Cybersecurity

TechGuide - Alura, FIAP e PM3

Cybersecurity

Level 1

Cryptography - Fundamentals:

Cryptography in cybersecurity is the conversion of data from a readable format into an encrypted format. Encrypted data can only be read or processed after it has been decrypted.

Contents

WebSite	GeeksForGeeks: Cryptography Introduction (	https://www.geeksforgeeks.org/cryptography-introduction/)
Article	Introduction to Cryptography: One time pads and stream ciphers (	https://medium.com/coinmonks/introduction-to-cryptography-one-time-pads-and-stream-ciphers-3b62c7003da8)
Article	A Whirlwind Tour of Modern Cryptography (	https://user3141592.medium.com/notes-on-computational-cryptography-98db5f2908f1)
Article	Understanding the 3 Main Types of Encryption (	https://spin.atomicobject.com/2014/11/20/encryption-symmetric-asymmetric-hashing/)
Article	Why Is Symmetric Key Encryption So Much Faster Than Asymmetric (Public) Key? (	https://medium.com/asecuritysite-when-bob-met-alice/why-is-symmetric-key-encryption-so-much-faster-than-asymmetric-public-key-e9e40d6475bc)
Article	Programming Encryption Algorithms	https://randerson112358.medium.com/programming-encryption-algorithms-520cb98c039d)

(

YouTube	Next Day Video: Crypto 101 (	https://www.youtube.com/watch?v=3rmCGsCYJF8&ab_channel=NextDayVideo)
YouTube	Simply Explained: Asymmetric Encryption (	https://www.youtube.com/watch?v=AQDCe585Lnc&ab_channel=SimplyExplained)
Article	itfreetraining: Symmetric Key and Public Key Encryption (	https://www.youtube.com/watch?v=ERp8420ucGs&ab_channel=itfreetraining)
Article	Eddie Woo: The RSA Encryption Algorithm (	https://www.youtube.com/watch?v=4zahvcJ9glg&ab_channel=EddieWoo)

Cybersecurity Framework:

The Cybersecurity Framework is a guidance guide for organizations - in any industry or community - that seek to improve cybersecurity risk management through the use of Frameworks. While the Cybersecurity Framework is not a one-size-fits-all approach to managing cybersecurity risks for organizations, it ultimately aims to reduce and better manage those risks. As such, this guide is intended for any and all organizations, regardless of industry or size.

Contents

WebSiteNIST (https://www.nist.gov/cyberframework)

WebSiteSOC2 (https://www.aicpa.org/home)

WebSiteWhat is ISO 27001? (https://advisera.com/27001academy/what-is-iso-27001/)

Article	Cybersecurity Framework 101 (	https://medium.com/edureka/cybersecurity-framework-89bbab5aaf17)
Article	Top 10 Cybersecurity Frameworks to Know (	https://medium.com/@niitwork0921/top-10-cybersecurity-frameworks-to-know-8ee51d4f5b3e)

ArticleCyber Security Guide (https://www.stanfieldit.com/cyber-security/)

YouTube	Optic Cyber: NIST Cybersecurity Framework Overview (	https://www.youtube.com/watch?v=4NSQCmAw6Ck)
YouTube	National Institute of Standards and Technology: The Cybersecurity Framework (	https://www.youtube.com/watch?v=J9ToNuwmyF0)

Hacker Techniques:

Understanding the methodologies and techniques attackers use to perform reconnaissance as a pre-attack step, including how they use open source intelligence, network scanning, and target enumeration attacks to find the gaps in their network security.

Using attacker techniques to assess the security of a target network, evaluating popular protocols and endpoints for Windows, Linux, and cloud destinations.

Contents

WebSitePTES (http://www.pentest-standard.org/index.php/Main_Page)

WebSiteOWASP (https://owasp.org)

WebSiteOSSTMM (https://www.isecom.org/OSSTMM.3.pdf)

ArticlePenetration Testing Steps: Anatomy of a Successful Pentest (https://www.securecoding.com/blog/penetration-testing-steps/)

ArticleMy pentesting methodology (Enumeration) (https://medium.com/@nclvnp/enumeration-1976c5d55b1b)

ArticlePassword Cracking (https://medium.com/rangeforce/password-cracking-6d9612915f03)

YouTubeTech Xpress: How To Become A Hacker In 2023 | Step By Step Guide For Beginners (https://www.youtube.com/watch?v=W6vcd2gJw3Q)

WebSiteHack The Box: A Massive Hacking Playground (https://www.hackthebox.com)

Vulnerability assessment:

Framework techniques and tactics from various services and tools that provide a vulnerability scanning and management solution.

Contents

ArticleNessus Vulnerability Scanner (https://medium.com/@justinwolbert/nessus-vulnerability-scanner-22719d3bd9f7)

ArticleNessus — a sensational vulnerability scanner and beyond (https://medium.com/@haox-hapot/nessus-a-sensational-vulnerability-scanner-and-beyond-d0863422c381)

`Article`	Open source vulnerability assessment tool OpenVAS (	https://medium.com/purple-team/open-source-vulnerability-assessment-tool-openvas-e7036c1e48fd	)
`WebSite`	GeeksForGeeks: OpenVAS Install (	https://www.geeksforgeeks.org/installing-openvas-on-kali-linux/	)
`YouTube`	Jon Good: Nessus Vulnerability Scanner Tutorial (	https://www.youtube.com/watch?v=x87gbgQD4eg&ab_channel=JonGood	)
`YouTube`	HackerSploit: Vulnerability Analysis With OpenVAS (	https://www.youtube.com/watch?v=koMo_fSQGlk&ab_channel=HackerSploit	)

`YouTube`Scanning Best Practices (https://www.youtube.com/watch?v=SlRyd3f57c0)

`WebSite`Qualys (https://www.qualys.com)

Firewalls, IDS and IPS:

Definitions and differences between network security devices, firewalls, intrusion prevention systems (IPS) and intrusion detection systems (IDS).

A firewall allows traffic depending on a set of rules that have been configured. It is based on source, destination and port addresses. A firewall can deny any traffic that does not meet the specified criteria.

IDS are passive monitoring system devices that monitor network traffic as it travels over the network, compare signature patterns, and trigger an alarm if suspicious activity or a known security threat is detected.

IPS is an active device that prevents attacks by blocking them.

Contents

`WebSite`pfSense (https://www.pfsense.org)

`Article`	A Guide to the Uncomplicated Firewall (UFW) for Linux (	https://medium.com/@jasonrigden/a-guide-to-the-uncomplicated-firewall-ufw-for-linux-570c3774d7f4	)
`Article`	Pf-sense Firewall explained (	https://the-dark-lord.medium.com/pf-sense-firewall-part-1-1d9d17c5a7a6	)
`Article`	Compare: Firewalld / Iptables / Nftables / Netfilter (	https://iceburn.medium.com/compare-firewalld-iptables-nftables-netfilter-de08a8d21b5b	)

WebSite	GeeksForGeeks: Intrusion Detection System (IDS) (	https://www.geeksforgeeks.org/intrusion-detection-system-ids/)
WebSite	GeeksForGeeks: Intrusion Prevention System (IPS) (	https://www.geeksforgeeks.org/intrusion-prevention-system-ips/?ref=lbp)
Article	Learning More about IPS and IDS (	https://gupta-bless.medium.com/learning-more-about-ips-and-ids-ef6d859c2ab3)
YouTube	Linode: iptables Complete Guide (	https://www.youtube.com/watch?v=6Ra17Qpj68c&ab_channel=Linode)
YouTube	CBT Nuggets: IDS vs. IPS (	https://www.youtube.com/watch?v=rvKQtRklwQ4&ab_channel=CBTNuggets)

Digital Investigation - Fundamentals:

Digital Investigation is the use of science to investigate digital crimes and determine facts, which has emerged from the use and spread of digital systems such as computers and smartphones.

Contents

YouTube	DFIRScience: Intro to Cybercrime and Networks (	https://www.youtube.com/watch?v=sKijlRCRiKU)
YouTube	DFIRScience: Cybersecurity and Cybercrime (	https://www.youtube.com/watch?v=3kEkXunWKaU)
YouTube	DFIRScience: Digital Investigation Methods (	https://www.youtube.com/watch?v=72Ihrc_MZ6o)
YouTube	My CS: Digital Forensics Tools (	https://www.youtube.com/watch?v=Hwbb7zAWamg)
Article	What is Digital Forensics (	https://haniahshafi.medium.com/what-is-digital-forensics-and-how-it-is-used-in-investigations-4389fdce7549)
Article	Digital Forensics Investigation Steps (	https://medium.com/cyversity/digital-forensics-investigation-steps-f06a82c2c4ac)

Password attack:

In cryptanalysis and security, password cracking is the process of recovering passwords from data that has been stored or transmitted by a computer system in encrypted form. A common approach (brute force attack) is to repeatedly try guesses

for the password and compare them with an available cryptographic hash of the password.

Contents

Article	Password Cracking (	https://medium.com/rangeforce/password-cracking-6d9612915f03	)
Article	Cyber Security: Password Attacks (	https://liu-111.medium.com/cyber-security-password-attacks-8ea7fbdf307a	)
Article	How to brute force FTP, SSH, login and password using Hydra (	https://twriting.medium.com/how-to-brute-force-ftp-ssh-login-and-password-using-hydra-5a5ceaf763f9	)
Article	Brute-force attacks with Kali Linux (	https://pentestit.medium.com/brute-force-attacks-using-kali-linux-49e57bb89259	)
Article	DVWA Brute Force Tutorial (Low Security) (	https://medium.com/@dannybeton/dvwa-brute-force-tutorial-low-security-463880d53e50	)
Article	Hashcat 101: Cracking Password Hashes (	https://medium.com/@cyberforensicator57/hashcat-101-cracking-password-hashes-bb524b115f71	)
YouTube	CertBros: How to HACK Website Login Pages | Brute Forcing with Hydra (	https://www.youtube.com/watch?v=-CMBoJ60K1A&ab_channel=CertBros	)
YouTube	Logan Therrien: Medusa Tutorial (	https://www.youtube.com/watch?v=hZQ3AumggaA	)

Open-Source Intelligence:

OSINT (Open Source Intelligence) can be defined as a set of activities to collect, store and analyze information from public sources, basically any data about a company or person that can be found through Internet tools or OSINT frameworks, such as search engines.

Contents

Article	What Is Open Source Intelligence? (	https://medium.com/codex/what-is-open-source-intelligence-osint-43e56eb113b4	)
Article	Open Source Intelligence (OSINT) 101 (	https://medium.datadriveninvestor.com/open-source-intelligence-osint-101-d96f47ff2ff1	)
WebSite	OSINT (https://osintframework.com/)		

`WebSite` haveibeenpwned (https://haveibeenpwned.com/)

`WebSite` checkusername (https://checkusernames.com/)

	OSINT What is it (	https://medium.com/transparent-data-eng/osint-what-is-it-and-what-does-it-have-to-do-with-open-sources-of-information-ec35daeea1c0	)
`Article`			
`YouTube`	Ntrepid: What is OSINT? (	https://www.youtube.com/watch?v=ZUZG1zaaKY4&ab_channel=Ntrepid	)
`YouTube`	XEye: Maltego - The Automated OSINT Tool for Ethical Hackers (	https://www.youtube.com/watch?v=a2ZvpwF3u-M&ab_channel=XEye	)

Security Operations Center:

SOC (Security Operations Center) is the department that comes to plan and support the entire I.T. security strategy, monitoring, preventing, and remedying breaches, failures, and possible attacks, all in a proactive way.

Contents

`Article`	SECURITY OPERATIONS CENTER — SOC (	https://medium.com/predict/security-operations-center-soc-e5f47e277a35	)
`Article`	What is the Blue Team? (	https://medium.com/@BurakDamoglu/introduction-to-security-operations-center-73e2e50f3ba7	)
`Article`	Security Operations Center (	https://medium.com/fnplus/security-operations-center-93e67268180a	)
`YouTube`	joe blaney: What is a Security operations centre SOC (	https://www.youtube.com/watch?v=3S01vLlvubE	)
`Article`	Future Of The SOC (	https://medium.com/anton-on-security/new-paper-future-of-the-soc-process-consistency-and-creativity-a-delicate-balance-paper-3-of-f73fe653c04d	)
`YouTube`	BitLyft: How to Build an Effective Security Operations Center (	https://www.youtube.com/watch?v=wtNewkBYVvQ&ab_channel=BitLyft	)
`YouTube`	Fujitsu: Inside the Security Operations Centre (	https://www.youtube.com/watch?v=6LwyTWPKDnQ	)
`YouTube`	Telstra Enterprise: Security Operations Centre (	https://www.youtube.com/watch?v=zadlfhl0XQc	)

Penetration Testing - Fundamentals:

Pentest (Penetration Testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker might exploit, simulating an attack against an organization's IT assets.

Contents

Article	What is Penetration Testing? (	https://medium.com/edureka/what-is-penetration-testing-f91668e2291a	)
Article	From Zero to your first Penetration Test (	https://medium.com/hootsuite-engineering/penetration-testing-d887d081c5c5	)
Article	Quick Guide to Web Penetration Testing (	https://corneacristian.medium.com/quick-guide-to-web-penetration-testing-546c6196c909	)
Article	Pentesting Fundamentals (	https://infosecwriteups.com/pentesting-fundamentals-tryhackme-717f51d6126b	)
YouTube	Loi Liang Yang: Simple Penetration Testing Tutorial for Beginners (	https://www.youtube.com/watch?v=B7tTQ272OHE&ab_channel=LoiLiangYang	)
YouTube	freeCodeCamp.org: Full Ethical Hacking Course - Network Penetration Testing for Beginners (	https://www.youtube.com/watch?v=H1auWPjioeU	)
YouTube	LiveOverflow: Pentesting vs. Bug Bounty (	https://www.youtube.com/watch?v=sXThugPk_zA&ab_channel=LiveOverflow	)

Level 2

Endpoint security:

Endpoint security, or endpoint protection, is the cybersecurity approach to defending endpoints such as desktops, laptops, and mobile devices against malicious activity.

Contents

Article	Endpoint Security: I (	https://medium.com/starting-up-security/endpoint-security-intuition-around-the-mudge-disclosures-dfbe014790f2	)
Article	Introduction to FireEye Endpoint Security (	https://medium.com/@knoldus/introduction-to-fireeye-endpoint-security-3534c9bf60fe	)

Article	EPP vs EDR vs XDR: Endpoint Security Comparison (	https://altexsoft.medium.com/epp-vs-edr-vs-xdr-endpoint-security-comparison-57409987f65e)
Article	Endpoint Security - Antivirus, EPP & EDR (	https://anandadip.medium.com/endpoint-security-antivirus-epp-edr-99496597b892)
Article	What is Endpoint Detection and Response (EDR) (	https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/)
Article	EDR vs. NGAV (	https://www.crowdstrike.com/cybersecurity-101/endpoint-security/edr-vs-ngav/)
Article	Introduction to Advanced Endpoint Protection (AEP) (	https://www.crowdstrike.com/cybersecurity-101/endpoint-security/advanced-endpoint-protection-aep/)
Article	Endpoint Security (	https://www.crowdstrike.com/cybersecurity-101/endpoint-security/)
YouTube	Heimdal: Endpoint Security - Definition, Benefits, and Key Components (	https://www.youtube.com/watch?v=2CVP9-Qslcw&ab_channel=Heimdal%C2%AE)

Metasploit - Attack and Analysis:

Metasploit is the world's most widely used penetration testing framework.

Contents

WebSite	Metasploit (https://www.metasploit.com/)	
Article	Kali Linux & Metasploit: Getting Started with Pen Testing (	https://medium.com/cyberdefendersprogram/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b)
Article	How to Create a Nearly Undetectable Backdoor using MSFvenom in Kali Linux (	https://www.wikihow.com/Create-a-Nearly-Undetectable-Backdoor-using-MSFvenom-in-Kali-Linux)
Article	Hack Windows 10 with Metasploit (	https://medium.com/@leandro.almeida/hack-windows-10-with-metasploit-329c283db99a)
YouTube	HackerSploit: Metasploit For Beginners 1 (	https://www.youtube.com/watch?v=8lR27r8Y_ik)

| YouTube | HackerSploit: Metasploit For Beginners 2 (| https://www.youtube.com/watch?v=6SNHuWaLuhU |) |
| YouTube | HackerSploit: Metasploit For Beginners 3 (| https://www.youtube.com/watch?v=CYB6Uta9VTI |) |

Web application - Security:

Web application security (also known as Web AppSec) is the idea of designing websites to function as expected, even when under attack. The concept involves a collection of security controls designed into a web application to protect its assets from potentially malicious agents.

Contents

Article	How to Secure Web Apps — A Web App Security Checklist (	https://medium.com/quick-code/how-to-secure-web-apps-a-web-app-security-checklist-bb27cf049d1d	)
Article	Web Application Security Basics (	https://mtrdesign.medium.com/web-application-security-basics-9b7553f51e8a	)
Article	Web Application Security (	https://pub.towardsai.net/web-application-security-top-11-best-practices-for-2020-c3a485e40de8	)
Article	Web Application Security Best Practices (	https://javascript.plainenglish.io/web-application-security-best-practices-881e3cfde2a1	)
YouTube	House Of Secure Network: Web Application Security - Best Practices (	https://www.youtube.com/watch?v=RedZvpyRd38	)
YouTube	freeCodeCamp.org: Web application security - 10 things developers need to know (	https://www.youtube.com/watch?v=3EdFeJ0_mB0	)
YouTube	Fireship: 7 Security Risks (	https://www.youtube.com/watch?v=4YOpILi9Oxs	)
YouTube	Crashtest Security: SAST, DAST, IAST, RASP Explained (	https://www.youtube.com/watch?v=5cOkNbH_jPU	)

Web application - Vulnerability:

Web application vulnerabilities involve a system flaw or weakness in a web-based application. They have existed for years, largely due to failure to validate or clean form entries, misconfigured web servers, and application design flaws, and can be exploited to compromise the security of the application. These vulnerabilities are not

the same as other common types of vulnerabilities, such as network or asset. They arise because web applications need to interact with multiple users on multiple networks, and this level of accessibility is easily exploited by hackers.

Contents

`WebSite`OWASP Top Ten (https://owasp.org/www-project-top-ten/)

`Article` Web Application Security Basics 101 (https://medium.com/nerd-for-tech/devsecops-basics-where-to-start-aa7babee4ac4)

`Article`Web Application Security: From Vulnerabilities to Monitoring (https://medium.com/swlh/web-application-security-from-vulnerabilities-to-monitoring-7a3c2dfbfa23)

`Article` How to Install DVWA Into Your Linux Distribution (https://medium.datadriveninvestor.com/setup-install-dvwa-into-your-linux-distribution-d76dc3b80357)

`Article` SQL Injection Attack in DVWA with Low Security Level (https://audreybetsy.medium.com/sql-injection-attack-in-dvwa-f6adc95f239b)

`Article` StackZero: Hack File Inclusion in DVWA: A Full Walkthrough (https://stackzero.net/hack-file-inclusion-in-dvwa-a-full-walkthrough/)

`Article` StackZero: How to Brute Force DVWA login with Python (https://stackzero.net/brute-force-dvwa-python/)

`YouTube`Cloud Security Training & Consulting: OWASP 2021 Top 10 Web Application Vulnerabilities (https://www.youtube.com/watch?v=NATCMnghei0)

`YouTube`CryptoCat: Damn Vulnerable Web Application (DVWA) (Playlist) (https://www.youtube.com/playlist?list=PLHUKi1UIEgOJLPSFZaFKMoexpM6qhOb4Q)

Mobile Device Management:

Mobile device management refers to any tool or software designed to help administrators control and secure mobile devices such as smartphones and tablets in an organization. Mobile device management is an important part of enterprise mobility management and endpoint management, especially as more companies adopt BYOD (bring your own device) policies that allow employees to access company data, files, and applications on their personal devices.

Contents

Article	What is Mobile Device Management (	https://hexnode.medium.com/what-is-mobile-device-management-mdm-3fd7fb4755b6	)
Article	Mobile Device Management Guide (	https://medium.com/codex/mobile-device-management-guide-2022-aosp-for-custom-mdm-6b9758aee4a8	)
Article	How To Address Privacy Concerns (	https://dennisturpitka.medium.com/how-to-address-privacy-concerns-when-building-a-mobile-device-management-solution-9bda148234df	)
Article	Top 5 mobile device management (	https://hexnode.medium.com/top-5-apple-mobile-device-management-platforms-for-2020-e6d626e68da5	)
YouTube	MTG, Inc.: What is MDM (Mobile Device Management)? (	https://www.youtube.com/watch?v=ug5KUH_jdA4&ab_channel=MTG%2CInc	.)
YouTube	Nutto 1981: Managing Microsoft 365 Mobility and Security MS 101 Day1 (	https://www.youtube.com/watch?v=2WTuDAwLTxA&ab_channel=Nutto1981	)
YouTube	Harry Lowton: What Is Microsoft Intune? (	https://www.youtube.com/watch?v=ildHLspps7M	)

SIEM e SOAR:

Security Information and Event management (SIEM) is software that aggregates and analyzes information from several different sources across the entire infrastructure.

Security Orchestration, Automation, and Response (SOAR) will help you with threat and vulnerability management, security incident response, and security operation automation.

Contents

Article	Introduction to SIEM and SOAR (	https://medium.com/@roddytech/introduction-to-siem-and-soar-f7c855df9f3d	)
WebSite	IBM: What is SIEM? (	https://www.ibm.com/topics/siem	)
Article	How to implement OSSIM (SIEM Solution) (	https://hamzamhirsi.medium.com/how-to-implement-ossim-siem-solution-e94e9f937f8	)
Article	Top Free Security Information and Event	https://kalhara-sampath.medium.com/top-free-security-information-and-event-management-	)

| | Management(SIEM) Software's (| [siem-softwares-20c6d8f32a6f](#) | |

| WebSite | What is the ELK Stack? (https://www.elastic.co/what-is/elk-stack) | | |

| YouTube | BlackPerl: SOC Open Source (| https://www.youtube.com/watch?v=t6PqjLIVgdA |) |

| YouTube | Introduction To Wazuh SIEM: Wazuh (| https://www.youtube.com/watch?v=Hq58_yGJwHk&ab_channel=HackerSploit |) |

Server Hardening:

A proteção do servidor é um conjunto de disciplinas e técnicas que melhoram a segurança de um servidor 'em produção'. Hardening é um requisito de estruturas de segurança em diversos frameworks.

Contents

| Article | Introduction to Server Hardening (| https://medium.com/@gabu_b/introduction-to-server-hardening-cf6435d0accd |) |

| WebSite | GeeksForGeeks: What is System Hardening? (| https://www.geeksforgeeks.org/what-is-system-hardening/ |) |

| Article | Linux Server Hardening (| https://medium.com/@thefoursec/linux-server-hardening-e659db8ec689 |) |

| Article | 5 Steps to (Secure)Hardening (| https://saeedrz.medium.com/5-steps-to-hardening-your-server-centos-7-25e1851c8204 |) |

| Article | Linux Hardening Guide (| https://madaidans-insecurities.github.io/guides/linux-hardening.html |) |

| Article | Server Architecture Security (Windows) (| https://medium.com/@jbrendan86/server-architecture-security-windows-2da580d58e62 |) |

| YouTube | Linode: Hardening Access to Your Server (| https://www.youtube.com/watch?v=eeaFoZlSq6I |) |

| YouTube | Christian Lempa: How to protect Linux from Hackers (| https://www.youtube.com/watch?v=Bx_HkLVBz9M |) |

| YouTube | INEtraining: Linux Security & Server Hardening - Linux PAM (| https://www.youtube.com/watch?v=N4DP68TK0AQ |) |

| YouTube | IT Ops Talk: How to Harden Windows Server (| https://www.youtube.com/watch?v=HG_z_Q7LMlM&ab_channel=ITOpsTalk |) |

Cloud forensics:

Investigating data stored in the cloud can be a variety of approaches, from open source intelligence investigations (OSINT) to investigations of cloud accounts of participating individuals who disclose their login credentials (more often from victims and witnesses than suspects), to obtaining and analyzing collateral returns from cloud service providers to gain access to suspects' accounts.

Contents

Article	Cloud Forensics Tools (	https://medium.com/@cloud_tips/cloud-forensics-788f0c8fe69c	)
Article	Cloud forensics (	https://kumarshivam-66534.medium.com/cloud-forensics-be18e14230de	)
Article	Digital Forensic Challenges In Cloud Computing (	https://medium.com/@frosky/digital-forensic-challenges-in-cloud-computing-part-1-c06301cbe174	)
Article	Overview of Cloud Forensics (	https://medium.com/sigma-xi-vit/overview-of-cloud-forensics-b928537791e6	)
Article	How to Think about Threat Detection (	https://medium.com/anton-on-security/how-to-think-about-threat-detection-in-the-cloud-1baff902afe5	)
YouTube	Forensic Focus: Forensics In The Cloud - How To Conduct An Office 365 Investigation (	https://www.youtube.com/watch?v=wFjFjemaxmI	)
YouTube	SANS Digital Forensics and Incident Response: Cloud Forensics & Incident Response Course (	https://www.youtube.com/watch?v=XoeuAVJwkQ8	)

Data Recovery:

Data recovery is a software-driven process that allows you to recover and restore lost, deleted, inaccessible, corrupted, or damaged files so that you can get back to work quickly. As the business landscape, and our lives in general, become more dependent on data, the need to protect data systems is growing.

Contents

Article	Data Recovery (	https://medium.com/@rohitpatil97/data-recovery-c9818f19441d	)

Article	Data Loss Restoration (	https://medium.com/@danielmop/survey-research-paper-data-loss-restoration-4fae9fa38685	)
Article	Data Recovery and AI (	https://medium.com/@joanna.riley/data-recovery-and-ai-what-you-need-to-know-75a44c79385d	)
Article	Upcoming Future Of Data Backup & Recovery (	https://kunalranjane.medium.com/upcoming-future-of-data-backup-recovery-509d7fc1690f	)
Article	How to Recover Deleted Files (	https://medium.com/android-news/how-to-recover-deleted-files-from-hard-drive-a-step-by-step-recovery-solution-14355745239a	)
YouTube	Techquickie: Data Recovery As Fast As Possible (	https://www.youtube.com/watch?v=PWuWOSOCGxE	)
YouTube	Techquickie: Data Recovery Services (	https://www.youtube.com/watch?v=v0QkafsInrM	)
YouTube	IBM Technology: Disaster Recovery vs. Backup (	https://www.youtube.com/watch?v=07EHsPuKXc0	)

Container Security:

Container security is the process of combining security policies to ensure that the integrity of the container is protected. Container security is important because the container image contains all the components that will eventually run your application. If there are vulnerabilities lurking in the container image, the risk and potential severity of security problems during production increases.

Contents

Article	Container Security Solutions (	https://medium.com/xenonstack-security/container-security-solutions-framework-mechanism-and-strategy-24de3891a12b	)
Article	Container Security Threats (	https://medium.com/oreillymedia/container-security-threats-38649261fb4f	)
Article	Top 20 Docker Security Tips (	https://towardsdatascience.com/top-20-docker-security-tips-81c41dd06f57	)
Article	Container Security (	https://blog.pentesteracademy.com/learning-path-container-security-9a9c47760250	)
YouTube	IBM Technology: Container Security Explained (	https://www.youtube.com/watch?v=b_euX_M82uI	)

YouTube	The Linux Foundation: Container Security 101 (	https://www.youtube.com/watch?v=PDDiOl7ckzQ	)
YouTube	HackerSploit: Docker Security Essentials (	https://www.youtube.com/watch?v=KINjl1tlo2w	)
YouTube	HackerSploit: Auditing Docker Security (	https://www.youtube.com/watch?v=mQkVB6KMHCg	)

Memory forensics:

Memory forensics (sometimes called memory analysis) refers to the analysis of volatile data in a computer's memory dump. Information security professionals perform memory forensics to investigate and identify attacks or malicious behavior that do not leave easily detectable traces on the hard drive data.

Contents

Article	Memory Analysis For Beginners (	https://infosecwriteups.com/memory-analysis-for-beginners-with-volatility-coreflood-trojan-part-1-89981433eeb6	)
Article	First steps to volatile memory analysis (	https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1	)
Article	Analyzing Memory Dump with Volatility (	https://blog.pentesteracademy.com/analyzing-memory-dump-with-volatility-302f30917713	)
Article	Memory Analysis For Beginners With Volatility (	https://infosecwriteups.com/memory-analysis-for-beginners-with-volatility-coreflood-trojan-part-2-42bdb46683f2	)
YouTube	13Cubed: Introduction to Memory Forensics (	https://www.youtube.com/watch?v=1PAGcPJFwbE	)
YouTube	DFIRScience: Introduction to Memory Forensics with Volatility 3 (	https://www.youtube.com/watch?v=Uk3DEgY5Ue8&ab_channel=DFIRScience	)
YouTube	SANS Digital Forensics and Incident Response: Using Memory Analysis for Faster Response to User Investigations (	https://www.youtube.com/watch?v=QzPk1oyzMzc	)
YouTube	13Cubed: Introduction to Windows Forensics (	https://www.youtube.com/watch?v=VYROU-ZwZX8	)

Network forensics:

Network forensics refers to the collection, monitoring, and analysis of network activities to discover the source of attacks, viruses, intrusions, or security breaches that occur on a network or in network traffic. As such, network forensics is considered along with mobile forensics or digital image forensics as residing under the umbrella of digital forensics.

Contents

Article	Network Analysis (	https://medium.com/@wenhaowu92/network-analysis-travel-time-and-accessibility-5848b4ae5f65	)
Article	What is Network Analysis? (	https://towardsdatascience.com/network-analysis-d734cd7270f8	)
Article	Using Wireshark to show you, how unsecure a public network can be (	https://bernardosr1.medium.com/using-wireshark-to-show-you-how-unsecure-a-public-network-can-be-f93e373767a8	)
Article	Analyzing a bot-infected host with Wireshark (	https://medium.com/geekculture/analyzing-a-bot-infected-host-with-wireshark-c707068fffa2	)
YouTube	Semi Yulianto: Digital Forensics – Analyzing Network Traffic (	https://www.youtube.com/watch?v=jPQCHZlN88g	)
YouTube	FreeEduHub: Network Forensics (	https://www.youtube.com/watch?v=VkIrX2IfCNk	)
YouTube	edureka!: Cybersecurity & Digital Forensics Tutorial (	https://www.youtube.com/watch?v=cg1p3SRZHNY	)
YouTube	Netsec Explained: Advanced Wireshark Network (	https://www.youtube.com/watch?v=e_dsGhvq9CU	)

PowerShell scripting for security:

A hidden script can be malicious and difficult to detect with visual inspection during the script approval process. Visually review PowerShell scripts and use inspection tools to help detect suspicious script issues. These tools cannot always determine the intent of the PowerShell author, so they may draw attention to a suspicious script.

Contents

Article	Using PowerShell for Password Security	https://medium.com/@jeffreypinkstaff/using-powershell-for-password-security-checks-	)

	Checks (	[3e229c39303](#))
Article	PowerShell — Testing your workstation security posture (	https://medium.com/@smurf3r5/powershell-testing-your-workstation-security-posture-add06d4061eb)
Article	Malicious PowerShell Usage Detection (	https://0xneel.medium.com/malicious-powershell-usage-detection-f0ce9b6cca81)
Article	Encrypt & Decrypt Data with PowerShell (	https://medium.com/@sumindaniro/encrypt-decrypt-data-with-powershell-4a1316a0834b)
Article	Run PowerShell without Powershell.exe (	https://bank-security.medium.com/how-to-running-powershell-commands-without-powershell-exe-a6a19595f628)
YouTube	QuickStart: Using PowerShell for Cyber Security (	https://www.youtube.com/watch?v=K9zVwijJ4nk)
YouTube	Michael Ferrie: Scripting for Security 1 - Introduction to PowerShell (	https://www.youtube.com/watch?v=XQIVi_OJ2ZA)
YouTube	SecurityFWD: Beginner's Guide to Building AD Security Tools with PowerShell (	https://www.youtube.com/watch?v=Kk7nJe1T-ik)

Level 3

Network Security Architecture:

Network security prepares you for tasks such as protecting company data from theft, damage, disruption, and more. A network security professional will design and implement a secure architecture for network devices, as well as provide security support and ensure their integrity.

Contents

Article	Network Architecture and How to Design a Secure Network (	https://nirasha.medium.com/network-architecture-and-how-to-design-a-secure-network-669848bff76c)
Article	Cybersecurity Architecture (	https://medium.com/cloud-security/cybersecurity-architecture-66714e39bd91)
Article	Security Architecture is Not A Checklist (	https://medium.com/cloud-security/security-architecture-is-not-a-checklist-b86f1dc0aa0c)

Article	CCNA security (	https://hamzamhirsi.medium.com/ccna-security-part-1-networking-security-concepts-aeaab60b506e)
YouTube	edureka!: Network Security Tutorial (	https://www.youtube.com/watch?v=6Jubl1UnJTE)
YouTube	Snap One: Networking Design (	https://www.youtube.com/watch?v=sckuGYiHYRA)
YouTube	SANS Institute: Introduction to Security Architecture (	https://www.youtube.com/watch?v=LREcVbHiqTo&ab_channel=SANSInstitute)

Threat Hunting:

Threat hunting is the practice of proactively looking for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find malicious actors in your environment that have made it past the initial endpoint security defenses.

Contents

Article	Threat Hunting: The Basics (	https://kostas-ts.medium.com/threat-hunting-series-the-basics-cccadac830c6)
Article	The Threat Hunting Process (	https://kostas-ts.medium.com/threat-hunting-series-the-threat-hunting-process-f76583f2475b)
Article	What Makes a Good Threat Hunter (	https://kostas-ts.medium.com/threat-hunting-series-what-makes-a-good-threat-hunter-e2b1d0d07e8c)
Article	Threat Hunting Guide (	https://medium.com/@joshuaspeshock/threat-hunting-guide-5cd1444d8d95)
YouTube	The PC Security Channel: Threat Hunting Tutorial - Introduction (	https://www.youtube.com/watch?v=qrZsc5lkchI&ab_channel=ThePCSecurityChannel)
YouTube	SANS EMEA: Effective (Threat) Hunting Techniques (	https://www.youtube.com/watch?v=JmKSnRMW_6w&ab_channel=SANSEMEA)
YouTube	SANS Institute: Hunting for Post-Exploitation Stage Attacks with Elastic Stack (	https://www.youtube.com/watch?v=PdCQChYrxXg)

Physical security:

Physical security is the protection of people, property, and physical assets from actions and events that could cause harm or loss. Although often overlooked in favor of cyber security, physical security is equally important.

Contents

Article	What Is Physical Security (	https://www.sine.co/blog/what-is-physical-security-understanding-workplace-safety/	)
Article	Cyber Security and Physical Security (	https://rchen8.medium.com/cyber-security-and-physical-security-are-very-different-22e31a933907	)
Article	What is a Physical Security Architect? (	https://jay-pang.medium.com/what-is-a-physical-security-architect-2e8bd8b4b130	)
YouTube	Tom Olzak: Physical Security Part 1 - Intro and Site Barriers (	https://www.youtube.com/watch?v=j9MQMVn3FV4	)
YouTube	Tom Olzak: Physical Security Part 2 - Walls, Doors, and Locks (	https://www.youtube.com/watch?v=EAeVUDMDSn4	)
YouTube	Tom Olzak: Physical Security Part 3 - Lights, Sensors, and Alarms (	https://www.youtube.com/watch?v=tyFkj5UrPJQ	)
YouTube	Tom Olzak: Physical Security Part 4 - Environmental Controls (	https://www.youtube.com/watch?v=o_ENagQ60nY	)

Incident Response Management:

Incident response is a structured process that organizations use to identify and handle cyber security incidents. The response includes several stages, including incident preparation, detection and analysis of a security incident, containment, eradication and full recovery, and post-incident analysis and learning.

Contents

Article	Incident Management (	https://hugooodias.medium.com/incident-management-8defb3812352	)
Article	An Incident Response Plan for Startups (	https://medium.com/starting-up-security/an-incident-response-plan-for-startups-26549596b914	)
Article	Incident Response Management (	https://fergusmacdermot.medium.com/incident-management-methods-cb9274c264fe	)
Article	Cybersecurity incident response plan (	https://strategicoutlook.medium.com/why-organizations-need-to-have-a-formal-cyber-security-incident-response-plan-2c13f2e4082	)
YouTube	Ascend Technologies: The Six Phases of Incident Response (	https://www.youtube.com/watch?v=X4IPEpATNxg	)

YouTube	Skillset: Incident Response Plan (	https://www.youtube.com/watch?v=PhROeWMPBqU)
YouTube	WissenX Akademie: Incident Response Process, Lifecycle & Methodology (	https://www.youtube.com/watch?v=Sr8tfoZJa3M)

Malware analysis:

Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL. The output of the analysis helps in the detection and mitigation of the potential threat.

Contents

Article	Malware Analysis- The art of understanding malware (	https://medium.com/techiepedia/malware-analysis-the-art-of-understanding-malware-ffc5e69feb3e)
Article	Malware Analysis 101 - Basic Static Analysis (	https://infosecwriteups.com/malware-analysis-101-basic-static-analysis-db59119bc00a)
Article	Malware Analysis — Tools And Resources (	https://nasbench.medium.com/malware-analysis-tools-and-resources-16eb17666886)
Article	Malware Analysis 101 - Sandboxing (	https://infosecwriteups.com/malware-analysis-101-sandboxing-746a06432334)
Article	Malware Analysis: Introduction to YARA (	https://medium.com/@ammadb/malware-analysis-introduction-to-yara-e11b89e02ba6)
YouTube	HuskyHacks: AMO - Malware Analysis In 5+ Hours - Full Course (	https://www.youtube.com/watch?v=qA0YcYMRWyI&ab_channel=HuskyHacks)
YouTube	OpenSecurityTraining2: Reverse Engineering Malware (Playlist) (	https://www.youtube.com/playlist?list=PLUFkSN0XLZ-kwukmQOAgCZ08C5REoZEIt)
YouTube	CryptoCat: Intro to Binary Exploitation (Playlist) (	https://www.youtube.com/playlist?list=PLHUKi1UlEgOIc07Rfk2Jgb5fZbxDPec94)

Software Application Security:

Application security describes the application-level security measures that aim to prevent data or code within the application from being stolen or hacked. It covers security considerations that occur during application development and design, but

also involves systems and approaches to securing applications after they are deployed.

Contents

Article	Application security vs. software security (	https://medium.com/@SW_Integrity/application-security-vs-software-security-whats-the-difference-3d345413927c	)
Article	A Comprehensive Guide To Application Security (	https://medium.com/edureka/application-security-tutorial-e6a0dda25f5c	)
Article	Application Security Best Practices (	https://medium.com/@cloud_tips/application-security-best-practices-c63b79f29a99	)
Article	Importance of Software Security (	https://medium.com/nerd-for-tech/importance-of-software-security-application-security-non-technical-hacking-encryption-and-365c93def04e	)
YouTube	Application Security 101 - What you need to know in 8 minutes (	https://www.youtube.com/watch?v=Dp019cWu1cg&t=1s&ab_channel=Snyk	)
YouTube	edureka!: Application Security (	https://www.youtube.com/watch?v=gfFKuiZ9Y7s	)
YouTube	GOTO Conferences: Secure by Design – the Architect's Guide to Security Design Principles (	https://www.youtube.com/watch?v=4qN3JBGd1g8	)
YouTube	Cybr: Introduction to Application Security - Course (	https://www.youtube.com/watch?v=3QOlo2pEpvc&ab_channel=Cybr	)

Zero Trust architecture:

Zero Trust is a network security model based on the philosophy that no person or device inside or outside an organization's network should be given access to connect to IT systems or services until they are authenticated and continuously verified.

Contents

Article	NIST - Zero Trust Architecture (	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf	)

Article	What does Zero Trust Architecture stand for? (	https://medium.com/databulls/what-does-zero-trust-architecture-stand-for-3facb50226b4)
Article	Zero Trust Architecture (	https://medium.com/geekculture/to-the-letter-zero-trust-architecture-zta-according-to-nist-800-207-1-3cf2b23d383b)
Article	What Is Zero Trust Architecture (	https://medium.com/magalix/what-is-zero-trust-architecture-and-how-does-it-work-23067912335c)
YouTube	IBM Technology: Zero Trust Explained in 4 mins (	https://www.youtube.com/watch?v=yn6CPQ9RioA&ab_channel=IBMTechnology)
YouTube	The CISO Perspective: What is Zero Trust Network Access (	https://www.youtube.com/watch?v=DLQAbJm4gFM)
YouTube	John Savill's Technical Training: Understanding and Getting Started with Zero Trust (	https://www.youtube.com/watch?v=hhS8VdGnfOU&ab_channel=JohnSavill%27sTechnicalTraining)
YouTube	IBM Technology: Cybersecurity and Zero Trust (	https://www.youtube.com/watch?v=FMMWSLIcaME&ab_channel=IBMTechnology)

Cloud Security:

Cloud security, also known as cloud computing security, is a set of security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, control access to data and resources, and protect data privacy. They also support regulatory data compliance.

Contents

Article	Security in Cloud Computing (	https://medium.com/cyversity/security-in-cloud-computing-8d77b20e7a2d)
Article	What Is Cloud Security Posture Management? (	https://blog.cloudboost.io/what-is-cloud-security-posture-management-7ca9650d18e6)
Article	Cloud Applications (	https://medium.com/databulls/new-era-cloud-applications-concept-and-security-4ccfe29db9d7)

Concept (

Article	Security IN the Cloud vs Security OF the Cloud (	https://medium.com/nerd-for-tech/security-in-the-cloud-vs-security-of-the-cloud-114dbcf962a9	)
YouTube	IBM Technology: What is Cloud Security? (	https://www.youtube.com/watch?v=jl8IKpjiCSM	)
YouTube	edureka!: Cloud Security Tutorial (	https://www.youtube.com/watch?v=0Iw4KU5wHsk	)
YouTube	Simplilearn: Cloud Security Fundamentals (	https://www.youtube.com/watch?v=M_9hRPVH5SA	)

Continuous Security - Automation and Monitoring:

Continuous security monitoring is an approach to security that involves automating a significant part of security management. This includes vulnerability detection, monitoring of cloud configurations, identities and their rights, and data security.

Contents

Article	Continuous Security (	https://medium.com/digital-transformation-and-platform-engineering/devsecops-automation-and-continuous-security-4b720d0082f0	)
Article	Continuous Security: A Necessity on Cloud (	https://nutanix.medium.com/continuous-security-a-necessity-on-cloud-848e6ef9cace	)
Article	DevOps Tools: Automation, Monitoring, CI/CD, and More (	https://altexsoft.medium.com/devops-tools-automation-monitoring-ci-cd-and-more-ac7c4ca31879	)
Article	Log Analysis for Digital Forensic Investigation (	https://medium.com/mii-cybersec/log-analysis-for-digital-forensic-investigation-e4a00f5a5c09	)
YouTube	SANS Cloud Security: Information Security Continuous Monitoring (	https://www.youtube.com/watch?v=1V5FyasVMaM	)
YouTube	Cyber Security Entertainment: Information Security Continuous Monitoring (ISCM) (	https://www.youtube.com/watch?v=2epVP58kn_Q	)
YouTube	WissenX Akademie: SOAR - Security Orchestration Automation and Response (	https://www.youtube.com/watch?v=i7H7VYkfUEw	)
YouTube	AppSec California: Continuous Cloud Security Monitoring (CCSM) (	https://www.youtube.com/watch?v=ePCK8quTP2o	)

Auxiliary Skill: Systems and technologies

Python - Fundamentals:

Python is a high-level, general-purpose programming language that is widely used in web applications, software development, data science, and machine learning. Its design philosophy emphasizes code readability with the use of significant indentation. Python is dynamically typed and garbage-collected.

Knowing the primitive types

Declaring variables, considering the different types

Using conditional structures ('if', 'else')

Knowing the assignment and comparison operators

Using repetition structures and loops ('while', 'for')

Using functions, passing parameters and arguments

Manipulating methods

Manipulating arrays and lists

Getting data from an API

Creating constructors

Contents

WebSite Documentation Python (https://docs.python.org/3/tutorial/)

WebSite W3Schools: Python Tutorial (https://www.w3schools.com/python/)

WebSite W3Schools: Python Variables (https://www.w3schools.com/python/python_variables.asp)

WebSite W3Schools: Python Data Types (https://www.w3schools.com/python/python_datatypes.asp)

WebSite W3Schools: Python Strings (https://www.w3schools.com/python/python_strings.asp)

WebSite W3Schools: Python Operators (https://www.w3schools.com/python/python_operators.asp)

WebSite W3Schools: Python If ... Else (https://www.w3schools.com/python/python_conditions.asp)

WebSite	W3Schools: Python While Loops (	https://www.w3schools.com/python/python_while_loops.asp)
WebSite	W3Schools: Python For Loops (	https://www.w3schools.com/python/python_for_loops.asp)
Article	What is Python? (https://aws.amazon.com/what-is/python/?nc1=h_ls)	
Article	Introduction to Python Classes (	https://towardsdatascience.com/introduction-to-python-classes-da526ff745df)
YouTube	Programming with Mosh: Python for Beginners - Learn Python in 1 Hour (	https://www.youtube.com/watch?v=kqtD5dpn9C8)
YouTube	freeCodeCamp.org: Learn Python - Full Course for Beginners (	https://www.youtube.com/watch?v=rfscVS0vtbw)

Computer Networking - Fundamentals:

A computer network is a mesh that interconnects thousands of computer systems for the transmission of data. Also known as nodes, these interconnected devices send, receive, and exchange data, voice, and video traffic, thanks to the hardware and software that make up the environment.

Contents

Article	Short summary regarding ISO/OSI Model (Computer Networks) (	https://medium.com/@anmolify/short-summary-regarding-iso-osi-model-computer-networks-53b025faafe8)
WebSite	GeeksForGeeks: Basics of Computer Networking (	https://www.geeksforgeeks.org/basics-computer-networking/)
WebSite	Digital Ocean: Understanding IP Addresses, Subnets, and CIDR Notation for Networking (	https://www.digitalocean.com/community/tutorials/understanding-ip-addresses-subnets-and-cidr-notation-for-networking)
WebSite	GeeksForGeeks: TCP/IP Model (https://www.geeksforgeeks.org/tcp-ip-model/)	
WebSite	SimpliLearn: The Best Guide To Understand What Is TCP/IP (	https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-tcp-ip-model)

Model (

YouTube Fireship: Computer Networking in 100 Seconds (https://www.youtube.com/watch?v=keeqnciDVOo&ab_channel=Fireship)

YouTube freeCodeCamp.org: Computer Networking Course (https://www.youtube.com/watch?v=qiQR5rTSshw&ab_channel=freeCodeCamp.org)

YouTube My CS: Computer Networking Complete Course - Basic to Advanced (https://www.youtube.com/watch?v=0PbTi_Prpgs&ab_channel=MyCS)

YouTube Vinsloev Academy: Learn Wireshark in 10 minutes (https://www.youtube.com/watch?v=lb1Dw0eIw0Q&ab_channel=VinsloevAcademy)

Course Enterprise Networking, Security, and Automation (https://www.netacad.com/courses/networking/ccna-enterprise-networking-security-automation)

Course Switching, Routing, and Wireless Essentials (https://www.netacad.com/courses/networking/ccna-switching-routing-wireless-essentials)

Course Introduction to Networks (https://www.netacad.com/courses/networking/ccna-introduction-networks)

HTTP - Fundamentals:

HTTP stands for Hyper Text Transfer Protocol. Communication between client computers and web servers is done by sending HTTP Requests and receiving HTTP Responses.

Understanding the difference between HTTP verbs

Testing requests and checking the status codes in the browser

Learning how to make a HTTP request on the command line with WGET

Downloading an image with WGET

Performing a POST

Contents

WebSite W3Schools: What is HTTP? (https://www.w3schools.com/whatis/whatis_http.asp)

WebSite MDN Web Docs: An overview of HTTP (https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview)

WebSite MDN Web Docs: HTTP request methods (https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods)

`WebSite`HTTP Cats (https://http.cat/)

`WebSite`HTTP Dogs (https://http.dog/)

`Article`	HTTP codes as Valentine's Day comics (	https://medium.com/@hanilim/http-codes-as-valentines-day-comics-8c03c805faa0)
`Article`	Here Are the most popular ways to make an HTTP request in JavaScript (	https://medium.com/free-code-camp/here-is-the-most-popular-ways-to-make-an-http-request-in-javascript-954ce8c95aaa)
`YouTube`	Traversy Media: HTTP Crash Course & Exploration (	https://www.youtube.com/watch?v=iYM2zFP3Zn0)
`YouTube`	Curious Code: HTTP Request Methods - GET, POST, PUT, DELETE (	https://www.youtube.com/watch?v=tkfVQK6UxDI)
`YouTube`	freeCodeCamp.org: Postman Beginner's Course - API Testing (	https://www.youtube.com/watch?v=VywxIQ2ZXw4)

Cloud - Fundamentals:

Cloud, or cloud computing, is the distribution of computing services over the Internet using a pay-as-you-go pricing model. A cloud is composed of various computing resources, ranging from the computers themselves (or instances, in cloud terminology) to networks, storage, databases, and everything around them. In other words, everything that is normally needed to set up the equivalent of a server room, or even a complete data center, will be ready to use, configured, and run.

Knowing the difference between IaaS, PaaS and SaaS

Knowing the largest cloud providers

Specializing in a specific provider of your choice

Contents

`WebSite`	Microsoft Azure: What is cloud computing? (	https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/)
`WebSite`	Amazon AWS: What is cloud computing? (	https://aws.amazon.com/en/what-is-cloud-computing/)
`Article`	A beginner's guide to the basics of what cloud computing is about (	https://scientya.com/a-beginners-guide-to-the-basics-of-what-cloud-computing-is-about-e8b3b7f25a30/)

Article	Cloud Computing for Beginners (	https://medium.com/hackernoon/cloud-computing-for-beginners-85d168959afb/)
Article	What are Cloud Computing Services [IaaS, CaaS, PaaS, FaaS, SaaS] (	https://medium.com/@nnilesh7756/what-are-cloud-computing-services-iaas-caas-paas-faas-saas-ac0f6022d36e)
YouTube	Simplilearn: Cloud Computing Tutorial for Beginners (	https://www.youtube.com/watch?v=RWgW-CgdIk0)
YouTube	Amazon Web Services: What is Cloud Computing? - Amazon Web Services (	https://www.youtube.com/watch?v=mxT233EdY5c)
YouTube	Ecourse Review: Cloud Computing Services Models - IaaS PaaS SaaS Explained (	https://www.youtube.com/watch?v=36zducUX16w/)

Command Line - Fundamentals:

CLI is a command line program that accepts text input to execute operating system functions.

Knowing the most important commands

Contents

WebSite	W3Schools: What is Command Line Interface (CLI)? (	https://www.w3schools.com/whatis/whatis_cli.asp)
WebSite	Microsoft Docs: Using command line arguments for Windows Terminal (	https://docs.microsoft.com/en-us/windows/terminal/command-line-arguments?tabs=windows)
Article	Advanced CLI: Commands You Should Know as a Developer (	https://betterprogramming.pub/advanced-cli-commands-you-should-know-as-a-developer-7bc48c752a5e)
YouTube	freeCodeCamp.org: Command Line Crash Course (	https://www.youtube.com/watch?v=yz7nYlnXLfE)
YouTube	Traversy Media: Command Line Crash Course For Beginners - Terminal Commands (	https://www.youtube.com/watch?v=uwAqEzhyjtw)

Linux - Fundamentals:

Linux is a term popularly used to refer to operating systems that use the Linux Kernel. Distributions include the Linux Kernel as well as system software and libraries.

Knowing the Linux directory system

Compacting and uncompressing files

Editing files in the console with VI

Managing the processes running on the machine

Knowing the environment variables and PATH

Managing packages

Performing remote communication with SSH and SCP

Contents

WebSite Digital Ocean: An Introduction to Linux Basics (https://www.digitalocean.com/community/tutorials/an-introduction-to-linux-basics)

WebSite Ubuntu: The Linux command line for beginners (https://ubuntu.com/tutorials/command-line-for-beginners#1-overview)

Article 10 Linux Commands Every Developer and DevOps Should Learn (https://medium.com/javarevisited/10-essential-linux-commands-every-developer-and-devops-should-know-9df39391aac7)

Article Useful Linux Commands — Files and Packages (https://blog.devgenius.io/useful-linux-commands-files-and-packages-ccd80da6da2b)

YouTube freeCodeCamp.org: Introduction to Linux – Full Course for Beginners (https://www.youtube.com/watch?v=sWbUDq4S6Y8)

YouTube freeCodeCamp.org: The 50 Most Popular Linux & Terminal Commands (https://www.youtube.com/watch?v=ZtqBQ68cfJc)

Course MIT - The Missing Semester of Your CS Education (inglês) (https://missing.csail.mit.edu/)

Auxiliary Skill: Information Security

Risk, threats and vulnerability management:

Risk management is the process of planning, organizing, and controlling resources and people to minimize damage or turn risks into opportunities. Predicting risks is an important practice, after all, this way it is possible to reverse what can go wrong and achieve positive results along the way.

Contents

`WebSite`CVSS (https://nvd.nist.gov/vuln-metrics/cvss)

`WebSite` What is vulnerability management? (https://www.ibm.com/topics/vulnerability-management)

`WebSite`Common Vulnerability Scoring System (https://www.first.org/cvss/user-guide)

`YouTube` Microsoft 365: Threat and Vulnerability Management (https://www.youtube.com/watch?v=Ez1s7nIgUPY&ab_channel=Microsoft365)

`YouTube` Josh Madakor - Tech, Education, Career: Vulnerability Management (https://www.youtube.com/watch?v=IT6Px9zJM3s&ab_channel=JoshMadakor-Tech%2CEducation%2CCareer)

`YouTube` edureka!: Cybersecurity Risk Management Simplified (https://www.youtube.com/watch?v=X31YZYetCBg&ab_channel=edureka%21)

Confidentiality, Integrity and Availability:

The 3 fundamental principles of information security. Any good information security management program should be designed to achieve the three information security principles commonly known as CIA (CIA stands for "Confidentiality", "Integrity" and "Availability").

Contents

`Article` Three Pillars of Infosec: Confidentiality, Integrity and Availability (https://www.cybereason.com/blog/three-pillars-of-infosec-confidentiality-integrity-and-availability)

`Article` Cybersecurity 101 — A Beginner's Guide to Cybersecurity World (https://medium.com/edureka/what-is-cybersecurity-778feb0da72)

`Article` The CIA Triad: Confidentiality, Integrity https://medium.com/coinmonks/the-cia-triad-confidentiality-integrity-and-availability-)

	and Availability (	[ef54d777cbd2](#)	
YouTube	IT Governance Ltd: What is ISO 27001? | A Brief Summary of the Standard (	https://www.youtube.com/watch?v=x792wXSeAhA&ab_channel=ITGovernanceLtd	)
YouTube	Cyber Today Academy: What is ISO 27002 Standard? (	https://www.youtube.com/watch?v=A7oeQYcfJz0&ab_channel=CyberTodayAcademy	)

Identity and access management (IAM):

Identity management, also known as identity and access management (IAM), is among the information security disciplines that enable the right individuals to access the right resources at the right time for the right reasons.

Contents

Article	What is Identity and Access Management (	https://medium.com/identity-beyond-borders/identity-and-access-management-10166c309f11	)
Article	Introduction to Identity and Access Management (	https://medium.com/identity-beyond-borders/introduction-to-identity-and-access-management-2f3b80862647	)
Article	What is IAM? (	https://bojithapiyathilake.medium.com/identity-and-access-management-components-c501d786db4c	)
Article	What is IAM as a service (	https://medium.com/hypto/identity-and-access-management-iam-e04d2354a57	)
Article	Open-source Identity and Access Management System (	https://medium.com/@devops.ent/top-identity-and-access-management-systems-iam-open-source-enterprise-92cf66560a55	)
YouTube	IBM Technology: Identity & Access Management (IAM) (	https://www.youtube.com/watch?v=aNj36g7fSsU&ab_channel=IBMTechnology	)
YouTube	VMware End-User Computing: Identity and Access Management - Technical Overview (	https://www.youtube.com/watch?v=Tcvsefz5DmA&ab_channel=VMwareEnd-UserComputing	)

Security Awareness:

As cyber attacks become more prevalent and sophisticated, companies must rely more on their employees to ensure that they do not put data at risk or fall victim to ransomware. But employees are busier than ever. And, creating a culture of cybersecurity at work becomes more important and more challenging when employees work from home.

Contents

Article	Why is cyber security awareness and training for employees a must? (	https://threatcop.medium.com/why-is-cyber-security-awareness-and-training-for-employees-is-a-must-74d89645966b)
Article	Your Complete Guide To End-User Security Awareness Training (	https://medium.com/@emma.woods/your-complete-guide-to-end-user-security-awareness-training-b2812023b84a)
Article	There Is No Cyber Security Silver Bullet (	https://medium.com/seek-blog/there-is-no-cyber-security-silver-bullet-we-arent-werewolves-ec4fc5e1f13c)
YouTube	Tom Olzak: Security Awareness, Education, and Training (	https://www.youtube.com/watch?v=F6EtbBLQE9Y&ab_channel=TomOlzak)
YouTube	TreeTop Security: Cybersecurity Awareness Training Presentation (	https://www.youtube.com/watch?v=tlmpSYlhdV0&ab_channel=TreeTopSecurity)
YouTube	StaySafeOnline.org: Security Awareness Episodes (Playlist) (	https://www.youtube.com/playlist?list=PL7QHbjPSF0r6qJonaROIxVaMLzwDnZyOL)

Data protection:

Data protection is the process of protecting important information in a way that ensures the confidentiality, integrity, and availability of that data.

Contents

Article	A quick Introduction to GDPR (	https://medium.com/geekculture/a-quick-introduction-to-gdpr-bc80022673e0)
Article	GDPR The Basic Facts — GDPR Processing Principles	https://medium.com/geekculture/gdpr-the-basic-facts-gdpr-processing-principles-9774b80a0791)

	(		
Article	Best UX practices for GDPR compliance (	https://medium.com/@AukaPay/best-ux-practices-for-gdpr-compliance-563b73362095	)
YouTube	Channel 4 News: GDPR explained (	https://www.youtube.com/watch?v=acijNEErf-c&ab_channel=Channel4News	)
YouTube	Privacy Kitchen: What are the 7 principles of GDPR? (	https://www.youtube.com/watch?v=NcHSD3fWJiQ&ab_channel=PrivacyKitchen	)
YouTube	Digitool: GDPR Compliance Summary - 10 Steps in 10 Minutes to Avoid Fines (	https://www.youtube.com/watch?v=WPwG-MNMuBQ&ab_channel=Digitool	)
YouTube	Google Cloud Tech: What is Data Loss Prevention (DLP)? (	https://www.youtube.com/watch?v=OjMnlizubTU&ab_channel=GoogleCloudTech	)

Authentication and password security:

A strong password makes all the difference when it comes to data protection. After all, it is constructed in a way that makes it very difficult for it to be cracked by a hacker or mass attack. A password, you know, is a mechanism that allows a person access to a particular service.

Contents

WebSite	How Secure is Your Password? (https://www.passwordmonster.com/)		
Article	Password 101 — How to create a more secure password (	https://medium.com/belong-blog/password-101-how-to-create-a-secure-password-8adfbe888d79	)
Article	Password Security: THM Writeup (	https://medium.com/bug-bounty-hunting/password-security-thm-writeup-cc9088207af3	)
Article	What Is a Secure Password? (	https://medium.com/geekculture/what-is-a-secure-password-97263aeedea9	)
YouTube	Bit Oxygen: Authentication in Computer Security (	https://www.youtube.com/watch?v=7oTkgG1v-rU	)
YouTube	Linus Tech Tips: Password Security Best Practices (	https://www.youtube.com/watch?v=t8SQo3R7qeU	)

Alura, PM3 e FIAP

O Techguide.sh é um projeto open source