EC-Council

Certified Network Defender

The Ultimate Certification for Network Administrators

EC-Council

THE WORLD IS BECOMING INCREASING INSECURE

SECURING NETWORKS IS A CRITICAL ISSUE

ABOUT CND CERTIFICATION

CND DESIGN APPROACH

CND COMPARISONS

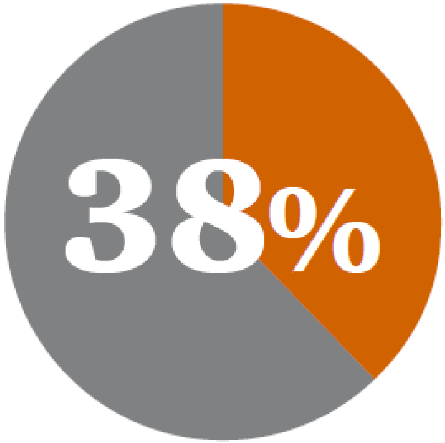
MARKETING PROGRAM

THE WORLD IS BECOMING INCREASING INSECURE

The Global State of Information Security Survey 2016

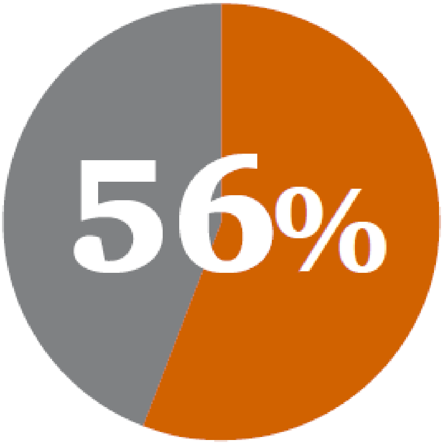
C|ND Certified Network Defender

Average number of security incidents



In 2015, **38%** more security incidents were detected than in 2014.

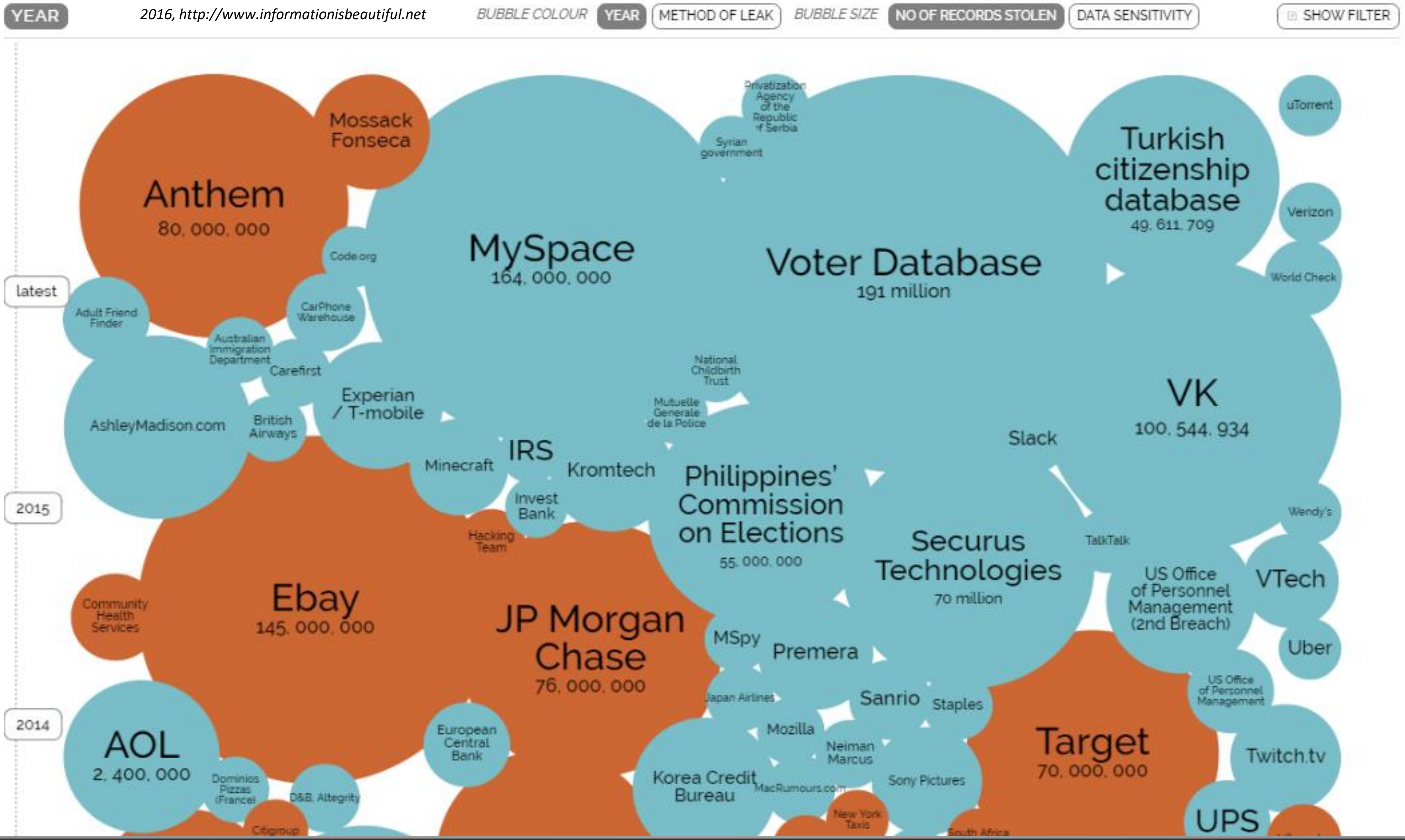
Impacts of security incidents



Theft of "hard" intellectual property increased **56%** in 2015.

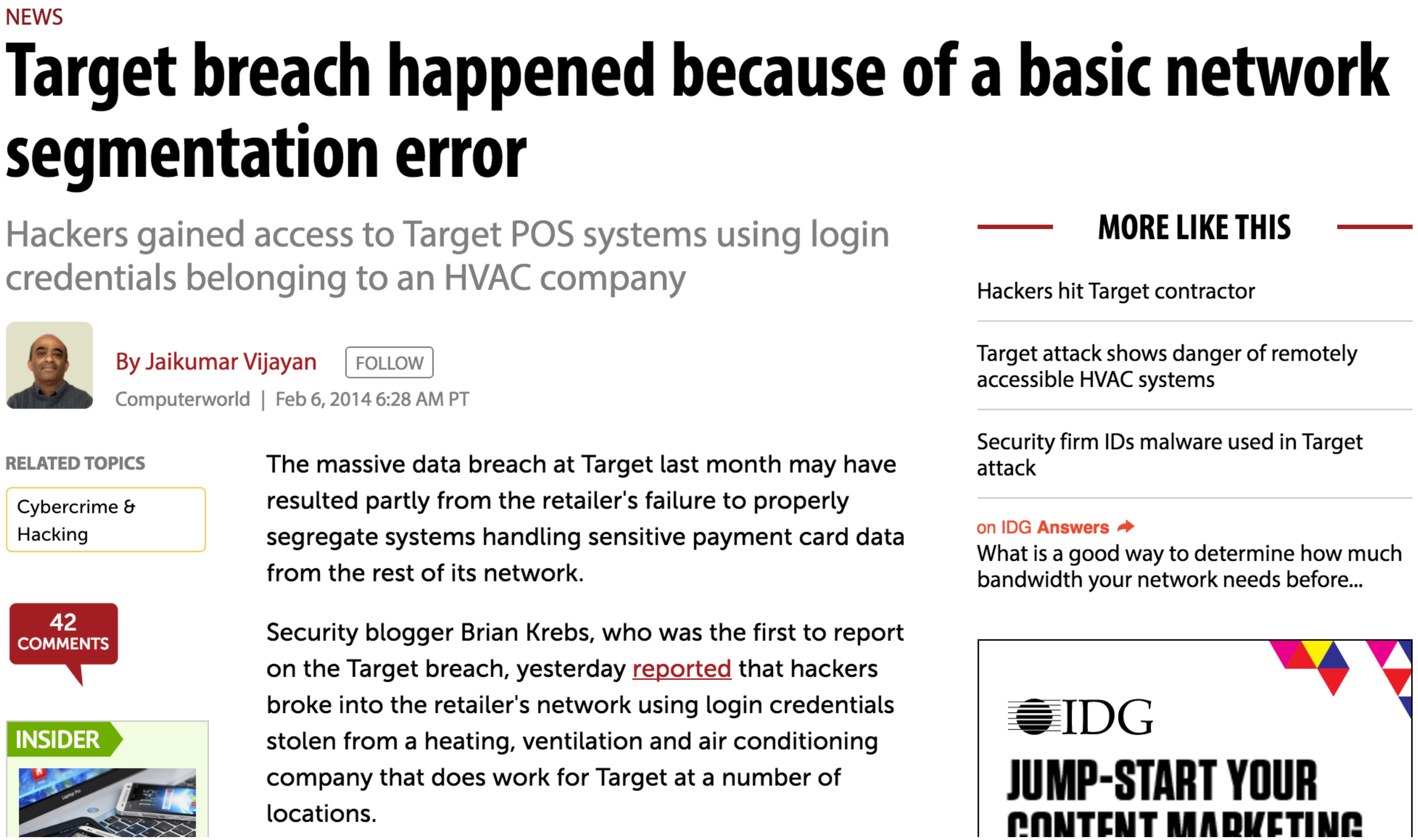
2016, http://www.pwc.com

Network Security Concerns:
World's Biggest Data Breaches



2016, http://www.informationisbeautiful.net

How Target Breach Happened?



NEWS

Target breach happened because of a basic network segmentation error

Hackers gained access to Target POS systems using login credentials belonging to an HVAC company

By Jaikumar Vijayan FOLLOW

Computerworld | Feb 6, 2014 6:28 AM PT

RELATED TOPICS

Cybercrime & Hacking

42 COMMENTS

INSIDER

The massive data breach at Target last month may have resulted partly from the retailer's failure to properly segregate systems handling sensitive payment card data from the rest of its network.

Security blogger Brian Krebs, who was the first to report on the Target breach, yesterday reported that hackers broke into the retailer's network using login credentials stolen from a heating, ventilation and air conditioning company that does work for Target at a number of locations.

MORE LIKE THIS

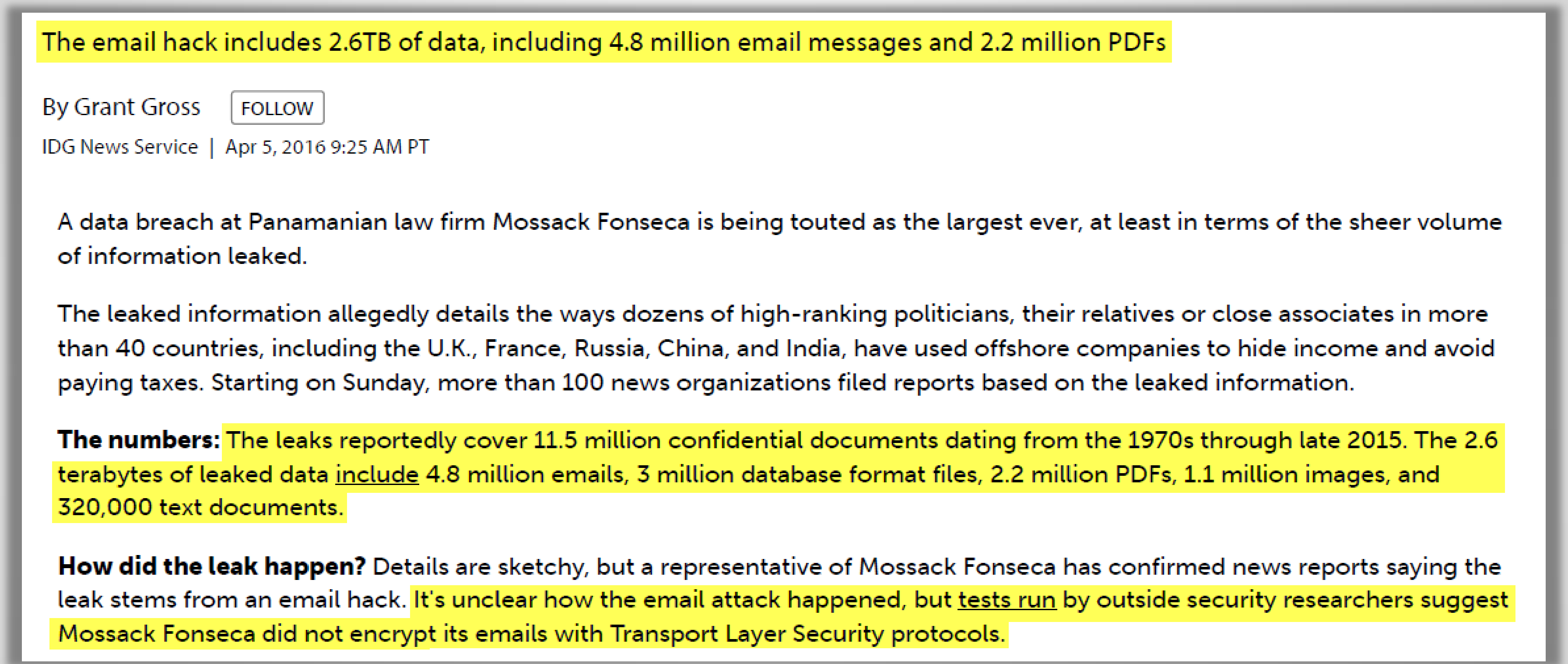
- Hackers hit Target contractor
- Target attack shows danger of remotely accessible HVAC systems
- Security firm IDs malware used in Target attack

on IDG Answers

What is a good way to determine how much bandwidth your network needs before...

2014, http://www.computerworld.com

The Security Flaws at the Heart of the Panama Papers



The email hack includes 2.6TB of data, including 4.8 million email messages and 2.2 million PDFs

By Grant Gross FOLLOW

IDG News Service | Apr 5, 2016 9:25 AM PT

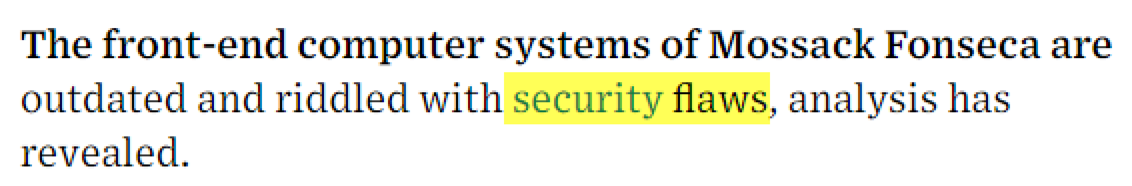
A data breach at Panamanian law firm Mossack Fonseca is being touted as the largest ever, at least in terms of the sheer volume of information leaked.

The leaked information allegedly details the ways dozens of high-ranking politicians, their relatives or close associates in more than 40 countries, including the U.K., France, Russia, China, and India, have used offshore companies to hide income and avoid paying taxes. Starting on Sunday, more than 100 news organizations filed reports based on the leaked information.

The numbers: The leaks reportedly cover 11.5 million confidential documents dating from the 1970s through late 2015. The 2.6 terabytes of leaked data include 4.8 million emails, 3 million database format files, 2.2 million PDFs, 1.1 million images, and 320,000 text documents.

How did the leak happen? Details are sketchy, but a representative of Mossack Fonseca has confirmed news reports saying the leak stems from an email hack. It's unclear how the email attack happened, but tests run by outside security researchers suggest Mossack Fonseca did not encrypt its emails with Transport Layer Security protocols.

2016, http://www.computerworld.com



The front-end computer systems of Mossack Fonseca are outdated and riddled with security flaws, analysis has revealed.

2016, http://www.wired.co.uk

2016 Network Protection Survey

“We control the electrical grid for 13 states. When the grid goes down it affects millions of people. In some cases it is a life and death issue. Without a doubt, network protection is really, really important to us.”

– **Network Analyst,** Major Public Utility, Northeastern United States

Networks, more than ever, are at the core of the enterprise. Analysts estimate the cost of a typical unplanned network outage now tops $740,000[1]. Protecting the network – from problems like breaches, outages and poor performance – is crucial for organizations.

- Ponemon Institute 2016 report Cost of Data Center Outages

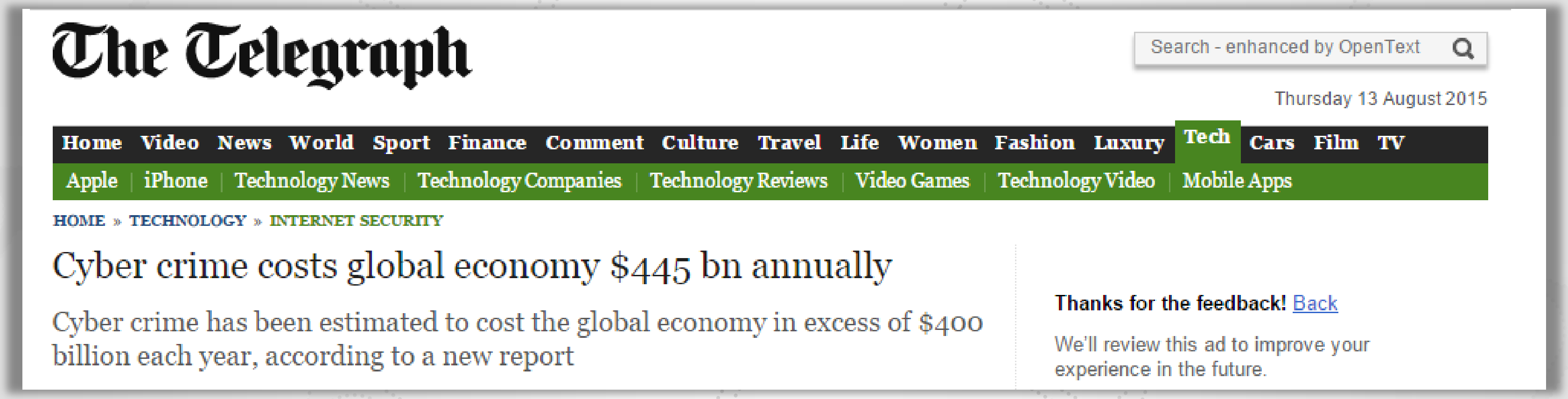
Infoblox wanted to explore how organizations are protecting and managing their networks in today’s chaotic world. We commissioned ReRez Research of Dallas, Texas, to survey 200 large organizations to discover network protection best practices and how adherence to these industry best practices affect eventual outcomes.

We were able to discover precisely what the very best organizations were doing to protect and manage their networks, and how these practices affected their outcomes. From this, we are able to make five recommendations for organizations trying to protect their networks in today’s complex and chaotic world.

2016, https://www.infoblox.com

Cyber Crime Costs

Cyber Crime Costs Projected to Reach $2 Trillion by 2019

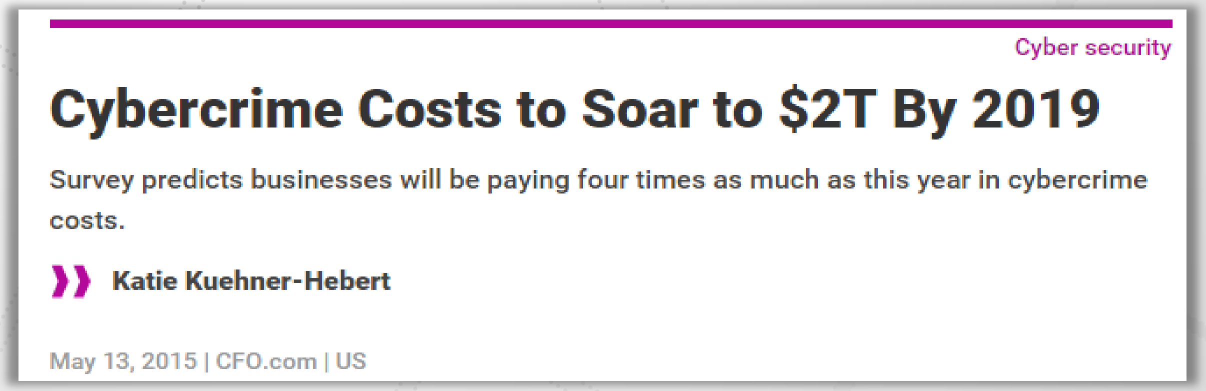

The Telegraph
Search - enhanced by OpenText
Thursday 13 August 2015
Home Video News World Sport Finance Comment Culture Travel Life Women Fashion Luxury Tech Cars Film TV
Apple | iPhone | Technology News | Technology Companies | Technology Reviews | Video Games | Technology Video | Mobile Apps
HOME » TECHNOLOGY » INTERNET SECURITY

Cyber crime costs global economy $445 bn annually

Cyber crime has been estimated to cost the global economy in excess of $400 billion each year, according to a new report

Thanks for the feedback! Back

We'll review this ad to improve your experience in the future.



Cybercrime Costs to Soar to $2T By 2019

Survey predicts businesses will be paying four times as much as this year in cybercrime costs.

❯❯ Katie Kuehner-Hebert

May 13, 2015 | CFO.com | US

2016, http://www.forbes.com
2014, http://www.telegraph.co.uk
2015, http://ww2.cfo.com

NETWORK SECURITY IS A CRITICAL ISSUE

ABOUT CYBER NETWORK DEFENCE

- **While there will be over 1.5 million cyber security jobs that remain unfilled by 2019, millions of IT and Network administrators remain untrained on network defense techniques.**

  Michael Brown – CEO Symantec

- **Network defence is a broader market globally as compared to ethical hacking and penetration testing.**

- **It forms the basis on which skilled professionals can pursue CEH and ECSA (the reverse works as well).**

- **Networking professionals with certifications from the likes of CCNA, Network+, Security+ are immediate targets segments.**

"**Network defense** is important to businesses of all sizes"…. Ron McKenzie

http://www.marketwired.com/

Blind Spots in Network Defense

C N D
Certified Network Defender

JUNE 30, 2016

*Organizations are facing the **blind spots** in their network defenses.*

*Organizations are finding it difficult to address blind spots because of **lack of Network Security Knowledge**.*

*Organizations are facing challenges in the **acquisition of human resources** with network security skills.*

https://securityintelligence.com

“Network Administrators can be become a **first line of defense** for the organization, if they have enough security skills or are trained properly”

Why Network Administrators are So Important for an Organization?

- Network administrators spend a lot of time with network environments, and are familiar with network traffic, performance and utilization, network topology, location of each system, security policy, etc.
- If they provide protection, detection and response to incidents in early stages, organizations can contain or minimize potential impact of an incident.

Rising Demand for Network Security Skills

CND
Certified Network Defender

"Constant breaches of organizational networks are leading to increased demands for trained and certified network administrators to install, configure, secure and optimize their network."

http://www.itcareerfinder.com

Rising Demand for Network Security Skills

C|ND Certified Network Defender

*"There is huge gap between **potential demand** of individuals with network security skills and their **availability**"*

IT careers: Network Security Talent is Red-Hot

IT SALARY SURVEY 2015 SAYS:

There is an especially strong demand for data security analysts, ***systems security administrators****,* ***network security administrators****,* ***network security engineers*** *and security managers, according to the RHT report.*

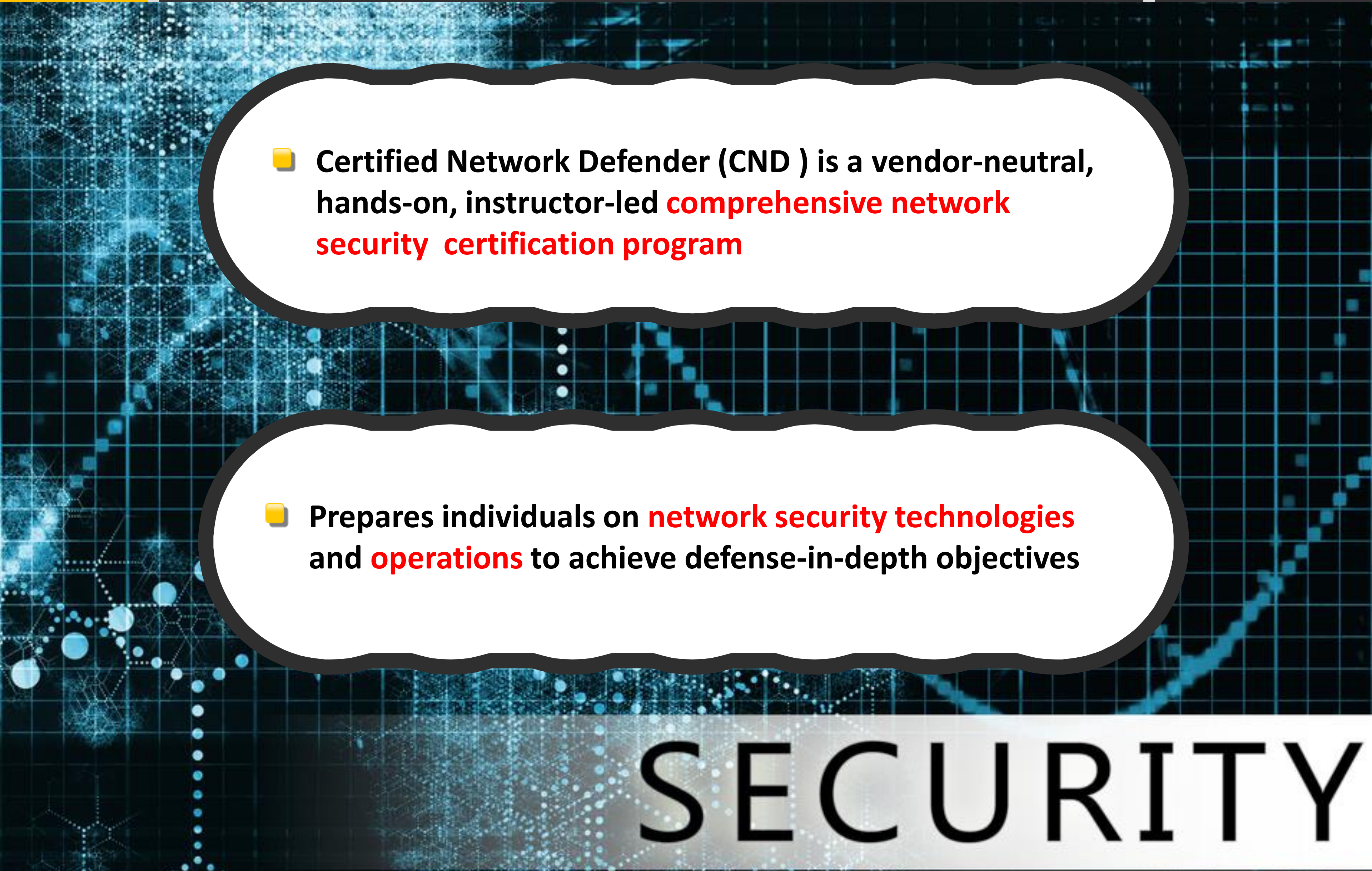
http://www.computerworld.com

ABOUT CND CERTIFICATION

What is CND Certification ?

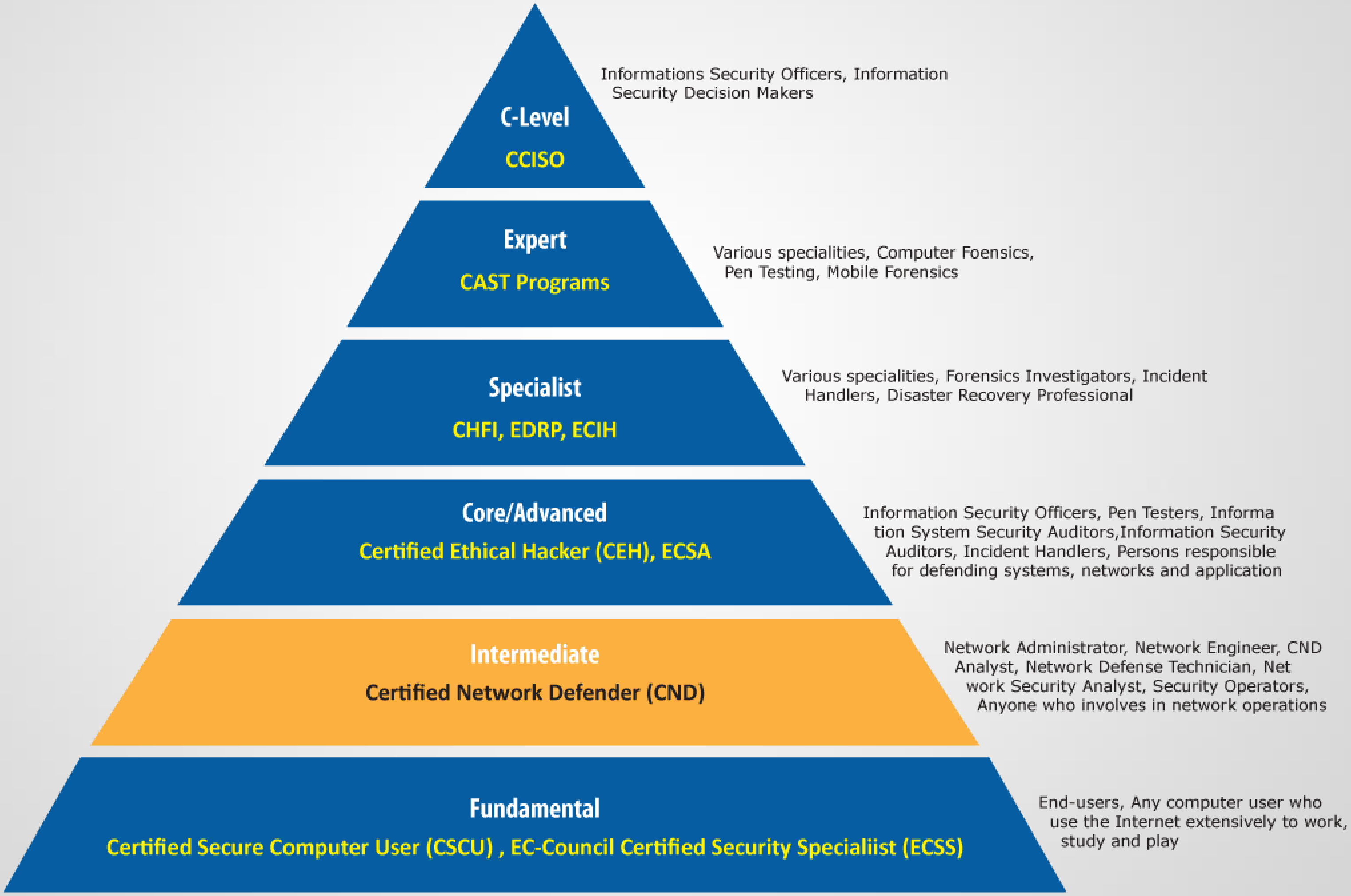
- Certified Network Defender (CND) is a vendor-neutral, hands-on, instructor-led comprehensive network security certification program

- Prepares individuals on network security technologies and operations to achieve defense-in-depth objectives



Where Does CND Fits in EC-Council Career Path?

C|ND Certified Network Defender



C-Level

CCISO

Informations Security Officers, Information Security Decision Makers

Expert

CAST Programs

Various specialities, Computer Foensics, Pen Testing, Mobile Forensics

Specialist

CHFI, EDRP, ECIH

Various specialities, Forensics Investigators, Incident Handlers, Disaster Recovery Professional

Core/Advanced

Certified Ethical Hacker (CEH), ECSA

Information Security Officers, Pen Testers, Information System Security Auditors,Information Security Auditors, Incident Handlers, Persons responsible for defending systems, networks and application

Intermediate

Certified Network Defender (CND)

Network Administrator, Network Engineer, CND Analyst, Network Defense Technician, Network Security Analyst, Security Operators, Anyone who involves in network operations

Fundamental

Certified Secure Computer User (CSCU) , EC-Council Certified Security Specialiist (ECSS)

End-users, Any computer user who use the Internet extensively to work, study and play

CND DESIGN APPROACH

How CND Will Help You – A Checklist for Network Managers

After attending the CND training, students will be able to:

☑ Design and implement the network security policies and procedures

☑ Troubleshoot the network for various network problems

☑ Identify various threats on organization’s network

☑ Determine and implement various physical security controls for their organizations

☑ Harden security of various hosts individually in the organization’s network

☑ Select appropriate firewall solution, topology, and configurations to harden security through firewall

☑ Determine appropriate location for IDS/IPS sensors, tuning IDS for false positives and false negatives, and configurations to harden security through IDPS technologies

☑ Implement secure VPN implementation for their organization

☑ Identify various threats to wireless network and mitigate them

☑ Maintain the inventory of computers, servers, terminals, modems and other access devices

☑ Provide security awareness guidance and trainings

☑ Manage, assign, and maintain the list of network addresses

How CND Will Help You – A Checklist for Network Managers

After attending the CND training, students will be able to:

- ☑ Perform risk assessment, vulnerability assessment/scanning through various scanning tools and generate detailed reports on it
- ☑ Identify the critical data, choose appropriate back up method, media and technique to perform successful backup of organization data on regular basis
- ☑ Provide first response to the network security incident and assist IRT team and forensics investigation team in dealing with an incident.
- ☑ Add, remove, or update user account information
- ☑ Apply operating system updates, patches and make configuration changes
- ☑ Update system configurations to maintain an updated security posture using current patches, device and operating system hardening techniques, and Access Control Lists.
- ☑ Manage network Authentication, Authorization, Accounting (AAA) for network devices
- ☑ Monitor network traffic and ensure the security of network traffic

How CND Will Help You – A Checklist for Network Managers

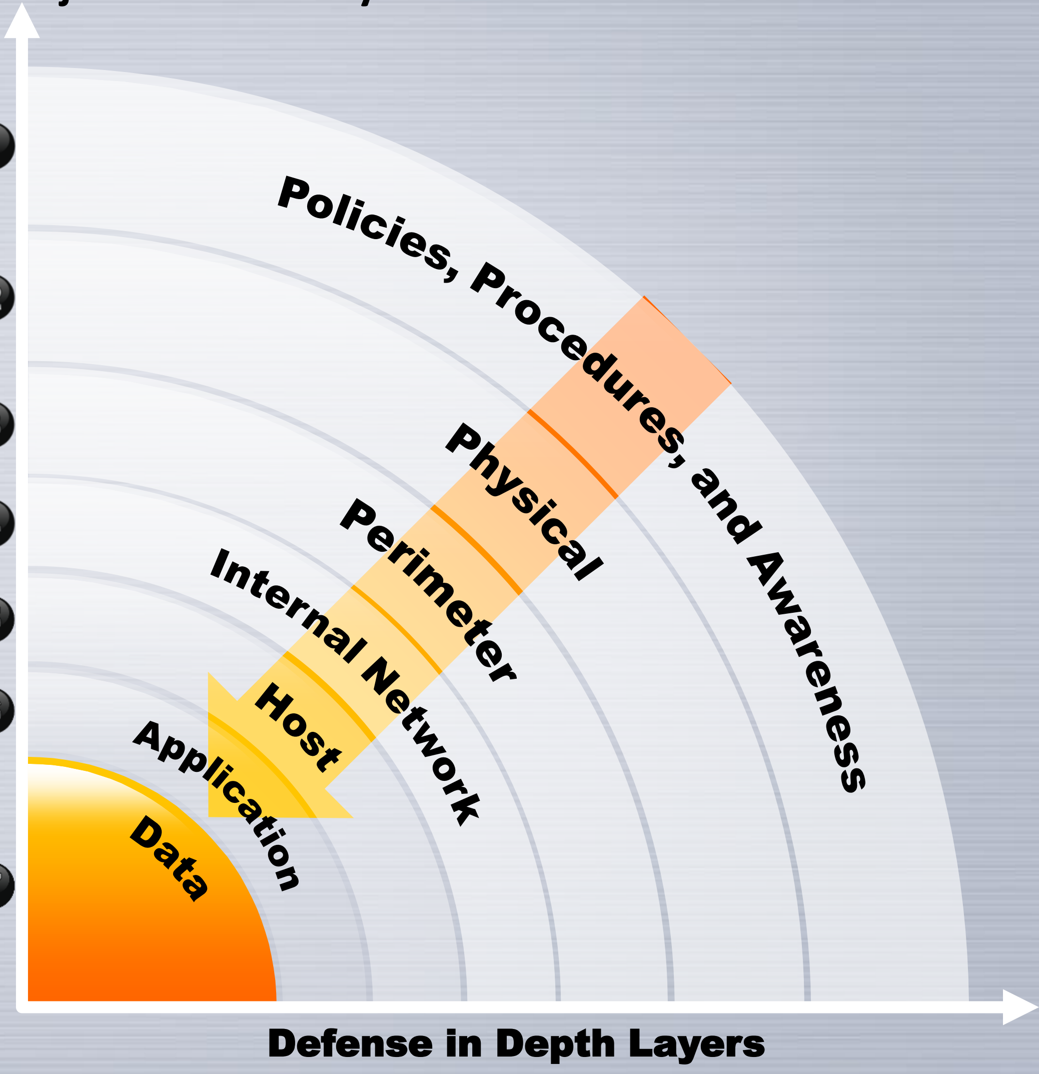
After attending the CND training, students will be able to:

- ☑ Manage Proxy and Content filtering
- ☑ Review audit logs from Firewall, IDS/IPS, servers and hosts on the internal, protected network
- ☑ Analyze, troubleshoot, and investigate security-related, information systems' anomalies based on security platform
- ☑ Maintain, configure, and analyze network and host-based security platforms
- ☑ Use File integrity verification and monitoring solutions
- ☑ Implement Network Access Control (NAC)
- ☑ Implement Data Loss Prevention (DLP) solutions
- ☑ Evaluate security products as well as security operations procedures and processes.
- ☑ Manage and maintain Windows Security Administration
- ☑ Manage and maintain Linux Security Administration
- ☑ Harden Routers and Switches

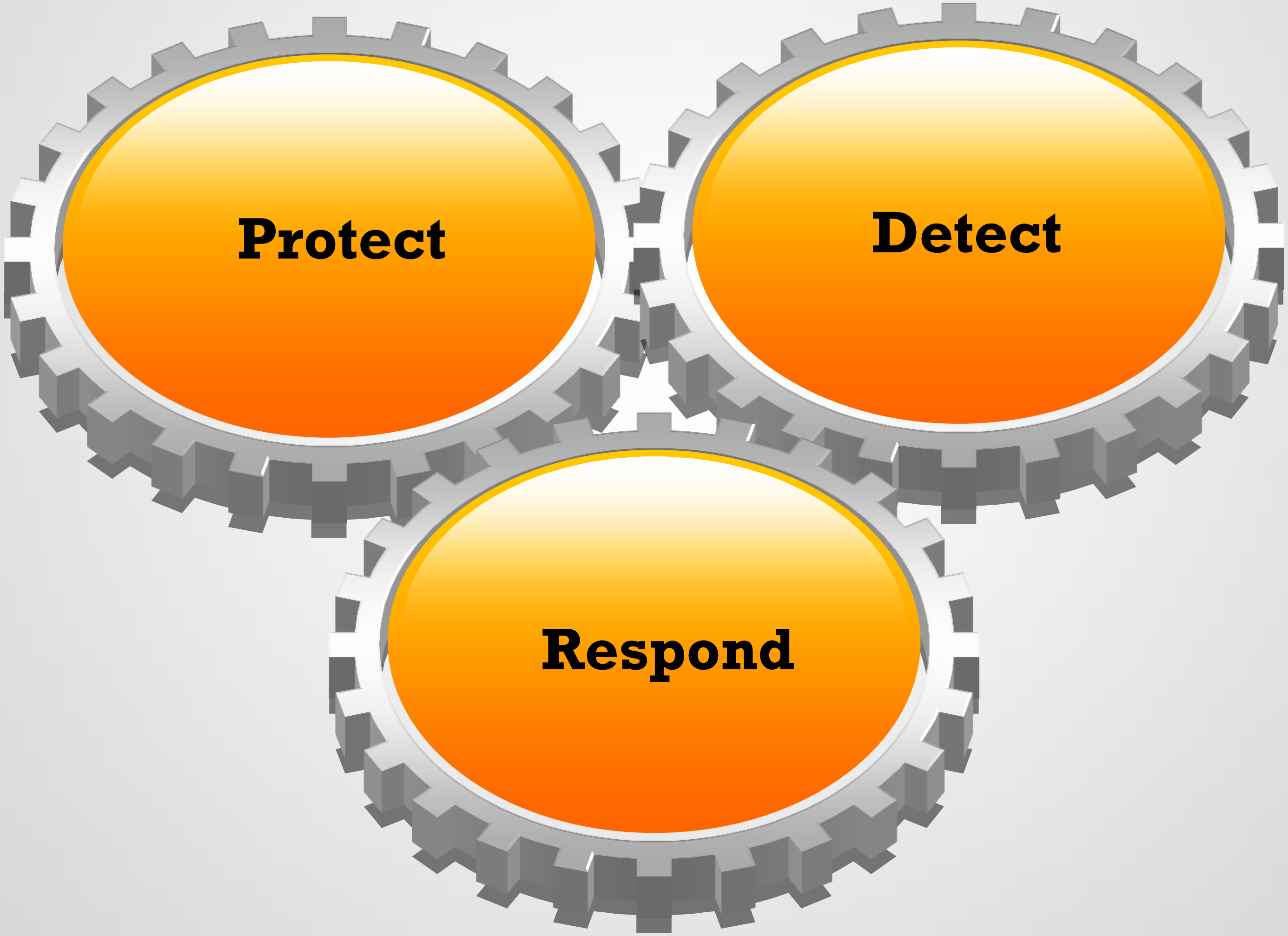
Network Security is a Major Component of Information Security Defense-in-Depth

- Network security components play major role in all layers of DID

1. Internet Access, Acceptable-Use, User-Account, Firewall-Management, Email Security, Passwords, Physical Security, BYOD, ISO/IEC 27001, PCI-DSS, HIPAA, etc.
2. Physical locks, Access controls, security personnel, Fire Fighting Systems, Power Supply, Video surveillance, Lighting, alarm system, etc.
3. Server, DNS, Email, Routers, Firewalls, Switches
4. Routers, Servers, Switches, Firewalls
5. OS , Antiviruses, Patches, Password Management, Logging, etc.
6. Blacklisting, whitelisting, patch management, password management, Application Configuration, firewall, etc.
7. Encryption, Hashing, permission, DLP



COMPONENTS OF CND FOCUS



PROTECT

“Refers to implementation of controls to achieve Defense-in-Depth protection”

Policies • Physical Security • Host Security • Firewalls • IDS/IPS

DETECT

“Refers to development and use of processes, techniques and tools to detect security bypass attempts; it guides you through **detection of incidents**”

Network Monitors • Log Management • Vulnerability Scanning • Risk Management

RESPOND

If an incident does occur, CND guides you through the **incident response process** and **post incident actions** to contain damage

Incident Handling• Incident Response • Data Back and Recovery

CND Phases And Core Domains

CND Phases	CND Modules
Introduction	Module 01: Computer Network and Defense Fundamentals
	Module 02: Network Security Threats, Vulnerabilities, and Attacks
	Module 03: Network Security Controls, Protocols, and Devices
Protection	Module 04: Network Security Policy Design and Implementation
	Module 05: Physical Security
	Module 06: Host Security
	Module 07: Secure Firewall Configuration and Management
	Module 08: Secure IDS Configuration and Management
	Module 09: Secure VPN Configuration and Management
	Module 10: Wireless Network Defense
Analysis and Detection	Module 11: Network Traffic Monitoring and Analysis
	Module 12: Network Risk and Vulnerability Management
Response	Module 13: Data Backup and Recovery
	Module 14: Network Incident Response and Management

What Does the Program Cover?

Technologies

- Physical security
- Firewalls /IDS implementation
- OS hardening/patching
- Antivirus protection
- Encryption mechanism
- Authentication mechanism
- Configuration management
- Access control mechanism
- Proxy servers
- Packet/content filtering
- Product evaluation based on common criteria
- Passwords security
- Network logs audit

Operations

- Creating and enforcing security policies
- Creating and enforcing standard network operating procedures
- Planning business continuity
- Configuration control management
- Creating and implementing incident response processes
- Planning data recovery
- Conducting forensics activities on incidents
- Providing security awareness and training
- Enforcing security as culture

People

- Network Administrator
- Network Security Administrator
- Network Security Engineer
- Security Architects
- Security Analysts
- Network Technicians
- End Users

Target Audience

“Network Administrators are the primary target audience of CND course”

However, The course will also be beneficial for:

- ✓ ***CND Analyst***
- ✓ ***Network Defense Technician***
- ✓ ***Network Engineer***
- ✓ ***Security Analyst***
- ✓ ***Security Operator***
- ✓ ***Anyone who involves in network operations***

Course Pre-requisites

- Student should have fundamental knowledge of networking concept.

Course Duration

Course Duration

- ✓ Days: 5 Days
- ✓ Time: 9.00 AM to 5.00 PM

CND Exam Information

- Number of Questions: 100
- Passing Score: 70%
- Test Duration: 4 Hours
- Test Format: Interactive Multiple Choice
- Test Delivery: ECC Exam

CND VALUE PROPOSITIONS

- It is designed and developed by experienced SMEs and network security professionals
- It covers all the three approaches, i.e. PREVENTIVE, REACTIVE, RETROSPECTIVE of network security
- The program is developed after a thorough job role analysis and market research
- Detailed labs for hands-on learning experience; approximately 50% of training time is dedicated to labs

CND VALUE PROPOSITIONS

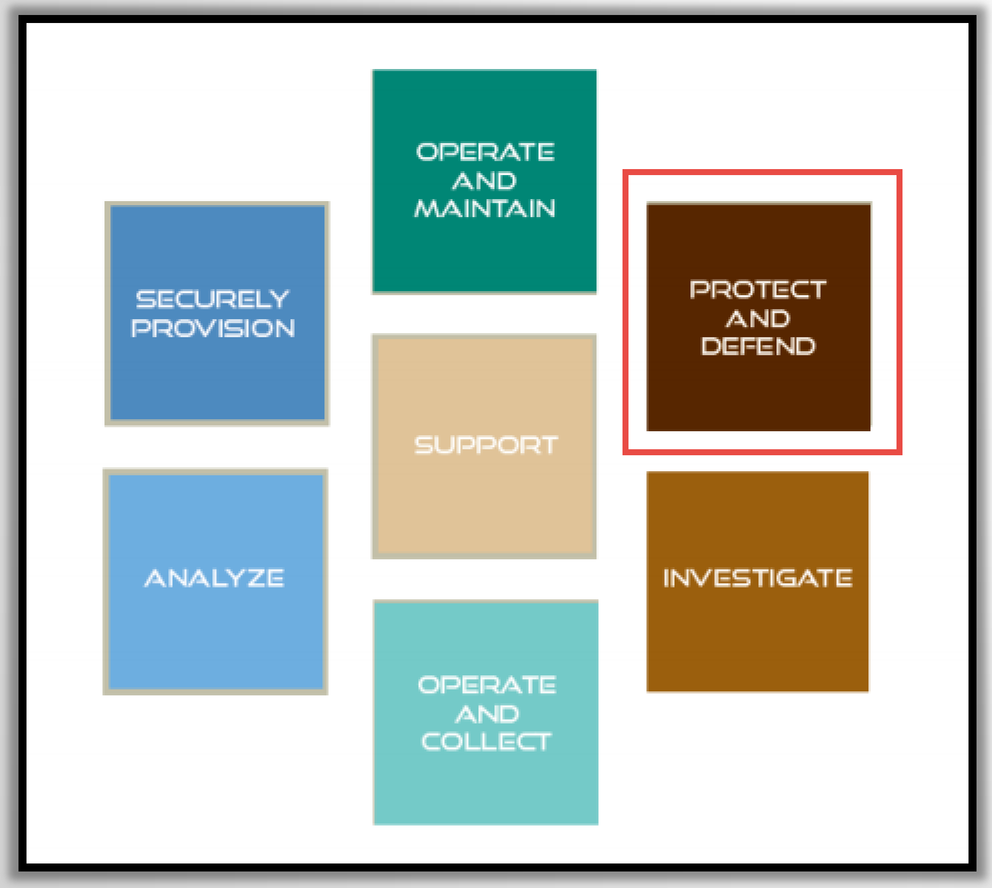
- It covers the relevant knowledge-bases and skills to meets with regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.

- More than 10 GB of network security, assessment and protection tools including various network policy templates, Wireshark filters, etc.

- The student kit contains large number of white papers for additional reading

CND VALUE PROPOSITIONS

CND Maps to NICE Framework



Compliance with National Initiative for Cybersecurity Education (NICE) "Protect and Defend" specialty area

Individual working under this specialty area holds following job titles:

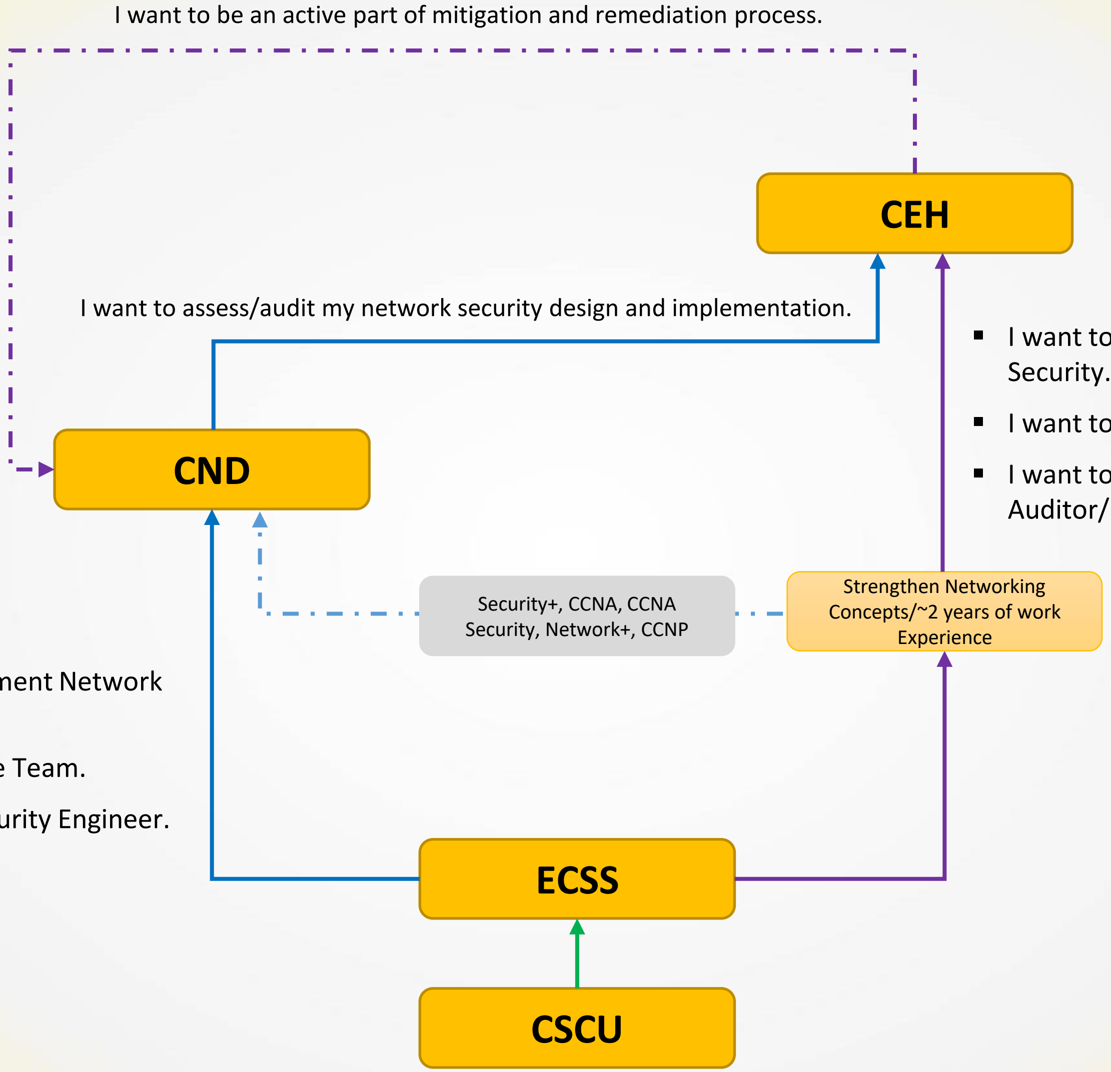
- CND Analyst (Cryptologic)
- Cyber Security Intelligence Analyst
- Focused Operations Analyst
- Incident Analyst
- Network Defense Technician
- Network Security Engineer
- Security Analyst
- Security Operator
- Sensor Analyst

CND VALUE PROPOSITIONS

CND maps Job Roles of
System Administrator specified by
Department of Defense (DoD)

CND COMPARISONS

CND - CEH Ecosystem


I want to be an active part of mitigation and remediation process.
CEH
I want to assess/audit my network security design and implementation.
CND
Security+, CCNA, CCNA Security, Network+, CCNP
Strengthen Networking Concepts/~2 years of work Experience
ECSS
CSCU

- I want to Assess & Audit Network Security.
- I want to be part of a Red Team.
- I want to be Network Security Auditor/Ethical Hacker.

- I want to Design & Implement Network Security.
- I want to be part of a Blue Team.
- I want to be Network Security Engineer.

CND vs CEH

Techniques/Domains	CND (Secure yourself)- (Blue Team)	CEH (Test how secure you are!)- (Red Team)
Firewall	Secure firewall design and implementations	Firewall Exploitation/Evasion techniques
IDS/IPS	Secure IDS design and implementations	IDS Exploitation/Evasion techniques
Vulnerability Scanning	Patching vulnerabilities	Finding out the vulnerabilities and exploiting them
System	System security techniques	System hacking techniques
Server	Server security techniques	Server hacking techniques
Wireless Network	Wireless network defense techniques	Wireless network hacking techniques
Cryptography	Cryptographic techniques	Cryptanalysis techniques to crack cryptography
Web Applications		Web Application hacking
Mobile Platform		Mobile platform hacking
Attack Explained	Introduction to attacks	Techniques to exploit network and system security using various attacks such as Malware, Sniffing, DoS, Session hijacking, etc.
Security Policies	Design and implementation of security policies	
VPN	VPN security design and implementation	
Threat Detection	Network monitoring and analysis	
Data Security	Data backup and recovery	
Response	Network Incident Response	

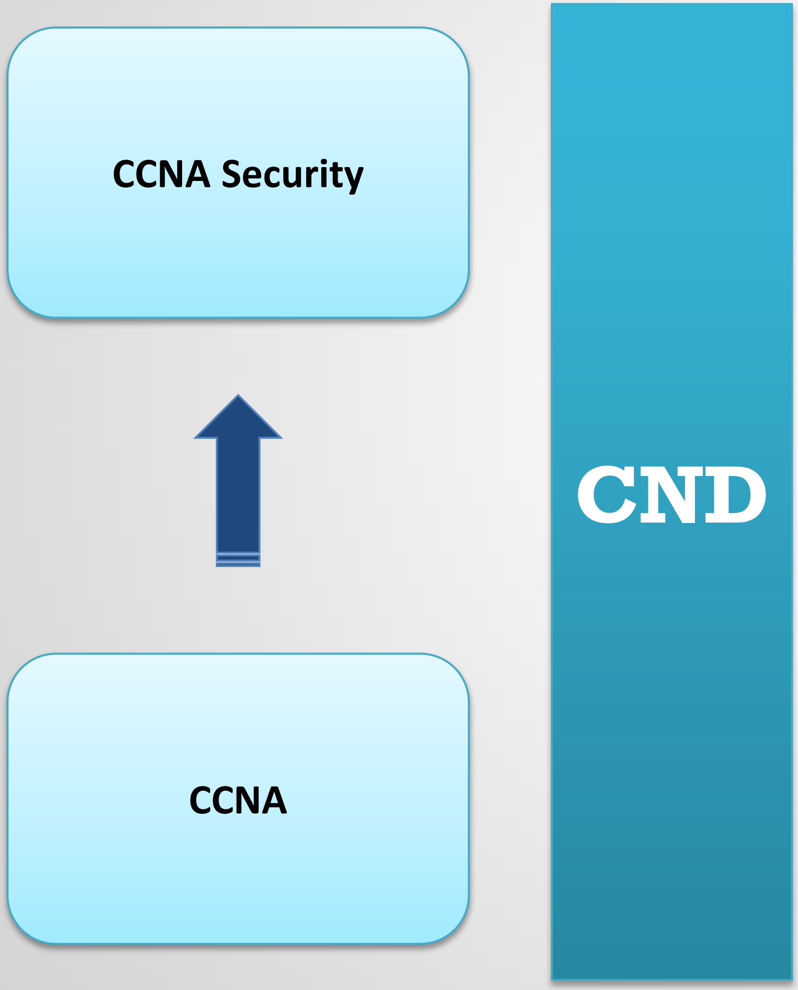
How CND is Different from Competition?

C|ND Certified Network Defender

- CND imparts and validates intermediate level network security knowledge and skills whereas Security+ validates only foundational IT security knowledge
- CND is a completely hands-on program with 50% time dedicates to labs whereas Security+ is a theoretical knowledge based program

Techniques	CND	Security+
Protection		
Security Threats, vulnerabilities, Attacks	Yes	Yes(Limited)
Network Security Controls	Yes	Yes
Network Policy Design	Yes	NO
Physical Security	Yes	Yes(Limited)
Host, Application, Data Security	Yes	Yes(Limited)
Firewall	Yes	Yes(Limited)
IDS	Yes	Yes(Limited)
VPN	Yes	Yes(Limited)
Wireless Security	Yes	Yes(Limited)
Detection		
Network Monitoring and Analysis	Yes	NO
Risk and Vulnerability Management	Yes	Yes(Limited)
Response		
Data Backup and Recovery	Yes	NO
Network Incident Response	Yes	Yes(Limited)

CND vs. CCNA/CCNA Security



CCNA Security

CCNA

CND

- ✓ CND is a vendor neutral program
- ✓ CND covers Defense-in-Depth including Technologies and Operations whereas CCNA/CCNA Security focus primarily on CISCO Technologies
- ✓ CND covers topics such as Network Monitoring and Analysis, Risk Management, Network Incident Response, Physical Security, etc. which are critical for current network security scenario whereas CCNA/CCNA Security do not include these topics
- ✓ CND covers Protection, Detection and Response for network security whereas CCNA/CCNA Security primarily focus on Protection part

Student Testimonials

"The knowledge tr
program will defini
especially in syster
dealing with my ve
management."

"The CND program v
haven't had a CEH cl
understanding of se
procedures, packet a
security processes."

Team Lead, Ne

"With the CND prog
handle issues and in
response, preventio
better"

"The knowledge gain from CND training program will hopefully help my employer by showing additional skills on paper when presenting a bid for a consulting contract."

Brady Cooper
Cyber security analyst
Booz Allen Hamilton
USA

"The CND program
encounter security
problem"

"The knowledge tra
program will help m
monitoring and ana

Ta

"The knowledge gair
make my day to day

"The CND program allows employers to better understand the importance of network information security , in order to devote more resources."

Hsien Lin Chu
ENGINEER
KPMG
Taiwn

CEI Testimonials

“It is very good and
good part is along v
of the content is giv
the students unders

“The exper
have to adj
and practic

The product of
better than the
instructors.

“In general, the course is very well focused and structured as well as the time necessary to cover topics”

› da Silva
›sulting SL
Spain

This class covers a wide range of areas and can seem over welling at first, but I think the material covers the topics well without going to in-depth. Over all I think the class went well, I believe there is a good balance of slides and labs. I was able to cover the slide material and then give the students time in class to work on the labs.

I think this is a great class and will be beneficial for network and system administrators. Thank you for the opportunity to give this class, and I look forward to teaching it again.

Wayne Pruitt
Stealth Entry
USA

Thank You