



# 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



# **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

# 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



# 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.

# How Tenable can help

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



# **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

# Frameworks of note

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



# 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.

# 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

# Dashboards and ARCs

## ISO 27000

9 Assurance Report  
Cards (ARCs)

11 Dashboards

## CIS Controls

8 Assurance Report  
Cards (ARCs)

7 Dashboards

# Framework Assurance Report Cards

SecurityCenter  Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾ Security Manager ▾

Assurance Report Cards + Add Options ▾

|                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>✗ CIS CSC: Data Protection (CSC 13,14)</b><br>Last Evaluated Aug 27, 2017 03:01  |
| ✗ 1. No data leakage has been detected                                                                                                                               |
| ✓ 2. No systems with data leakage events communicate outside the network                                                                                             |
| ✓ 3. Less than 5% of systems have data exposure vulnerabilities                                                                                                      |
| ✓ 4. Less than 5% of systems have cryptographic vulnerabilities                                                                                                      |
| ✓ 5. Less than 5% of systems have plaintext/cleartext vulnerabilities                                                                                                |
| ✗ 6. Less than 5% of data protection compliance checks failed                                                                                                        |
| ✗ 7. Less than 5% of file integrity compliance checks failed                                                                                                         |
| ✗ 8. Less than 5% of removable media and USB compliance checks failed                                                                                                |
| ✗ 9. No systems have been detected interacting with malicious IPs                                                                                                    |

|                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>✗ CIS CSC: Devices and Software (CSC 1,2,3,8,18)</b><br>Last Evaluated Aug 27, 2017 03:00  |
| ✗ 1. No new hosts detected Actively, Passively or by Event last 72 hours                                                                                                       |
| ✓ 2. No new MAC address found on the network in the last 72 hours.                                                                                                             |
| ✗ 3. No Unsupported Software installed on any host.                                                                                                                            |
| ✗ 4. No systems have missing patches over 30 days old.                                                                                                                         |
| ✓ 5. No Software installation events have been detected over the last 72 hours                                                                                                 |
| ✗ 6. No systems are infected with malware.                                                                                                                                     |

|                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>✗ CIS CSC: Foundational Cyber Hygiene (CSC 1,2,3,4,5)</b><br>Last Evaluated Aug 27, 2017 03:01  |
| ✗ 1. No new hosts detected Actively, Passively or by Event last 72 hours.                                                                                                           |
| ✗ 2. No Unsupported Software installed on any host.                                                                                                                                 |
| ✗ 3. Less than 5% of secure configuration compliance checks failed.                                                                                                                 |
| ✗ 4. No systems have exploitable vulnerabilities.                                                                                                                                   |
| ✓ 5. Less than 5% of user access and least privilege compliance checks failed                                                                                                       |

|                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SecurityCenter  Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾ <span>Security Manager ▾</span></b> |
| <b>✗ ISO/IEC27000 - Asset Management</b><br>Last Evaluated Aug 27, 2017 04:01                                               |
| ✗ 1. At least 70% of actively and passively detected systems have been scanned in the last 7 days                                                                                                            |
| ✗ 2. At least 70% of systems are registered in DNS                                                                                                                                                           |
| ✗ 3. Scanned mobile devices that have been detected within the last 7 days                                                                                                                                   |
| ✗ 4. Wireless access point devices that have been detected within the last 7 days                                                                                                                            |
| ✗ 5. At least 70% of systems have had their software inventoried in the last 90 days                                                                                                                         |
| ✗ 6. At least 70% of systems have been inventoried for Microsoft Office or Adobe applications                                                                                                                |
| ✓ 7. Less than 5% of systems are running unsupported software                                                                                                                                                |
| 287 / 11834                                                                                                                                                                                                  |
| 337 / 11834                                                                                                                                                                                                  |
| 0                                                                                                                                                                                                            |
| 0                                                                                                                                                                                                            |
| 198 / 11834                                                                                                                                                                                                  |
| 9 / 11837                                                                                                                                                                                                    |
| 76 / 11834                                                                                                                                                                                                   |

|                                                                                         |
|-----------------------------------------------------------------------------------------|
| <b>✗ ISO/IEC27000 - Compliance Management</b>                                           |
| *****  |

|                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>✗ ISO/IEC27000 - Continuous Monitoring</b><br>Last Evaluated Aug 27, 2017 04:01  |
| ✗ 1. No systems have high indicator alerts                                                                                                                           |
| ✓ 2. Less than 15% of systems have detected intrusion activity                                                                                                       |
| ✗ 3. No high usage activity has been detected                                                                                                                        |
| ✓ 4. Less than 5% of systems report activity spikes                                                                                                                  |
| ✗ 5. Less than 5% of systems report continuous activity                                                                                                              |
| ✓ 6. Less than 5% of systems are reporting invalid user login attempts                                                                                               |
| 53 / 11867                                                                                                                                                           |
| 110 / 11891                                                                                                                                                          |
| 8 / 11837                                                                                                                                                            |
| 385 / 12111                                                                                                                                                          |
| 1337 / 12658                                                                                                                                                         |
| 39 / 11853                                                                                                                                                           |

|                                                                                          |
|------------------------------------------------------------------------------------------|
| <b>✗ ISO/IEC27000 - Data Leakage Monitoring</b>                                          |
| ***✓✓✓  |

|                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>✗ ISO/IEC27000 - Vulnerability Management</b><br>Last Evaluated Aug 26, 2017 20:01  |
| ✗ 1. At least 90% of Windows, Mac OS X, and Linux/UNIX detected systems have been audited in the past 7 days                                                            |
| ✗ 2. Less than 25% of systems scanned have critical and high severity vulnerabilities                                                                                   |
| ✗ 3. Less than 5% of systems have unpatched vulnerabilities where patch was published over 30 days ago                                                                  |
| ✗ 4. No scanned mobile devices have exploitable vulnerabilities                                                                                                         |
| ✓ 5. Less than 5% of systems are running unsupported software that have exploitable vulnerabilities                                                                     |
| ✗ 6. Less than 10% of Windows systems have exploitable vulnerabilities                                                                                                  |
| ✗ 7. Less than 10% of Linux systems have exploitable vulnerabilities                                                                                                    |
| ✗ 8. Less than 10% of Mac OS X systems have exploitable vulnerabilities                                                                                                 |
| 215 / 463                                                                                                                                                               |
| 1791 / 11834                                                                                                                                                            |
| 1994 / 11834                                                                                                                                                            |
| 42 / 1276                                                                                                                                                               |
| 75 / 11834                                                                                                                                                              |
| 91 / 93                                                                                                                                                                 |
| 255 / 339                                                                                                                                                               |
| 0 / 0                                                                                                                                                                   |

# Framework Dashboards

SecurityCenter SC Dashboard Analysis Scans Reporting Assets Workflow Users Security Manager

Add Dashboard Template

All CIS Q Back

**CIS Audit Summary**

When dealing with compliance regulations, servers, and databases used within organization.

**CIS CSC: Logging and Monitoring (CSC 1)**

Monitoring of system logs is critical in reducing monitoring efforts, and can aid in improving vulnerability.

**CIS CSC: Software and Application (CSC 2, 3, 7, 8, and 10)**

Identifying when software is installed, changed from unwanted or potentially dangerous applications presented aligns with CIS CSC 2, 3, 7, 8, and 10.

**CIS CSC: Foundational Cyber Hygiene (CSC 1-10)**

Establishing a starting point, which can improve presented in this dashboard contains basic security dashboard aligns with CIS CSC and the NIST organization.

**CIS CSC: Account Monitoring and Management (CSC 1-10)**

User account management, access control, and data loss is increased. This dashboard aligns with CIS CSC 1-10.

**CIS CSC: Devices and Ports (CSC 1-10)**

As new technologies continue to advance, per organization. The data presented aligns with CIS CSC 1-10.

SecurityCenter SC Dashboard Analysis Scans Reporting Assets Workflow Users Security Manager

Add Dashboard Template

All ISO Q Back

**ISO/IEC27000: Data Leakage Monitoring**

Updated: Aug 27, 2017

One of the biggest challenges that organizations face today regarding data leakage are employees that deliberately or unknowingly leak confidential information. Although some data loss occurs from external breaches, the majority of data leakage stems from employees engaging in behaviors that place the organization at risk. The ISO/IEC27000 Data Leakage Monitoring dashboard can assist organizations in identifying potential data leakage, which can aid in reducing risk, protect customer privacy, and keep confidential data secure.

NS PVS LCE

**ISO/IEC27000: Change Control Management**

Updated: Aug 27, 2017

As changes to devices, policies, files, and folders occur on a daily basis, many organizations often lose track of changes that can leave a network vulnerable to attack. The smallest change can lead to system outages, data loss, and can add unwanted security risks and increased costs for an organization. The ISO/IEC27000 Change Control Management dashboard can assist the organization in monitoring device, software, and network change control events.

LCE

**ISO/IEC27000: Boundary Defense**

Updated: Aug 27, 2017

Firewalls and routers are normally the first layer of defense in protecting a network against threats, however without a multi-layered defense strategy, boundary devices can be easier to breach. Devices that are misconfigured or have weak security policies can leave critical systems exposed to attacks and network breaches. The ISO/IEC27000 Boundary Defense dashboard can assist the organization in detecting intrusion events, identifying suspicious activity, and monitoring remote access devices on a network.

NS PVS LCE

**ISO/IEC27000: Malware Detection**

Updated: Aug 27, 2017

With the explosive rise in malware, many organizations fall short of having adequate protection. As the threat landscape continues to evolve, some malware can bypass traditional security prevention tools, which can leave an organization vulnerable to attack. The ISO/IEC27000 Malware Detection dashboard can assist the organization in monitoring network endpoints for potential malware, botnet interactions, malicious processes, and suspicious mobile code.

NS PVS LCE

**ISO/IEC27000: Asset Management**

Updated: Aug 27, 2017

Assets within an organization are moving, joining, and leaving a network on a daily basis, which can be difficult to manage properly. Organizations that have an accurate asset management system can gain complete visibility on what devices are in use, and what software is installed on the network. The ISO/IEC27000 Asset Management dashboard can assist the organization in providing an accurate asset inventory data, which can aid in minimizing potential threats, manage software licensing, and ensure compliance.

NS PVS LCE

**ISO/IEC27000: Vulnerability Management**

Updated: Aug 27, 2017

With the growing number of threats against network infrastructures, many organizations still do not have an adequate patch management system in place. This can leave critical systems unpatched and vulnerable for a significant period of time till the next patch cycle, or till a manual patch is applied. The ISO/IEC27000 Vulnerability Management dashboard provides valuable information on outstanding vulnerabilities, mitigation progress, and opportunities to reduce risk.

# 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

# 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...

# 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

