Chue Moua
Connect with me online at
https://www.linkedin.com/in/cmoua

BREAKTHROUGH INTO THE CYBERSECURITY FIELD

What is Cybersecurity?

Many experts reference Cybersecurity as a body of technologies, processes, procedures and policies that is designed to protect cloud resources.

Why Cyber? Cyber references a virtual setting of network, systems and technologies, consider it "**cloud technology**".

In today's session, we'll go through:

- Types of Data
- Architecture and Identifying exposures
- Cybersecurity Area's of focus
- Recommended Security Framework
- Entry Challenges
- Value's of being certified and what certifications hold weight
- Working in Cybersecurity – The Pro's and Con's

Types of Data

Data is the most important to any security initiative or program. You must know the 5W's of Data. "What, Why, When, Where and Who + How".

Example questions to ask yourself:

1. What data are we collecting?
2. Where is the data hosted?
3. What applications are used to collect the data and how it's collected?
4. How is the data being accessed, processed and transmitted?

Other questions would include access control, encryption, storage, etc. Think of all use cases and how you can protect the data.

A short list of data types that are heavily regulated

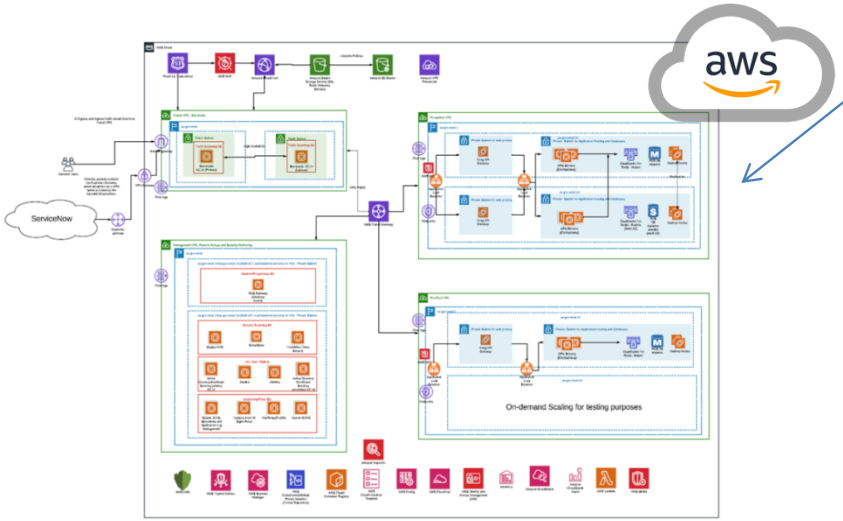
- PII – Personal Identifiable Information
- PHI – Protected Health Information
- PCI – Payment Card Industry
- CUI – Controlled Unclassified Information
- IP – corporate technology - Any data that is generated, collected or created.

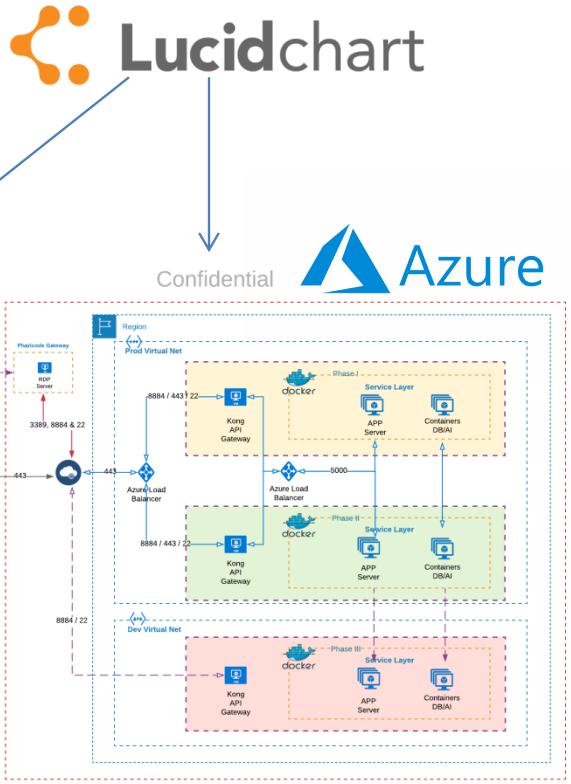
Basic Network & Architecture

Understanding the basic details of an architecture, endpoints, connectivity and network exposures will help identify risk and vulnerabilities.

- Exposable public endpoints
- Applications used
- ACL (Access Control List) - UDP/TCP ports
- Connectivity (public, customer, partner networks)
- Purpose of exposure

Network diagrams and data flow





Cybersecurity Area's of focus

The Cybersecurity space is huge and I haven't met a person that is an expert. There's forensics, pen test, AISecOps, etc. but here's a short list I've recently used for a P-ATO FedRAMP project:

- Cloud Provider – AWS, Azure, Google, IBM, Oracle Cloud, Salesforce, ServiceNow, etc.
- Firewalls – local or vFirewall – Federal Information Processing Standard (FIPS 140-2)
- Operating Systems – LINUX, Windows, MAC
- Endpoint Hardening and Vulnerability Management – Stig / CIS Compliance hardening
- Endpoint Security – Endpoint Antivirus, Antimalware, Firewall, Threat protection, etc.
- SIEM (System Information and Events Management) – Log processing
- Monitoring – Cloud, systems and applications monitoring
- Access Control and Management – Active Directory or OAUTH SAML (Security Assertion Markup Language) some sort of network authentication system and maintains ACL.
- DLP (Data Loss Prevention) - helps with insider threats to block, capture and report.
- Backup / DR / CP – Backup and restoration, Disaster Recovery and Contingency Plans.
- Configuration Management which creates baselines and automation – Puppet / Chef / Salt / Ansible
- Cloud Security, WAF (Web Application Firewall) and DNSsec
- GRC (Governance Risk Management and Compliance) – Manage the compliance lifecycle

Frameworks and Compliance

The most recommended Cybersecurity framework at the moment would be the **NIST (National Institute of Standards and Technology) SP 800-53 Framework, originally FISMA** (Federal Information Security Management Act). The NIST framework is heavily used in the Federal Government and FedRAMP (Federal Risk and Authorization Management Program).

https://nvd.nist.gov/800-53

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

Challenges

Why is it so difficult to get an entry into the Cybersecurity field?
Cybersecurity requires an understanding of cloud computing, systems, network and applications. It's not a field for beginners. Lowering and eliminating risks has been at the forefront of every security agenda.

RISKS:

- Cloud misconfigurations cost companies nearly $5 trillion last year
- Misconfiguration Remains the #1 Cause of Data Breaches in the cloud.

But you need to start some where and I will share with you the shortest path to a successful entry into Cybersecurity.

Latest news for IT or Cybersecurity field?

Newly introduced legislation in the U.S. House could deliver **$28 billion in federal funds** to state and local governments for the purposes of overall upgrades to IT and cybersecurity infrastructure.

House Bill Could Mean Billions for State, Local IT

If I was to start over…

What advice would I give my younger self?

1. RHEL (Redhat Enterprise Linux) certified

- Start with RHCSA (Red Hat Certified Systems Administrator), then onto RHCE (Redhat Certified Engineer) and finally RHCA (Redhat Certified Architect)

Why? Windows and MAC is easy to learn. Over 70% of web applications are built on LINUX. Requires an understanding of systems, networks and applications. Learn Docker, containerizing applications will be the future of simplifying automation.

2. AWS (Amazon Web Services) certified or Azure

- AWS Certified Cloud Practitioner – Foundational
- Azure Fundamentals

Why? By learning Cloud, you'll learn about IaaS. Understand systems resources , Serverless services, networking ipv4/ipv6 and subnetting, security ACL, applications, load balancing, App, firewalls, etc. This is "CYBER" in Cybersecurity.

3. CISSP or CISA Certifications

Why? Deep Understanding in security, risks, assessments, calculate and predict losses, processes, policies and analyze security with an incident response plan and resolution.

If a person hits it right and dedicates to this roadmap which takes an average 2-3 years, they can anticipate to be worth within the range of 100k-200k annually. **No college degree required!**

Value of Certifications

Education is important and I fully encourage anybody that wants to continue higher education. But it's NOT required for the Information Technology industry. A college degree doesn't guarantee you a job.

Google Will Be The Biggest Disruption In Higher Education - Forbes

Be a specialist, not a generalist.

Get certified in a product or technology. Btw, Comptia certs are the last certifications I would suggest getting. Don't bother wasting your time, it doesn't hold weight vs RHEL / AWS / Azure or CISSP.

What most IT Management and I typically look for in a candidate?

1. Experience – proven experience, if none, certifications and skills will compensate
2. Skills - intelligent, fast learner and able to elaborate in unknown areas.
3. Industry Certifications that meets a requirement will move to the top stack
4. Attitude and Personality – personable, team player, eager to learn and learns fast.
5. Education – a degree would be nice, but **not required**. Unless it's from top school such as MIT, Stanford, Princeton, Harvard, etc.
6. Diversity – this is also very important, wouldn't want the entire department all men or women, single race or religion. It needs to be diversified.

Thank you!

PRO'S: The Cybersecurity space is in shortage of talent. We need more professionals, young fresh minds and motivated individuals! There's been an increase of funding for DevOps and the Cybersecurity industry.

CON'S: Most times, you will need to be available 24/7/365! Regardless if it's Christmas, New Years, family birthdays or funerals. There is definitely flexibility and exceptions, but you do have an obligation. There could be very high stress level.

BENEFITS: It's a very rewarding position if you stay committed. It's a high paying career no matter where you go in the world. A Mon-Fri type of environment and very professional, but availability IS A MUST.

HOW TO CONNECT WITH ME.

I've set a goal for myself to mentor and help as many people as I can to be successful in Cybersecurity!

The best way to communicate with me is through LinkedIn at

https://www.linkedin.com/in/cmoua

Email: chuemoua@gmail.com

You are welcome to ask any questions, address security concerns, ask for guidance or a simple hello. Please no sales pitch asking for 30 minutes of time.