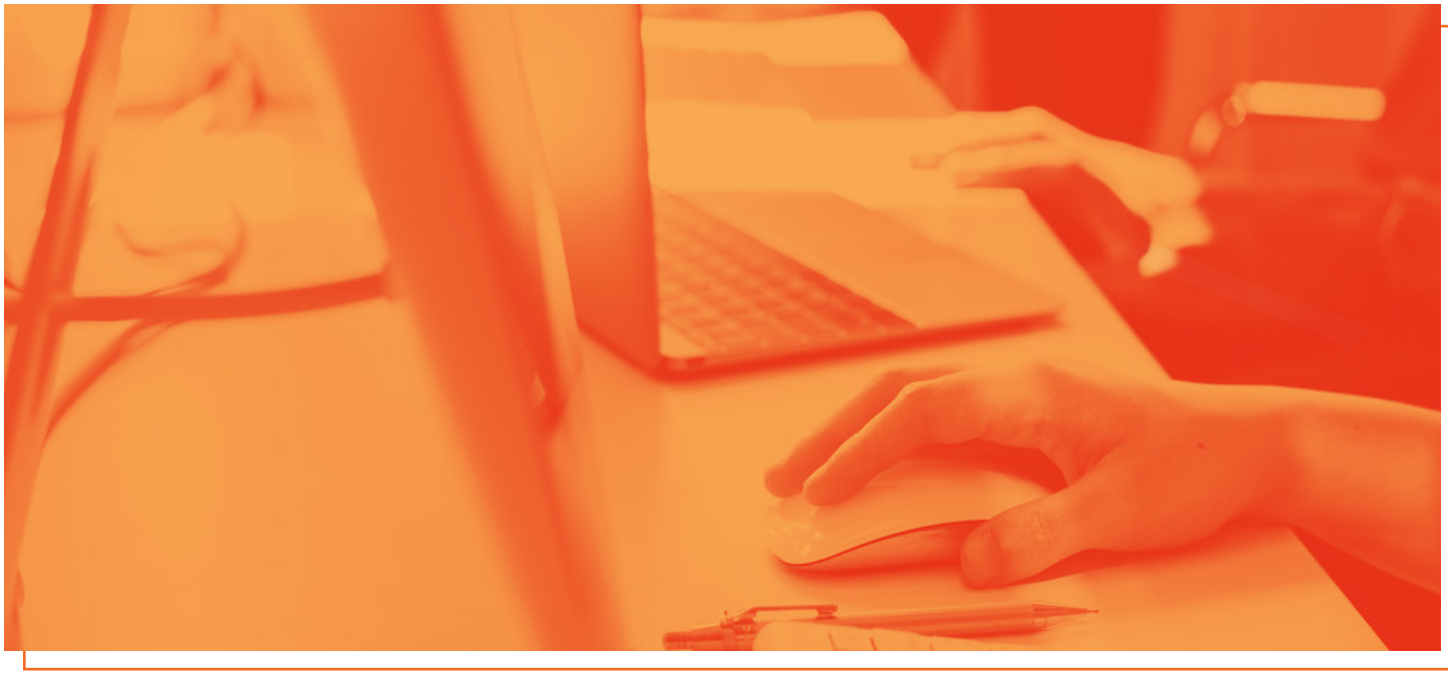
Other standards in the ISO/IEC 27000 family of standards provide additional guidance on certain aspects of designing, implementing and operating an ISMS, for example on information security risk management (ISO/IEC 27005).

ISO/IEC 27002 provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS).

The standard covers the following areas:

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and environmental security
- Operation security - procedures and responsibilities, protection from malware, backup, logging and monitoring, control of operational software, technical vulnerability management and information systems audit coordination
- Communication security - network security management and information transfer
- System acquisition, development, and maintenance - security requirements of information systems, Security in development and support processes and test data
- Supplier relationships - information security in supplier relationships and supplier service delivery delivery management
- Information security incident management - management of information security incidents and improvements
- Information security aspects of business continuity management - information security continuity and redundancies
- Compliance - compliance with legal and contractual requirements and information security reviews

Each section outlines and specifies best-practice information security controls and their objectives. For each of the controls, the section provides implementation guidance.



ATTIVO NETWORKS SUPPORT FOR THE ISO/IEC 27000 FAMILY OF STANDARDS

The Attivo Networks ThreatDefend™ Deception and Response Platform meets or supports 15 areas within the guidance set forth by the ISO/IEC 27000 Family of Standards. It is comprised of the Attivo BOTsink® Deception server, ThreatStrike™ Endpoint Deception Suite, ThreatPath™ visibility solution, DecoyDocs for data loss tracking, and ThreatOps™ Incident response playbooks. With the most comprehensive deception solution covering the widest attack surfaces, the ThreatDefend Platform efficiently and accurately detects attackers already inside the network, early in the attack cycle through network, endpoint, application, and data decoys. These deceptions are projected to user networks, datacenters, and specialized networks such as ICS-SCADA, IoT, or POS whether on premise, in the cloud, or at remote or branch offices. The platform automatically learns the environment and crafts mirror-match decoys and deception lures for the highest authenticity. The Attivo Networks solution is easy to deploy and operate, requiring little effort to manage while providing unparalleled visibility to available attack surfaces, exposed credentials, vulnerable misconfigurations, credential-based attacks, Man-in-the-Middle activity, Active Directory attacks, reconnaissance, and attacker lateral movement. It can detect known and unknown attacks with engagement-based, forensic-backed alerts that reduce mean-time-to-detect with high fidelity and accuracy while providing offense-based intelligence for a proactive defense. The platform's numerous third-party integrations reduce mean-time-to-respond, accelerating the incident response process.

In evaluating the ThreatDefend Platform against the ISO/IEC 27000 family of standards, Attivo Networks compared the solution with the published guidance in ISO/IEC 27001 and 27002. The following table lists the specific reference policies and controls, and how the ThreatDefend Platform meets or supports each one.

From these reference policies, the ThreatDefend Platform meets or supports the following 27 control requirements:

POLICIES	OBJECTIVES	CONTROL	ATTIVO CAPABILITY
RESPONSIBILITY FOR ASSETS			
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	The ThreatOps solution supports defining playbooks and rules based on acceptable information and asset use to detect violations of the organization's rules.
BUSINESS REQUIREMENTS FOR ACCESS CONTROL			
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	The ThreatDefend Platform alerts when access policies are violated.
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	The ThreatPath solution alert when access policies are violated.
USER ACCESS MANAGEMENT			
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	The ThreatPath solution rules alert when user access rights policies are violated.
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	The ThreatDefend platform monitors disabled cloud accounts and alerts when they are used.
USER RESPONSIBILITY			
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	The ThreatStrike suite generates an alert and identifies any user that attempts to use stolen credentials and violates the organization's best practices.
SYSTEM AND APPLICATION ACCESS CONTROL			
A.9. 4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	The ThreatDefend platform alerts when access policies are violated. The platform can also implant decoy documents that alert when information access happens beyond the restriction policies.

POLICIES	OBJECTIVES	CONTROL	ATTIVO CAPABILITY
PROTECTION FROM MALWARE			
A.12.2.1	Controls against malware	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	The ThreatDefend Platform can detect malware, lateral movement, and targeted attacks when they interact with a decoy system or attempt to spread to deceptive shares.
LOGGING AND MONITORING			
A.12. 4.1	Event logging	Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept and regularly reviewed.	The ThreatDefend platform logs all activity, engagement information, and faults and can send them to a SIEM.
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	The ThreatDefend platform protects all logs inside the BOTsink server, and can also send them to a SIEM or an ACM server for back up.
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	The ThreatDefend platform keeps an audit log of all user activities on the system.
A.12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	The ThreatDefend platform syncronizes time across all BOTsink servers and ACM servers for consistent event tracking.
TECHNICAL VULNERABILITY MANAGEMENT			
A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	The ThreatDefend platform can provide the full TTPs of an attack to showcase which vulnerability the attacker exploited. The ThreatDefend platform can also emulate specific CVEs to identify if an attacker is attempting to exploit it within the environment.
SECURITY REQUIREMENTS OF INFORMATION SYSTEMS			
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	The BOTsink server can present network decoys with deceptive services and decoy documents to detect unauthorized access.

POLICIES	OBJECTIVES	CONTROL	ATTIVO CAPABILITY
SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES			
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	The BOTsink server can deploy deceptive development server decoys, deceptive documents, and deceptive credentials in the development environment to detect activity that targets it.
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	The BOTsink server can deploy deceptive development server decoys, deceptive documents, and deceptive credentials in the contractor development environment and any other environment they can access to detect unauthorized activity. The BOTsink server can also deploy deceptive credentials that are beyond the development environment. This will alert if a contractor violates policy beyond development requirements.
INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS			
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	The ThreatDefend platform can be implemented on the supplier network, endpoints, and segments they are accessing to monitor for policy violations. This deception layer can be part of any agreement between the company and suppliers.
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	The ThreatDefend platform can be implemented on the supplier network, endpoints, and segments they are accessing to monitor for policy violations. This deception layer can be part of any agreement between the company and suppliers.

POLICIES	OBJECTIVES	CONTROL	ATTIVO CAPABILITY
INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS CONT.			
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	The ThreatDefend platform can be implemented on the supplier network, endpoints, and segments they are accessing to monitor for policy violations. This deception layer can be part of any agreement between the company and suppliers.
MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS			
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	The ThreatOps solution enables organizations to create orchestrated response playbooks that can feed information from one security technology to another for an efficient and quick response against any incident.
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	The ThreatDefend platform can disseminate information and reports automatically to appropriate management in real time.
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	The ThreatDefend platform enables the SOC analysts to easily hunt down vulnerabilities and weaknesses with the forensics information presented in the platform.
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	The ThreatDefend platform supports all processes and procedures through its visibility and detection functions. The ThreatOps solution can automate some response procedures through repeatable playbooks.

POLICIES	OBJECTIVES	CONTROL	ATTIVO CAPABILITY
MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS CONT.			
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.	The ThreatDefend platform automatically collects and catalogs all attacker activity withing the system to assist in hunting, remediation, and reporting of events.
INFORMATION SECURITY CONTINUITY			
A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation.	The ThreatDefend platform is a highly scalable and flexible solution that supports any process and can automate the deployment and enforcement of security controls.
REDUNDANCIES			
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	The BOTsink server supports LACP for high availability and continued coverage.
COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS			
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	The ThreatDefend platform protects all logs inside the BOTsink server, backs them up to the ACM server, and can also send them to a SIEM.

Deception Technology is a powerful threat detection mechanism that bridges gaps left open and exploitable by attackers when adversaries successfully penetrate a perimeter defense. By adding the Attivo Networks® ThreatDefend™ Platform to the security stack, organizations gain early and accurate eyes-inside-the-network visibility to attacks that either bypass existing controls or are perpetrated by malicious actors already inside the network while gaining capabilities that help them meet the guidance set forth by the ISO/IEC 27000 Family of Standards.

ABOUT ATTIVO NETWORKS

Attivo Networks® provides real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, IoT, and other specialized attack surfaces by deceiving an attacker into revealing themselves. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. For more information, visit www.attivonetworks.com.