# Using SecurityCenter CV for GDPR

## Where can technology help?

# Agenda

- Data controller vs Data processor
- Article 32
- How Tenable can help the DPO
- Information Security Frameworks
- SecurityCenter Continuous View for GDPR
  - Dashboards
  - Reports
  - PII
- Summary

tenable™

tenable™

# Data Controller vs Data Processor

# Data Controller vs Data Processor

## Data Controller

- Organisation or person who determines the purposes and method in which personal data is processed
- Includes organisations like retailers, medical centers, banks, law firms that collect data on their client

## Data Processor

- Organisation or person who processes data on behalf of the Data Controller
- Includes organisations like payroll companies, cloud storage providers, accounting firms
- All could hold or process data on behalf of another organisation

tenable™

# Article 32

- Defines security measures regarding the processing of personal data
- Provides specific measures that could be considered “appropriate to the risk”
- These include
  - Pseudonymisation and encryption
  - Ensure CIA and resilience of processing systems
  - Restoration of availability and access
  - Process for regular testing assessing and evaluating the measures implemented

tenable™

# How Tenable can help the DPO

# What is the DPO?

- Data Protection Officer
  - Roles and activities outlined in articles 37-39
  - Involved in the Data Protection Impact Assessment (DPIA) – Outlined in article 35
  - Primary purpose is to advise a Data Controller and Data Processor on compliance with the GDPR

# DPO requirements

- Perform assessments required for the security of hosts in order to verify compliance with the GDPR
- These assessments primarily fall into the areas of:
  - Host Discovery
  - Vulnerability Management
  - Compliance

- NOTE: This role is primarily advisory. Process definition lies with the DC, DP and the entire organisation, not the DPO alone.

tenable™

# How Tenable can help

- Information Security Framework
- Asset discovery and management
- Vulnerability Management
- Compliance and Audit reports
- PII in the clear

tenable™

tenable™

# Information Security Frameworks

# Information Security Frameworks

- The GDPR does not prescribe a particular framework
- However, adhering to a framework will make demonstrating compliance with Article 32 and Article 83 much more likely in the event of a breach

tenable™

# Frameworks of note

- ISO/IEC 27000
- Critical Security Controls for Effective Cyber Defense (CIS Controls)
- NIST 800-53 and 800-171

tenable™

# SecurityCenter Continuous View

# What is SecurityCenter CV?


## True Continuous Monitoring

SecurityCenter Continuous View® delivers a real-time, holistic view of all IT assets, network activity and events so you can find exploits and fix vulnerabilities faster.

tenable™

# Asset Discovery and Management

- Discover all assets on your network
  - Agent-based scanning
  - Active network scanners
  - Passive network monitors
- Classify and combine assets
  - Define your network
  - Automatically
  - Logically

tenable™

# Dashboards and ARCs

## ISO 27000

9 Assurance Report Cards (ARCs)

11 Dashboards

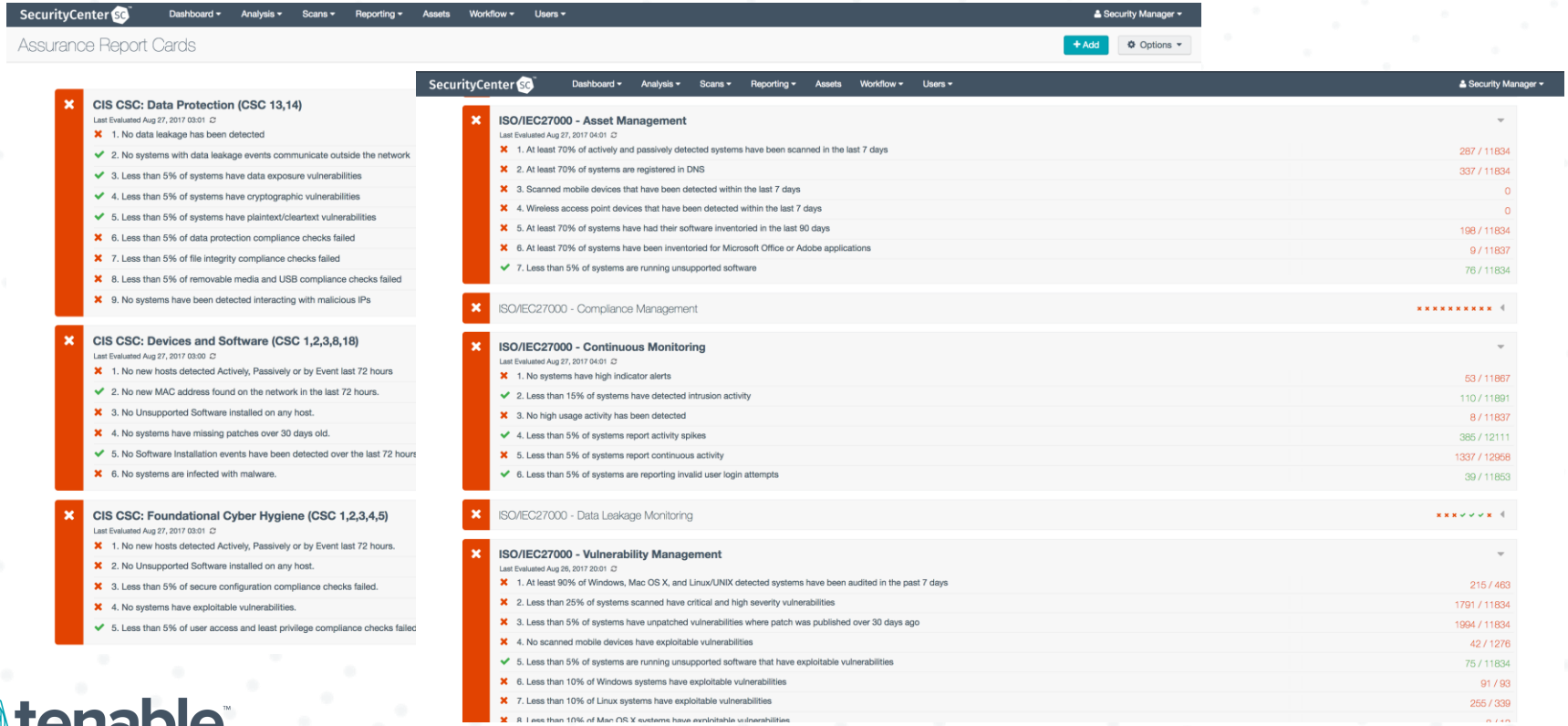
## CIS Controls

8 Assurance Report Cards (ARCs)

7 Dashboards

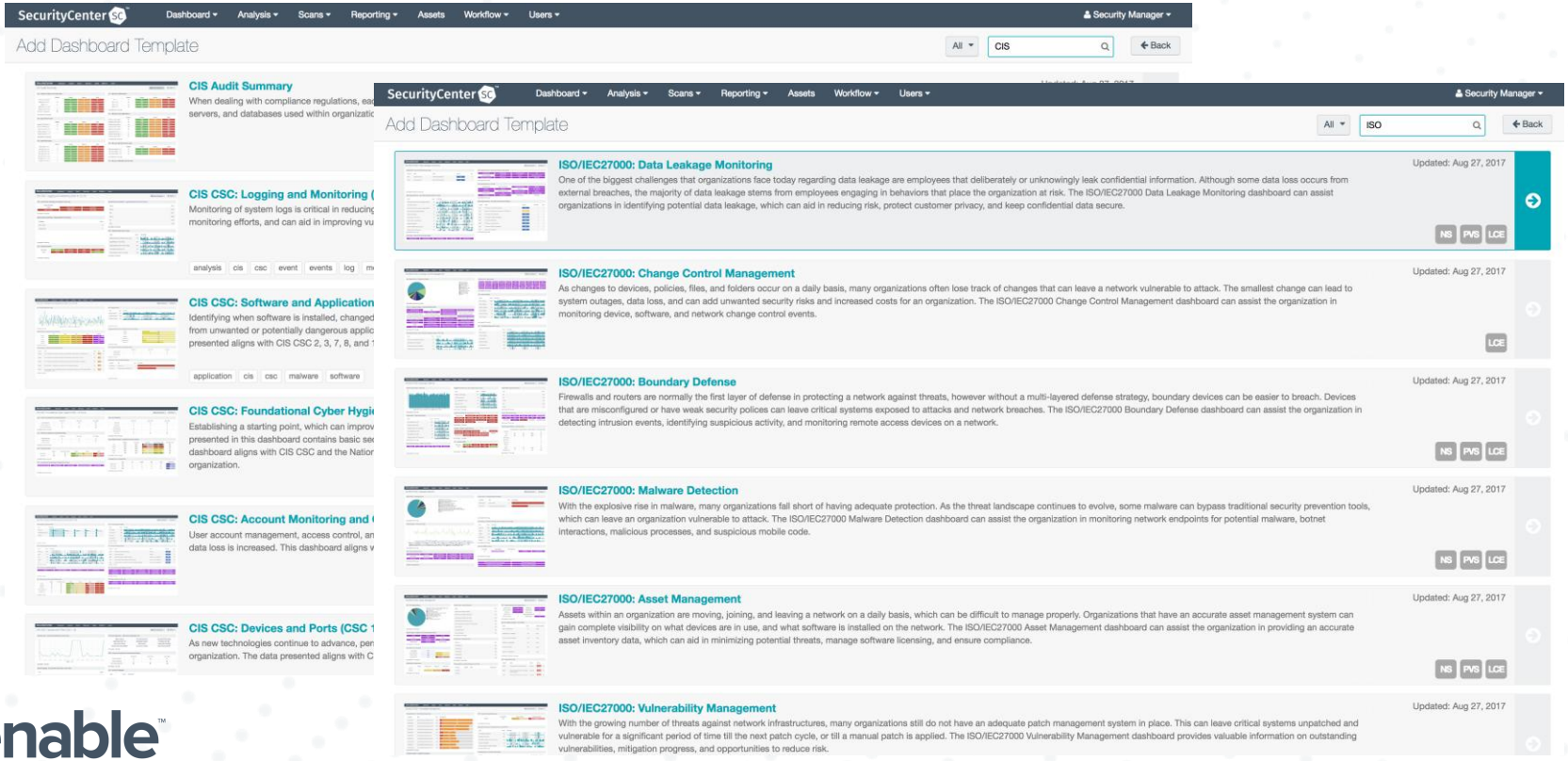
tenable™

# Framework Assurance Report Cards




tenable™

# Framework Dashboards




tenable™

# Framework Reports

- ISO27000 – Asset Management
  - Information on new and existing assets
- ISO27000 – Vulnerability Management
  - Current and recently fixed vulnerabilities
- ISO27000 – Compliance Management
  - Latest information on configuration compliance
- ISO27000 – Data Leakage
  - Variety of information to complement other DLP solutions

tenable™

# PII in the clear

- SecurityCenter CV allows you to scan typical file types for potential PII
  - National Insurance Numbers
  - Social Security Numbers (International)
  - Credit Card Numbers
  - SWIFT Details
  - Drivers license
  - More…

tenable™

# Summary

- Tenable SecurityCenter CV assists you in your GDPR endeavours in multiple ways
  - Offers multiple framework options to support GDPR activities
  - Comprehensive asset discovery and coverage
  - Out of the box framework analysis components (ARCs/Dashboards)
  - Multiple audit reports for compliance
  - Support and integration into other key systems

tenable™


tenable™