Performing a Penetration Test (1 of 4)

- Performing a successful pen test involves *determination, resolve, and perseverance*
- A variety of actions take place when performing a pen test, however, they can be grouped into two phases:
  - Reconnaissance
  - Penetration

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Performing a Penetration Test (2 of 4)

- Phase 1: Reconnaissance
  - The first task is to perform preliminary information gathering from outside the organization (called **footprinting**)
  - Information can be gathered using two methods: **active reconnaissance** and **passive reconnaissance**
  - Active reconnaissance involves directly probing for vulnerabilities and useful information
    - **War driving** is searching for wireless signals from an automobile or on foot while using a portable device
    - **War flying** uses drones, which are officially known as **unmanned aerial vehicles** (**UAVs**)
  - A disadvantage of active reconnaissance is that the probes are likely to alert security professionals that something unusual is occurring

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Performing a Penetration Test (3 of 4)

- Phase 1: Reconnaissance (continued)
  - Passive reconnaissance occurs when the tester uses tools that do not raise any alarms
  - This may include searching online for publicly accessible information called **open source intelligence** (**OSINT**) that can reveal valuable insight about the system
- Phase 2: Penetration
  - A pen test is intended to simulate the actions of a threat actor
  - The initial system compromised usually does not contain the data that is the goal of the attack
  - That system usually serves as a gateway for entry into an organization network
  - Once inside the network, threat actors turn to other systems to be compromised until they reach the ultimate target

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Performing a Penetration Test (4 of 4)

- Phase 2: Penetration (continued)
  - Lessons to be learned from how threat actors work include:
    - When a vulnerability is discovered, the pen tester must determine how to pivot (turn) to another system using another vulnerability to continue moving toward the target
    - Vulnerabilities that are not part of the ultimate target can still provide a gateway to the target
    - Pen tests are manual, therefore, a pen tester needs to design attacks carefully
    - Pen testers must be patent and persistent, just like the threat actors

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Knowledge Check Activity 2

What are the two primary phases of penetration testing in order?

a. Penetration, escalation

b. Penetration, pivoting

c. Reconnaissance, footprinting

d. Reconnaissance, penetration

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Knowledge Check Activity 2: Answer

What are the two primary phases of penetration testing in order?

Answer: d. Reconnaissance, penetration

Reconnaissance is a necessary first phase because proper reconnaissance gathers the information needed to perform a proper penetration test. Reconnaissance is followed by the second phase; the actual attempt at penetration.

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Vulnerability Scanning

- **Vulnerability scanning** in some ways complements pen testing
- Studying vulnerability scanning involves understanding:
  - What it is
  - How to conduct a scan
  - How to use data management tools
  - How threat hunting can enhance scanning

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

What is a Vulnerability Scan?

- A penetration test is a single event using a manual process often performed only after a specific amount of time has passed
- A **vulnerability scan** is a frequent and ongoing process that continuously identifies vulnerabilities and monitors cybersecurity progress

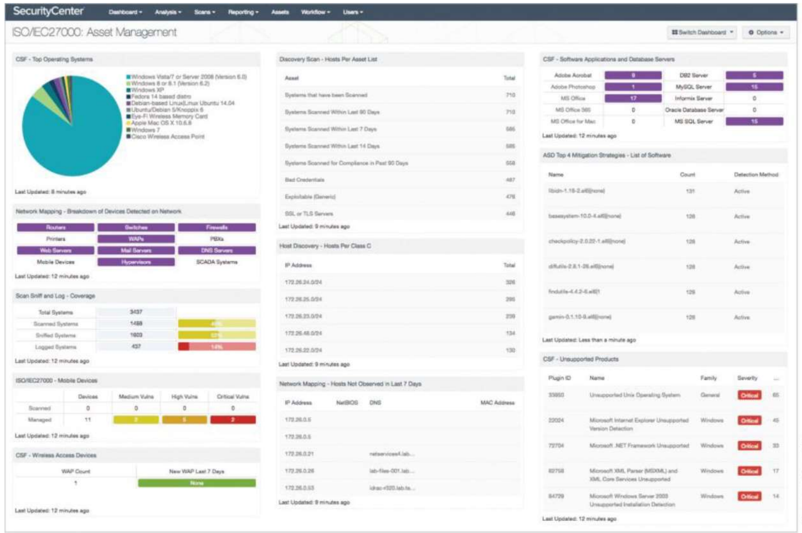
Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Conducting a Vulnerability Scan (1 of 6)

- Conducting a vulnerability scan involves:
  - Knowing what to scan and how often
  - Selecting a type of scan
  - Interpreting vulnerability information
- When and What to Scan
  - Two primary reasons for not conducting around-the-clock vulnerability scans:
    - *Workflow interruptions*
    - *Technical constraints*
  - A more focused approach is to know the location of data so that specific systems with high-value data can be scanned more frequently

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Conducting a Vulnerability Scan (2 of 6)


SecurityCenter
Dashboard ▾
Analysis ▾
Scans ▾
Reporting ▾
Assets
Workflow ▾
Users ▾
Switch Dashboard ▾
Options ▾
Windows Vista/7 or Server 2008 (Version 6.0)
Windows 8 or 8.1 (Version 6.2)
Windows XP
Fedora 14 based distro
Debian-based Linux|Linux Ubuntu 14.04
Ubuntu/Debian 5/Knoppix 6
Eye-Fi Wireless Memory Card
Apple Mac OS X 10.6.8
Windows 7
Cisco Wireless Access Point

ISO/IEC27000: Asset Management

CSF - Top Operating Systems

Last Updated: 8 minutes ago

Network Mapping - Breakdown of Devices Detected on Network

Routers	Switches	Firewalls
Printers	WAPs	PBXs
Web Servers	Mail Servers	DNS Servers
Mobile Devices	Hypervisors	SCADA Systems

Last Updated: 12 minutes ago

Scan Sniff and Log - Coverage

Total Systems	3437	
Scanned Systems	1488	[illegible]
Sniffed Systems	1803	[illegible]
Logged Systems	437	14%

Last Updated: 12 minutes ago

ISO/IEC27000 - Mobile Devices

	Devices	Medium Vulns	High Vulns	Critical Vulns
Scanned	0	0	0	0
Managed	11	2	5	2

Last Updated: 12 minutes ago

CSF - Wireless Access Devices

WAP Count	New WAP Last 7 Days
1	None

Last Updated: 12 minutes ago

Discovery Scan - Hosts Per Asset List

Asset	Total
Systems that have been Scanned	710
Systems Scanned Within Last 90 Days	710
Systems Scanned Within Last 7 Days	586
Systems Scanned Within Last 14 Days	585
Systems Scanned for Compliance in Past 90 Days	558
Bad Credentials	487
Exploitable (Generic)	478
SSL or TLS Servers	448

Last Updated: 9 minutes ago

Host Discovery - Hosts Per Class C

IP Address	Total
172.26.24.0/24	326
172.26.25.0/24	295
172.26.23.0/24	239
172.26.48.0/24	134
172.26.22.0/24	130

Last Updated: 9 minutes ago

Network Mapping - Hosts Not Observed in Last 7 Days

IP Address	NetBIOS	DNS	MAC Address
172.26.0.5			
172.26.0.5			
172.26.0.21		netservices4.lab...	
172.26.0.26		lab-files-001.lab...	
172.26.0.53		idrac-r320.lab.te...	

Last Updated: 9 minutes ago

CSF - Software Applications and Database Servers

Adobe Acrobat	9	DB2 Server	5
Adobe Photoshop	1	MySQL Server	15
MS Office	17	Informix Server	0
MS Office 365	0	Oracle Database Server	0
MS Office for Mac	0	MS SQL Server	15

Last Updated: 12 minutes ago

ASD Top 4 Mitigation Strategies - List of Software

Name	Count	Detection Method
libidn-1.18-2.el6[none]	131	Active
basesystem-10.0-4.el6[none]	128	Active
checkpolicy-2.0.22-1.el6[none]	128	Active
diffutils-2.8.1-28.el6[none]	128	Active
findutils-4.4.2-6.el6[1	128	Active
gamin-0.1.10-9.el6[none]	128	Active

Last Updated: Less than a minute ago

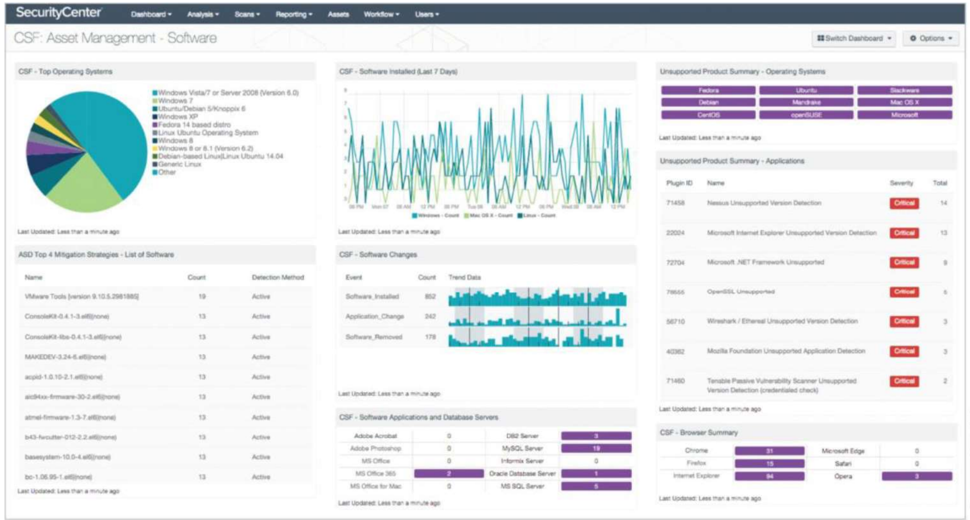
CSF - Unsupported Products

Plugin ID	Name	Family	Severity	...
33850	Unsupported Unix Operating System	General	Critical	65
22024	Microsoft Internet Explorer Unsupported Version Detection	Windows	Critical	45
72704	Microsoft .NET Framework Unsupported	Windows	Critical	33
82758	Microsoft XML Parser (MSXML) and XML Core Services Unsupported	Windows	Critical	17
84729	Microsoft Windows Server 2003 Unsupported Installation Detection	Windows	Critical	14

Last Updated: 12 minutes ago

Source: Tenable

Figure 2-4 Nessus hardware asset management



CSF: Asset Management - Software

CSF - Top Operating Systems

Last Updated: Less than a minute ago

ASD Top 4 Mitigation Strategies - List of Software

Name	Count	Detection Method
VMware Tools [version 9.10.5.2981885]	19	Active
ConsoleKit-0.4.1-3.el6[none]	13	Active
ConsoleKit-libs-0.4.1-3.el6[none]	13	Active
MAKEDEV-3.24-6.el6[none]	13	Active
acpid-1.0.10-2.1.el6[none]	13	Active
aic94xx-firmware-30-2.el6[none]	13	Active
atmel-firmware-1.3-7.el6[none]	13	Active
b43-fwcutter-012-2.2.el6[none]	13	Active
basesystem-10.0-4.el6[none]	13	Active
bc-1.06.95-1.el6[none]	13	Active

Last Updated: Less than a minute ago

CSF - Software Installed (Last 7 Days)

Last Updated: Less than a minute ago

CSF - Software Changes

Event	Count	Trend Data
Software_Installed	852	
Application_Change	242	
Software_Removed	178	

Last Updated: Less than a minute ago

CSF - Software Applications and Database Servers

Adobe Acrobat	0	DB2 Server	3
Adobe Photoshop	0	MySQL Server	19
MS Office	0	Informix Server	0
MS Office 365	2	Oracle Database Server	1
MS Office for Mac	0	MS SQL Server	5

Last Updated: Less than a minute ago

Unsupported Product Summary - Operating Systems

Fedora	Ubuntu	Slackware
Debian	Mandrake	Mac OS X
CentOS	openSUSE	Microsoft

Last Updated: Less than a minute ago

Unsupported Product Summary - Applications

Plugin ID	Name	Severity	Total
71458	Nessus Unsupported Version Detection	Critical	14
22024	Microsoft Internet Explorer Unsupported Version Detection	Critical	13
72704	Microsoft .NET Framework Unsupported	Critical	9
78555	OpenSSL Unsupported	Critical	5
56710	Wireshark / Ethereal Unsupported Version Detection	Critical	3
40362	Mozilla Foundation Unsupported Application Detection	Critical	3
71460	Tenable Passive Vulnerability Scanner Unsupported Version Detection (credentialed check)	Critical	2

Last Updated: Less than a minute ago

CSF - Browser Summary

Chrome	31	Microsoft Edge	0
Firefox	15	Safari	0
Internet Explorer	94	Opera	3

Last Updated: Less than a minute ago

Source: Tenable

Figure 2-5 Nessus software asset management

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Conducting a Vulnerability Scan (3 of 6)

- Because a vulnerability scan should be limited, a configuration review of software settings should be conducted
  - Define the group of target devices to be scanned
  - Ensure that a scan should be designed to meet its intended goals
  - Determine the sensitivity level or the depth of a scan
  - Specify the data types to be scanned

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Conducting a Vulnerability Scan (4 of 6)

- Types of Scans
  - Two major types of scans are credentialed scans and intrusive scans
  - In a **credentialed scan**, valid authentication credentials are supplied to the vulnerability scanner to mimic the work of a threat actor who possesses these credentials
  - A **non-credentialed scan** provides no such authentication information
  - An **intrusive scan** attempts to employ any vulnerabilities that it finds
  - A **nonintrusive scan** does not attempt to exploit the vulnerability but only records that it was discovered
- Vulnerability Information
  - Vulnerability scanning software compares the software it scans against a set of known vulnerabilities
  - Vulnerability information is available to provide updated information to scanning software about the latest vulnerabilities

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Conducting a Vulnerability Scan (5 of 6)

- Examining Results
  - When examining the results of a vulnerability scan, you should assess the importance of vulnerability as well as its accuracy
  - Questions that may help identify which vulnerability needs early attention:
    - Can the vulnerability be addressed in a reasonable amount of time?
    - Can the vulnerability be exploited by an external threat actor?
    - If the vulnerability led to threat actors infiltrating the system, would they be able to pivot to more important systems?
    - Is the data on the affected device sensitive or is it public?
    - Is the vulnerability on a critical system that runs a core business process?
  - Another part of prioritizing is making sure that the difficulty and time for implementing the correction is reasonable

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Conducting a Vulnerability Scan (6 of 6)

- Examining Results (continued)
  - Another consideration when examining results is accuracy
  - Be sure to identify **false positives**, which is an alarm raised when there is no problem
  - A means to identify false positives is to correlate the vulnerability scan data with several internal data points
    - Most common are related to log files
    - **Log reviews**, or an analysis of log data, can be used to identify false positives

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

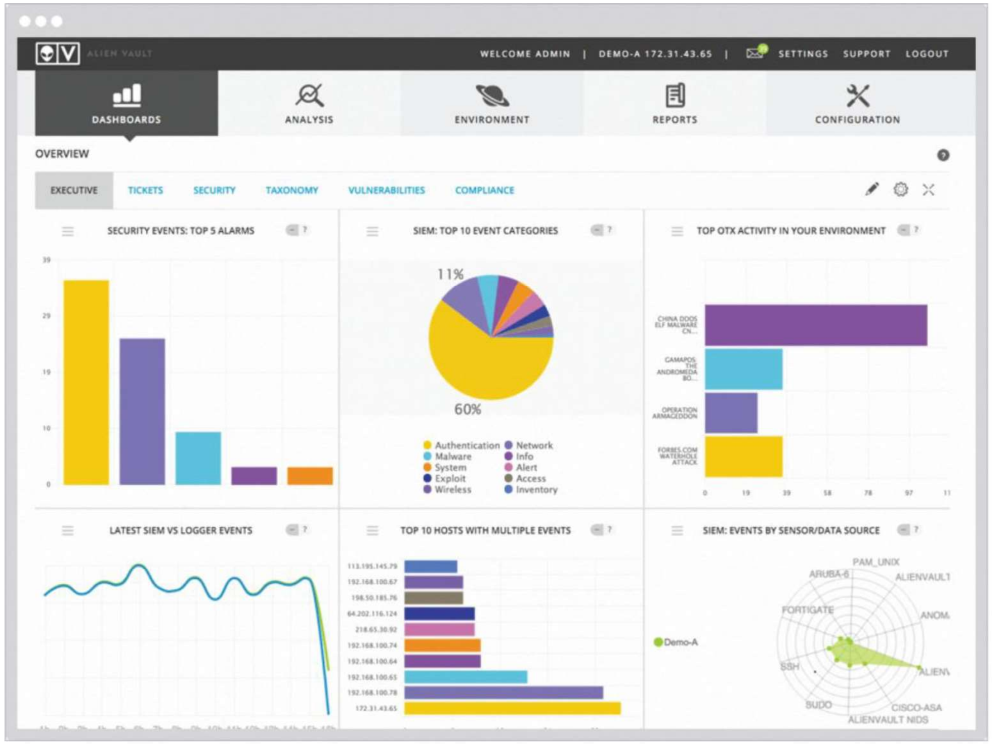
Data Management Tools (1 of 3)

- Two data management tools are used for collecting and analyzing vulnerability scan data:
  - **Security Information and Event Management (SIEM)**
  - **Security Orchestration, Automation, and Response (SOAR)**
- Security Information and Event Management (SIEM)
  - A SIEM typically has the following features:
    - *Aggregation*
    - *Correlation*
    - *Automated alerting and triggers*
    - *Time synchronization*
    - *Event duplication*
    - *Logs*

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Data Management Tools (2 of 3)



Source: Alien Vault

Figure 2-8 SIEM dashboard

Figure 2-8 SIEM dashboard

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Data Management Tools (3 of 3)

- SIEMS can also perform **sentiment analysis**, which is the process of computationally identifying and categorizing opinions to determine the writer’s attitude toward a particular topic
  - Sentiment analysis has been used when tracking postings threat actors make in discussion forums with other attackers to better determine the behavior and mindset of threat actors
- Security Orchestration, Automation, and Response (SOAR)
  - A SOAR is similar to a SIEM in that it is designed to help security teams manage and respond to security warnings and alarms
  - SOARs combine more comprehensive data gathering and analytics to automate incident responses

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Threat Hunting

- **Threat hunting** is proactively searching for cyber threats that thus far have gone undetected in a network
  - It begins with a critical premise: *threat actors have already infiltrated our network*
  - It proceeds to find unusual behavior that may indicate malicious activity
- Threat hunting investigations often use crowdsourced attack data such as:
  - Advisories and bulletins
  - Cybersecurity **threat feeds –** data feeds of information on the latest threats
  - Information from a **fusion center –** a formal repository of information from enterprises and the government used to share information on the latest attacks

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Knowledge Check Activity 3

Which of the following is NOT typically a feature of a SIEM?

a. Aggregation
b. Remediation
c. Correlation
d. Event duplication

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Knowledge Check Activity 3: Answer

Which of the following is NOT typically a feature of a SIEM?

Answer: b. Remediation

The typical features found in a SIEM are aggregation, correlation, automated triggers and alerts, time synchronization, event duplication, and logs. A SIEM provides analysis and reporting but does not commonly provide remediation of security events.

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Cybersecurity Resources

- External cybersecurity resources are available to organizations:
  - Frameworks
  - Regulations
  - Legislation
  - Standards
  - Benchmarks/secure configuration guides
  - Information sources

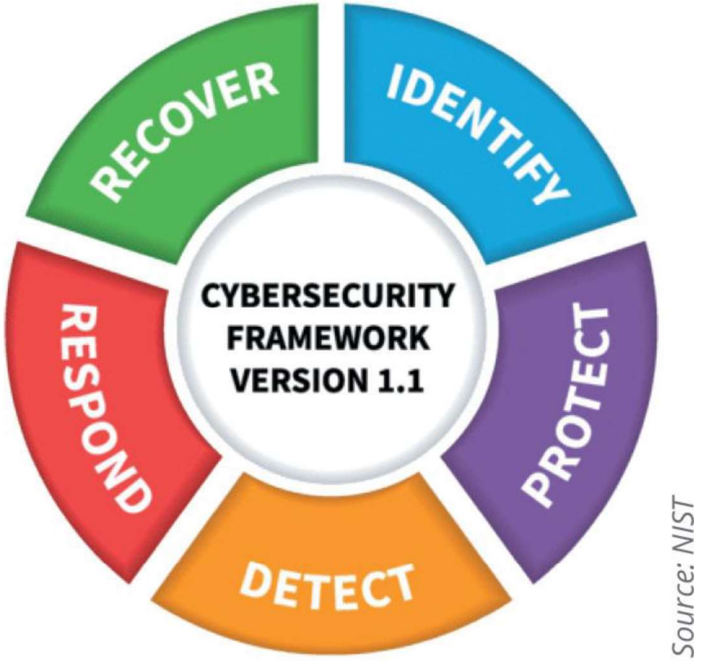
Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Frameworks (1 of 3)

- A **cybersecurity framework** is a series of documented processes used to define policies and procedures for implementing and managing security controls in an enterprise environment
- The most common frameworks are from the:
  - National Institute of Standards and Technology (NIST)
  - International Organization for Standardization (ISO)
  - American Institute of Certified Public Accountants (AICPA)
  - Center for Internet Security (CIS)
  - Cloud Security Alliance (CSA)

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Frameworks (3 of 3)



Source: NIST

Figure 2-9 NIST Cybersecurity Framework (CSF) functions

Figure 2-9 NIST Cybersecurity Framework (CSF) functions

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Regulations

- The process of adhering to regulations is called *regulatory compliance*
- **Industry regulations** are typically developed by established professional organizations or government agencies using the expertise of seasoned security professionals
- Sample of cybersecurity regulations categories:
  - *Broadly applicable regulations*
  - *Industry-specific regulations*
  - *U.S. state regulations*
  - *International regulations*

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Legislation

- Specific legislation can also be enacted by governing bodies
  - These include national, territorial, and state laws
- Due to a lack of comprehensive federal regulations for data breach notification, many states have amended their breach notification laws from the basic definitions
  - No two state laws are the same

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Standards

- A standard is a document approved through consensus by a recognized standardization body
    - It provides for framework, rules, guidance, or characteristics for products or related processes and production methods
- One cybersecurity standard is the Payment Card Industry Data Security Standard (PCI DSS)

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Benchmarks/Secure Configuration Guides

- **Benchmark/secure configuration guides** are usually distributed by hardware manufacturers and software developers
  - They serve as guidelines for configuring a device or software so that it is resilient to attacks
- Usually, they are usually **platform/vendor-specific guides** that only apply to specific products
- Guides are available for:
  - Network infrastructure devices
  - OSs
  - Web servers
  - Application servers

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Information Sources

- There are a variety of information sources including:
  - Vendor websites
  - Conferences
  - Academic journals
  - Local industry groups
  - Social media
- A specialized research source is a **Request for comments** (**RFC**)
  - Which are white papers documents that are authored by technology bodies employing specialists, engineers, and scientists who are experts in their field

CENGAGE

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition. © 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.