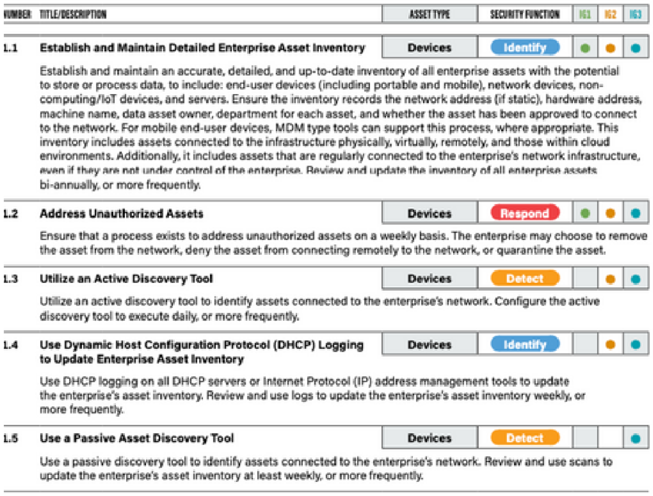
CompuNet

CYBERSECURITY SERVICES

CIS GAP ASSESSMENT

The Center for Information Security Gap Analysis (CIS Gap) is an interview style engagement reviewing an organization's tools, processes and procedures against the CIS controls framework. This engagement is performed during two phases: the interview process and the reporting process.

Security program posture data is collected during the interview process through team interviews and questionnaires. Data collected is trusted for integrity and not independently verified during this engagement. Findings and recommendations are presented during the reporting process, with actionable outcomes identified.



NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
1.1	**Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Devices	Identify	●	●	●
1.2	**Address Unauthorized Assets** Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Devices	Respond	●	●	●
1.3	**Utilize an Active Discovery Tool** Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	Devices	Detect		●	●
1.4	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory** Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	Devices	Identify		●	●
1.5	**Use a Passive Asset Discovery Tool** Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	Devices	Detect			●

WHAT WE DO

CompuNet takes pride in designing **tailored solutions** to solve complex problems. When tackling information security challenges, there is no one-size-fits-all approach. We combine **decades of experience** and published industry frameworks to provide an attainable security blueprint for our customers.

WHO WE ARE

CompuNet, Inc. is an **engineering-led** information technology solution provider that offers **consulting, design and implementation services** on-premise or in the cloud. Our engineering-led approach focuses on our clients' **business needs** and we architect solutions that solve business problems.

WORKSHOPS **ASSESSMENTS** **SERVICES**

www.compunetsecurity.com

help@compunet.biz

1-877-822-2841