A vertical decorative bar on the left side of the page, transitioning from red at the top to orange at the bottom.

# How Ivanti Maps to CIS Controls Version 8

## Table of Contents

Introduction: A Brief Overview of CIS	3
Using this document	3
Ivanti's Integrated Solutions	3
How Ivanti Solutions Map to CIS Controls Version 8	4
Ivanti-to-CIS Mapping Details	6
About Ivanti	19

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit [ivanti.com](https://www.ivanti.com)

## Introduction: A Brief Overview of CIS

The CIS Critical Security Controls are developed by the Center for Internet Security, intended to help organizations prevent and respond to cyberattacks. These CIS Controls are regularly updated and are meant to help organizations of all sizes and types improve their cybersecurity posture and resilience.<sup>1</sup>

This is why keeping pace with changes and updates to the CIS Controls is vital, and why the solutions implemented by an organization's IT and security teams should be as current as possible.

### Using this document

Ivanti's solutions packages are designed to help organizations identify and prioritize potential threats and vulnerabilities, protect their critical assets and data, detect and respond to threats and incidents and complete the cybersecurity cycle by recovering from attacks.

In this document, we map Ivanti's solutions to the latest CIS Controls Safeguards. This will help you assess how Ivanti solutions will enable you to fulfill CIS best practices.

### Ivanti's Integrated Solutions

Ivanti provides five integrated solutions to support an organization's cybersecurity posture:

- **Enterprise Service Management (ESM)** reduces costs, optimizes service performance and creates a secure, agile environment that is ready for the future.
- **Secure Unified Endpoint Management (SUEM)** provides a unified view of devices, enabling efficient discovery, management and security of endpoints and vulnerabilities with accurate and actionable insights to enable faster remediation.
- **Vulnerability Management and Response (VM&R)** lets you efficiently and effectively prioritize the vulnerabilities and weaknesses that pose your organization the most risk, enabling faster remediation and better protection against data breaches, ransomware and other cyberthreats.
- **Zero Trust Network Access (ZTNA)** secures remote access to the web, cloud services and private applications.
- **Cyber Asset Attack Surface Management (CAASM)** allows an organization to see all internal and external assets, identify and assess vulnerabilities and gaps in security controls and provide risk management with prioritization of vulnerabilities to quickly remediate threats.

## How Ivanti Solutions Map to CIS Controls Version 8

This table shows how each of Ivanti's five integrated solutions aligns with the 18 CIS Controls in Version 8.

Ivanti Solution/ CIS Critical Security Controls	1: Inventory and Control of Enterprise Assets	2: Inventory and Control of Software Assets	3: Data Protection	4: Secure Configuration of Enterprise Assets and Software	5: Account Management	6: Access Control Management	7: Continuous Vulnerability Management	8: Audit Log Management	9: Email and Web Browser Protections
<b>Enterprise Service Management (ESM)</b>	1.1, 1.3, 1.5	2.1, 2.2, 2.4	3.1, 3.5	4.1			7.1, 7.2		
<b>Secure Unified Endpoint Management (SUEM)</b>	1.1, 1.3, 1.5	2.1, 2.2, 2.3, 2.4, 2.5	3.6, 3.9, 3.10, 3.11	4.3, 4.4, 4.5, 4.11, 4.12		6.3			9.1, 9.2, 9.3
<b>Vulnerability Management &amp; Response (VM&amp;R)</b>							7.3, 7.4, 7.7		
<b>Zero Trust Network Access (ZTNA)</b>	1.1		3.10, 3.13, 3.14				7.5, 7.6, 7.7		9.2, 9.3
<b>Cyber Asset Attack Surface Management (CAASM)</b>	1.1, 1.3, 1.5						7.6		

Ivanti Solution/ CIS Critical Security Controls	10: Malware Defenses	11: Data Recovery	12: Network Infrastructure Management	13: Network Monitoring and Defense	14: Security Awareness and Skills Training	15: Service Provider Management	16: Application Software Security	17: Incident Response Management	18: Penetration Testing
Enterprise Service Management (ESM)		11.1				15.1, 15.2, 15.3, 15.5		17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9	
Secure Unified Endpoint Management (SUEM)	10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7			13.2			16.1		
Vulnerability Management & Response (VM&R)							16.1, 16.2, 16.5, 16.6		
Zero Trust Network Access (ZTNA)	10.5, 10.7		12.2, 12.7	13.5					
Cyber Asset Attack Surface Management (CAASM)									

These solutions offer a **comprehensive, unified approach to cybersecurity**, addressing the CIS Critical Security Controls and sub-controls best practices. With them, organizations can effectively and efficiently secure their critical systems, applications and data.

Ivanti always recommends a **multilayered defense-in-depth cybersecurity strategy** to mitigate today's threats. Simply, the solution is to place as many impediments as possible in front of cybercriminals, increasing the chance that they will give up.

## Ivanti-to-CIS Mapping Details

In-depth descriptions of how Ivanti solutions align with CIS Controls Version 8.

### CIS Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track and correct) all enterprise assets (end user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns with CIS Sub-Controls
<b>ESM and SUEM</b>	Discovery, Service Mapping, ITAM	<b>Ivanti Neurons for Discovery, Ivanti Neurons for Service Mapping</b> and <b>Ivanti Neurons for IT Asset Management (ITAM)</b> can each provide accurate real-time visibility of all of an organization's enterprise hardware assets connected to the corporate network, including end user devices, network devices, servers, IoT, OT and supply chain devices, using active and passive scanning methods to identify and manage assets. Connector integrations are available to ingest third-party data to provide a more comprehensive view, including unmanaged, shadow IT, BYOD, ghost and rogue devices. (Sub-Controls 1.1, 1.3, 1.5)
<b>ZTNA</b>	Policy Secure	<b>Ivanti Policy Secure</b> using <b>Profiler</b> provides full, detailed inventory and visibility into connected network devices, including shadow IT and unmanaged devices. (Sub-Control 1.1)
<b>CAASM</b>	EASM, Discovery	<b>Ivanti Neurons for External Attack Surface Management (EASM)</b> leverages <b>Ivanti Neurons for Discovery</b> to continuously discover all enterprise assets that can pose a threat to the enterprise, including unknown and unmanaged shadow IT devices. (Sub-Controls 1.1, 1.3, 1.5)



## CIS Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
ESM and SUEM	Discovery, Spend Intelligence, ITAM, MDM, MTD, Application Control	<p><b>Ivanti Neurons for Discovery</b> provides accurate real-time visibility of all an organization's enterprise software assets connected to the corporate network, including operating systems and applications, using active and passive scanning methods to identify and manage assets. Connector integrations are available to ingest third-party data to provide a more comprehensive view of assets, including unmanaged and unauthorized software. (Sub-Controls 2.1, 2.4)</p> <p><b>Ivanti Neurons for Spend Intelligence</b> ingests software assets discovery to provide a normalized, reconciled and deduplicated software inventory across all enterprise assets. Management of this software inventory enables an organization to understand licensed and unlicensed software and identify software that is end of life/end of support. (Sub-Controls 2.1, 2.2, 2.3)</p> <p><b>Ivanti Neurons for IT Asset Management (ITAM)</b> provides full asset lifecycle across enterprise assets, maintains the lifecycle of the asset and identifies and documents risks associated against the software. (Sub-Control 2.2)</p> <p><b>Ivanti Neurons for Modern Device Management (MDM), Ivanti Neurons for Mobile Threat Defense (MTD)</b> and <b>Ivanti Application Control</b> can permit or block installation of applications or block applications from executing if a threat is found on the device. (Sub-Controls 2.1, 2.2, 2.3, 2.4, 2.5)</p> <p>Ivanti Neurons for MTD is an add-on to Ivanti Neurons for MDM.</p>

## CIS Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain and dispose of data.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
ESM	ITSM, ITAM	<p><b>Ivanti Neurons for IT Service Management (ITSM)</b> and <b>Ivanti Neurons for IT Asset Management (ITAM)</b> allow an organization to establish and maintain data protection management processes, and through those processes address data sensitivity, data owner, handling of data, data retention limits and disposal requirements based on sensitivity and retention standards for the enterprise. They also let organizations review and update documentation annually (or when significant enterprise changes occur that could impact this safeguard) and document secure disposal of hardware devices (verified by appropriate certifications). (Sub-Controls 3.1, 3.5)</p>
SUEM	MDM, Ivanti Tunnel	<p><b>Ivanti Neurons for Unified Endpoint Management (UEM)</b> can enable, check and enforce file-based encryption on iOS, iPadOS and Android mobile devices and full-disk encryption using BitLocker for Windows and FileVault for macOS clients to protect data at rest. It can also enable WPA3-Personal (Simultaneous Authentication of Equals) and WPA3-Enterprise for wireless networks. <b>Ivanti Tunnel</b> supports Transport Layer Security (TLS) 1.2 cipher suites to protect sensitive data in transit. (Sub-Controls 3.6, 3.9, 3.10, 3.11)</p>
ZTNA	ICS, ZTA	<p><b>Ivanti Connect Secure (ICS)</b> implements the stronger cryptographic cipher suites with TLS version 1.3 to protect data in transit, along with enforcing:</p> <ul style="list-style-type: none"> <li>▪ User behavior, analytics and risk</li> <li>▪ Multi-factor and adaptive authentication and authorization</li> <li>▪ Device posture</li> <li>▪ Trusted application</li> <li>▪ Access context (location and time) controls</li> </ul> <p>(Sub-Control 3.10)</p> <p>Like ICS, <b>Ivanti Neurons for Zero Trust Access (ZTA)</b> encrypts data traffic, preventing snooping. Further, ZTA is a more potent solution than ICS as it eliminates general network access by connecting users directly with applications. (Sub-Controls 3.13, 3.14)</p>



## CIS Control 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
ESM	ITAM, CMDB	<b>Ivanti Neurons for IT Asset Management (ITAM)</b> can track and manage all enterprise assets through the configuration management database (CMDB), including data from the network, end user and cloud computing devices. (Sub-Control 4.1)
SUEM	UEM, MDM, UWM	<b>Ivanti Neurons for Unified Endpoint Management (UEM)</b> and <b>Ivanti Neurons for Modern Device Management (MDM)</b> can enforce a device lock for inactivity session timer for iOS/iPadOS, Android, Windows, macOS and Chrome OS endpoints. The application firewall can be configured for Windows and macOS devices. Managed enterprise-owned devices can be remotely wiped of enterprise data (via retire) when they are lost, stolen or when an individual leaves the company. Separate workspaces for personal and enterprise personas can be configured on iOS/iPadOS and macOS via User Enrollment, Android Enterprise via Work Profile and Windows via Windows Information Protection. (Sub-Controls 4.3, 4.5, 4.11, 4.12)  <b>Ivanti User Workspace Manager (UWM)</b> can configure and manage a firewall on servers. (Sub-Control 4.4)

## CIS Control 5: Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software. Ivanti does not offer a solution in this regard.

## CIS Control 6: Access Control Management

Use processes and tools to create, assign, manage and revoke access credentials and privileges for users, administrators and service accounts for enterprise assets and software.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
SUEM	MDM, Access, ZSO	<b>Ivanti Access</b> , using the <b>Ivanti Neurons for Modern Device Management (MDM)</b> client, can enforce strong multi-factor authentication (MFA) to access external cloud-based applications. <b>Ivanti Zero Sign-On (ZSO)</b> uses FIDO2 security keys or mobile device analogs to access all enterprise resources that can also be used in an MFA solution. It also supports single sign-on (SSO) functionality with MFA to cloud-based applications. Additionally, it supports federation between all common service providers and identity providers and allows access to cloud applications based on device compliance and conditional access rules. (Sub-Control 6.3)

## CIS Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure to remediate and minimize the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
ESM	ITSM, GRC, RBVM	<p><b>Ivanti Neurons for IT Service Management (ITSM), Ivanti Neurons for Governance, Risk and Compliance (GRC) and Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)</b> can establish and maintain a documented vulnerability management process for enterprise assets. Administrators can review and update documentation annually or when significant enterprise changes occur that could impact an organization.</p> <p>Together, they can also establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly or more frequent reviews. (Sub-Controls 7.1, 7.2)</p>
VM&R	RBVM, Patch Management	<p><b>Ivanti Neurons for Risk-Based Vulnerability Management (RBVM) and Ivanti Neurons for Patch Management</b> provide an end-to-end workflow driving from vulnerability risk identification to prioritization, assessment and patching for operating systems and applications. (Sub-Controls 7.3, 7.4, 7.7)</p>
ZTNA	ZTA + SSE	<p><b>Ivanti Neurons for Zero Trust Access (ZTNA)</b> with Lookout <b>Security Service Edge (SSE) (CASB and SWG)</b> continuously scans, assesses and responds to device risk. It also scores device risk based on running applications and processes, regardless of whether the asset is internal or external, and alerts based on dynamic access decisions for remediation. (Sub-Controls 7.5, 7.6, 7.7)</p>
CAASM	EASM	<p><b>Ivanti Neurons for External Attack Surface Management (EASM)</b> performs automated vulnerability scans of externally exposed enterprise assets and equips teams with the intelligence they need to assess their external attack surface from the adversary's perspective. (Sub-Control 7.6)</p>

## CIS Control 8: Audit Log Management

Collect, alert, review and retain audit logs of events that could help detect, understand or recover from an attack. Ivanti does not offer a solution in this regard.

## CIS Control 9: Email and Web Browser Protections

Improve protection and detection of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
SUEM	UEM, MDM, MTD	<p><b>Ivanti Neurons for Unified Endpoint Management (UEM)</b> and <b>Ivanti Neurons for Mobile Device Management (MDM)</b> using Application Control can ensure only approved web browsers and email clients can be used within the organization. Web content filter can enforce and update network-based URL filters to protect enterprise devices from connecting to malicious or unapproved websites. (Sub-Controls 9.1, 9.3)</p> <p><b>Ivanti Neurons for Mobile Threat Defense (MTD)</b> implements phishing and content protection and secure DNS to block an enterprise device's access to malicious domains and unapproved websites. (Sub-Controls 9.2, 9.3)</p> <p>Ivanti Neurons for MTD is an add-on to Ivanti Neurons for MDM.</p>
ZTNA	ZTA + SSE	<p><b>Ivanti Neurons for Zero Trust Access (ZTA)</b> with Lookout <b>Security Service Edge (SSE) (CASB and SWG)</b> provides secure access to the web, cloud services and private applications. It also provides full visibility into shadow IT and data usage to minimize the risk of data leaking to personal apps and public websites. (Sub-Controls 9.2, 9.3)</p>

## CIS Control 10: Malware Defenses

Prevent or control the installation, spread and execution of malicious applications, code or scripts on enterprise assets.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
SUEM	UEM, MTD	<p><b>Ivanti Neurons for Unified Endpoint Management (UEM)</b>'s antivirus functionality and <b>Ivanti Neurons for Mobile Threat Defense (MTD)</b> can centrally manage, deploy and maintain anti-malware software, configure automatic updates for signatures files, configure anti-malware software to automatically scan removable media and use behavior-based anti-malware software. (Sub-Controls 10.1, 10.2, 10.4, 10.6, 10.7)</p> <p>The device control feature of <b>Ivanti Neurons for Modern Device Management (MDM)</b> and <b>Ivanti Neurons for Unified Endpoint Management (UEM)</b> can disable autorun, autoplay and auto-execute functionality on removable media. (Sub-Control 10.3)</p> <p><b>Ivanti Neurons for Modern Device Management (MDM)</b> and <b>Ivanti Neurons for Mobile Threat Defense (MTD)</b> enable built-in anti-exploit (root, jailbreak and application security) features. (Sub-Control 10.5)</p> <p>Ivanti Neurons for MTD is an add-on to Ivanti Neurons for MDM.</p>
ZTNA	ZTA + SSE	<p><b>Ivanti Neurons for Zero Trust Access (ZTA)</b> with Lookout <b>Security Services Edge (SSE) (CASB and SWG)</b> protects users from internet threats such as malware, root/jailbreak detection and zero-day exploits with integrated advanced threat protection and user and entity behavior analytics (UEBA) to detect anomalies.</p> <p><b>Ivanti Connect Secure</b> can perform network isolation using remediation LAN. (Sub-Controls 10.5, 10.7)</p> <p>SSE is an add-on to Ivanti Neurons for ZTA.</p>

## CIS Control 11: Data Recovery

Establish and maintain data-recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
ESM	ITSM	<b>Ivanti Neurons for IT Service Management (ITSM)</b> can manage baselines of assets with the should-be state, compare to as-is state and flag variances. It can also manage and maintain the approved or pre-incident states as noted in the configuration management database (CMDB). (Sub-Control 11.1)

## CIS Control 12: Network Infrastructure Management

Establish, implement and actively manage (track, report, correct) network devices to prevent attackers from exploiting vulnerable network services and access points.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
ZTNA	ZTA, Policy Secure	<b>Ivanti Neurons for Zero Trust Access (ZTA)</b> and <b>Ivanti Policy Secure</b> establish and maintain a secure network infrastructure using a comprehensive solution for secure access and visibility to all networks and applications, protecting data and devices from malicious threats like viruses, malware and ransomware.  They can also enforce authentication to enterprise-managed VPN and authentication services before accessing enterprise resources for end user devices. (Sub-Controls 12.2, 12.7)

## CIS Control 13: Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
SUEM	MTD	<p><b>Ivanti Neurons for Mobile Threat Defense (MTD)</b> is a host-based intrusion detection system (IDS) and can block or quarantine a device if a threat is detected from the network. (Sub-Control 13.2)</p> <p>Ivanti Neurons for MTD is an add-on to Ivanti Neurons for MDM.</p>
ZTNA	ZTA + SSE	<p><b>Ivanti Neurons for Zero Trust Access (ZTA)</b> with Lookout <b>Security Service Edge (SSE) (CASB and SWG)</b> provides a comprehensive solution to manage access to remote access and visibility to all networks and applications, protecting data and devices from malicious threats like viruses, malware and ransomware. It also provides secure access to private, cloud and SaaS apps anytime, anywhere, with real-time security and traffic optimization for the best user experience. (Sub-Control 13.5)</p> <p>SSE is an add-on to Ivanti Neurons for ZTA.</p>

## CIS Control 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise. Ivanti does not offer a solution in this regard.



## CIS Control 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
ESM	ITSM, ITAM, GRC	<p><b>Ivanti Neurons for IT Service Management (ITSM)</b> and <b>Ivanti Neurons for IT Asset Management (ITAM)</b> can maintain an inventory of service providers through its vendor workspace as part of its vendor management capabilities. It can also manage underpinning contracts related to services provided by service providers and any security requirements related to those contracts.</p> <p>ITSM: (Sub-Controls 15.1, 15.2)</p> <p>ITAM: (Sub-Controls 15.3, 15.5)</p> <p><b>Ivanti Neurons for ITSM</b> and <b>Ivanti Neurons for ITAM</b> provide a supplier management module to document and manage providers across an organization. The supplier management solution manages contacts, vendor status, managed assets (if any), contracts, performance and scorecards. Contracts are managed against a vendor and cover types of contracts, scorecards, terms and conditions and can include security-specific information. (Sub-Controls 15.1, 15.2, 15.3, 15.5)</p> <p><b>Ivanti Neurons for Governance, Risk and Compliance (GRC)</b> manages suppliers against Authority documents. Controls ensure adherence to defined policies. Risk Assessments can also be run against a supplier to determine mitigated and unmitigated supplier risk. (Sub-Controls 15.2, 15.3, 15.4, 15.5)</p>

## CIS Control 16: Application Software Security

Manage the security life cycle of in-house developed, hosted or acquired software to prevent, detect and remediate security weaknesses before they can impact the enterprise.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
SUEM	incapptic Connect	<p><b>Ivanti incapptic Connect</b> employs a third-party application scanning service (Zimperium) to establish and maintain a secure application development process through the use of:</p> <ul style="list-style-type: none"> <li>▪ Secure application design standards</li> <li>▪ Secure coding practices</li> <li>▪ Developer training</li> <li>▪ Vulnerability management</li> <li>▪ Security of third-party code</li> <li>▪ Application security testing procedures</li> </ul> <p>(Sub-Control 16.1)</p>
VM&R	ASOC	<p><b>Ivanti Neurons for Application Security Orchestration &amp; Correlation (ASOC)</b> integrates with SAST, DAST, OSS and container scanners to manage the application vulnerabilities within an organization. These types of application scanners allow organizations to identify and resolve issues with code, OSS libraries, docker configurations and other application vulnerabilities and weaknesses.</p> <p><b>Ivanti Neurons for ASOC</b> also establishes and maintains a process to accept and address software vulnerabilities and establishes and maintains a severity-rating system and process for application vulnerabilities.</p> <p>(Sub-Controls 16.1, 16.2, 16.5, 16.6)</p>

## CIS Control 17: Incident Response Management

Establish a program to develop and maintain an incident-response capability (e.g., policies, plans, procedures, defined roles, training and communications) to prepare, detect and quickly respond to an attack.

Ivanti Solution(s)	Product(s)	How Ivanti Aligns With CIS Sub-Controls
ESM	SOM	<p><b>Ivanti Neurons for Security Operations Management (SOM)</b> can designate teams and team members to manage incidents, and also manage their roles and responsibilities related to the incident-management process.</p> <p>It can record contacts for incidents (including who logged the record and who needs to be notified regarding updates), set priority of the incident and establish communication mechanisms.</p> <p>It can also track and manage process documentation with approvals and review times and differentiate incident and event record types. Security incidents can be categorized as malware, data breach, phishing, vulnerability and others. (Sub-Controls 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9)</p>

## CIS Control 18: Penetration Testing

Test the effectiveness and resiliency of enterprise assets by identifying and exploiting weaknesses in controls (people, processes and technology) and by simulating the objectives and actions of an attacker. Ivanti does not offer a solution in this regard.


## About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive.

We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".

ivanti®

A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

For more information, or to contact Ivanti, please visit [ivanti.com](https://www.ivanti.com).