A Day in the Life of an Enterprise Security Architect

Grow, Transform

Deven Gengan
Enterprise Security Architect – Derivco

Welcome

How to start a career in Enterprise Security Architecture

Roles   Skills and Certifications

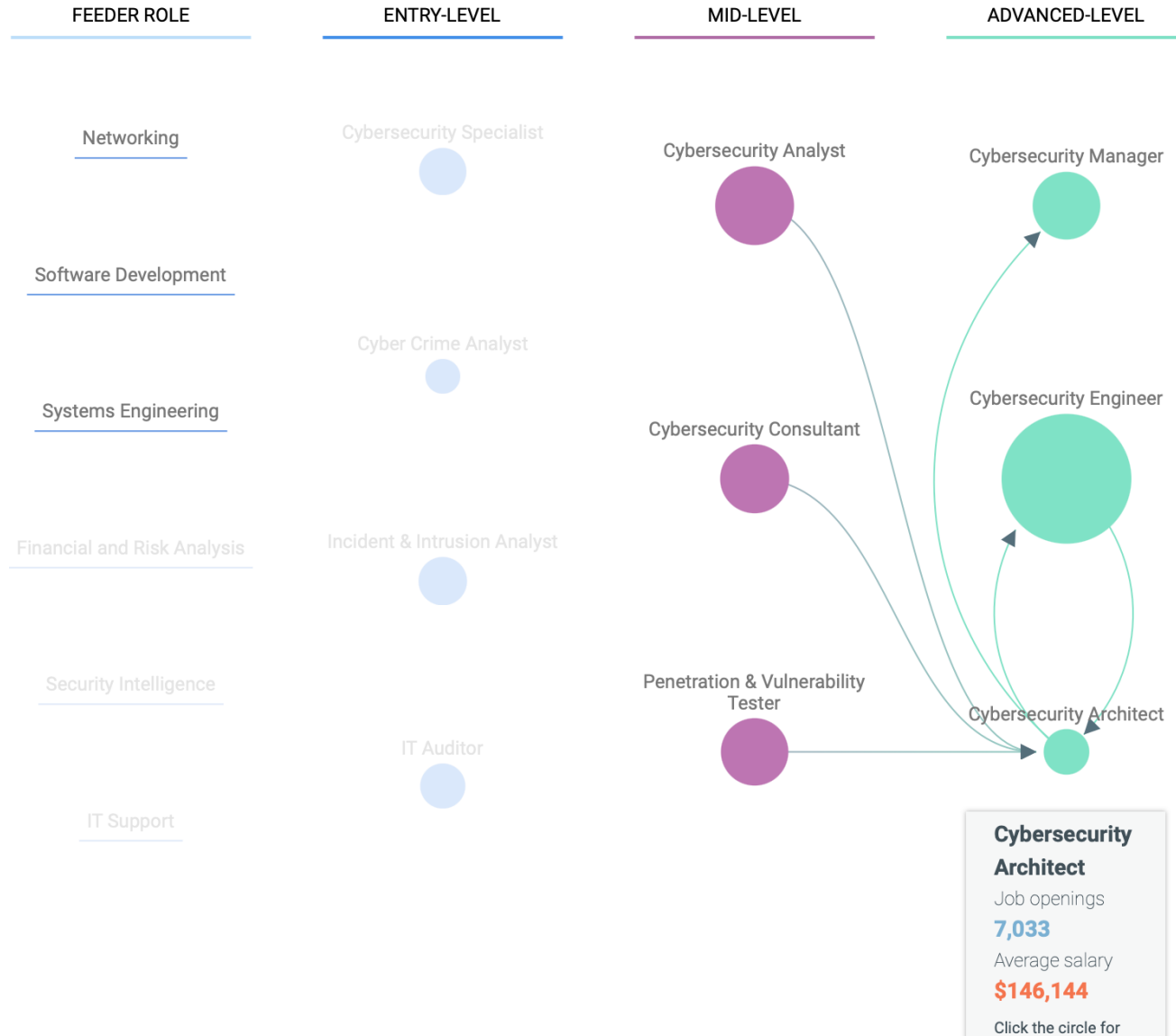| FEEDER ROLE	ENTRY-LEVEL	MID-LEVEL	ADVANCED-LEVEL
Networking	Cybersecurity Specialist	Cybersecurity Analyst	Cybersecurity Manager
Software Development			
Systems Engineering	Cyber Crime Analyst	Cybersecurity Consultant	Cybersecurity Engineer
Financial and Risk Analysis	Incident & Intrusion Analyst		
Security Intelligence		Penetration & Vulnerability Tester	Cybersecurity Architect
IT Support	IT Auditor		

- Many ways to get into ESA

- ESA is an advanced level role so skill development starts from entry level, progresses to mid-level and continues in advanced level jobs.

- In most cases, all of us as ESA's came from feeder roles in the first place !!

- So, ESA is a cumulative job with several years of experience over feeder, entry level, mid-level roles.

Source: https://www.cyberseek.org/pathway.html

How to start a career in Enterprise Security Architecture

FEEDER ROLE | ENTRY-LEVEL | MID-LEVEL | ADVANCED-LEVEL

Networking

Software Development

Systems Engineering

Financial and Risk Analysis

Security Intelligence

IT Support

Cybersecurity Specialist

Cyber Crime Analyst

Incident & Intrusion Analyst

IT Auditor

Cybersecurity Analyst

Cybersecurity Consultant

Penetration & Vulnerability Tester

Cybersecurity Manager

Cybersecurity Engineer

Cybersecurity Architect

Cybersecurity Architect
Job openings
7,033
Average salary
$146,144
Click the circle for

- A typical path, mostly found in large organizations with large security teams

- Foundational experience and knowledge is key:
  - Networking
  - Software development
  - Systems engineering

- So, ESA is a cumulative job with several years of experience over feeder, entry level, mid-level roles.

- My path
  - Career: Software Dev, Systems Eng
  - Learned the other feeder roles and explored them out of a work context.
  - Same with entry-level security roles.
  - Backup: Great investments in academics (Computer science)

Source: https://www.cyberseek.org/pathway.html

What does Enterprise Security Architecture entail ?

- Big picture thinking
- Ability to move from big picture to hands on engineering
- Some of the work deliverables
    - Strategy
    - Current state views
    - Future state views
    - Transitions
    - Proof of Concepts
    - Emerging technologies
        - Strategy to production
    - Stakeholder management
        - Internal to your organization
        - External such as regulators, technical working bodies etc

- Learning
- My decisions: OSCP or CEH : CEH because of where I was in my career .... And I did the learning for OSCP anyway !
- My decision: AWS, AZURE or CSA CCSK ? CCSK because I needed to secure both clouds quickly. And I did the learnings for AWS and Azure after that.

- Summary :
    - You always need to learn and transition your learnings into the work context as operational competence is first prize.
    - Get some core certificates that can open job opportunities.
    - For the other certificates, consider doing the learnings and transition the knowledge into the workplace !!

You don't need to go certification crazy, some *foundational certifications* to help such as CISSP ☺
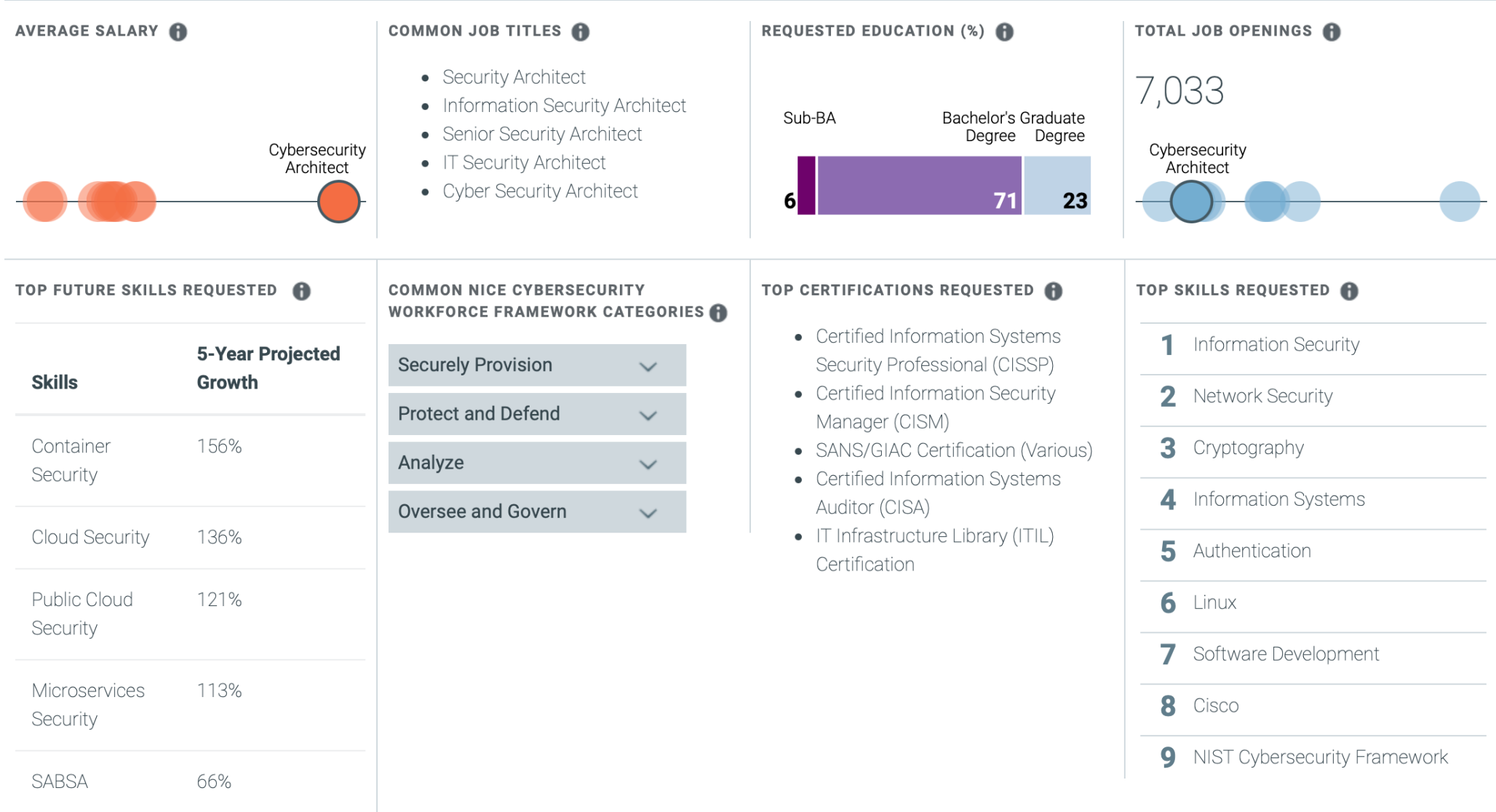
Daily tasks and functions of an Enterprise Security Architect

- Working with stakeholders
  - Meetings
  - Workshops
  - 1-1 discussions etc..
- Creating Enterprise Architecture artefacts, done with high levels of collaboration
  - Strategies
  - Frameworks
  - Current states
  - Transitions states
  - Future states
- Solutions engineering
  - Scripting
  - Infrastructure as Code
  - Creating proof of concept solutions

- Being involved in relevant operational issues

- Emerging technology research which includes sharing what you know
- Threat landscape research and reviewing threat intel relevant to your interests.
- Learning always - improve outcomes and practice methodology
- Coaching
- Mentorship
- Line management

Collaboration is key
Building relationships is what you want
Ability to write for multiple audiences and express complex topics simply
Ability to "telescope" from strategic to detailed

What is a competent and skilled Enterprise Security Architect

Cybersecurity Architect

AVERAGE SALARY ⓘ

Cybersecurity Architect

COMMON JOB TITLES ⓘ

- Security Architect
- Information Security Architect
- Senior Security Architect
- IT Security Architect
- Cyber Security Architect

REQUESTED EDUCATION (%) ⓘ

Sub-BA | Bachelor's Degree | Graduate Degree
6 | 71 | 23

TOTAL JOB OPENINGS ⓘ

7,033

Cybersecurity Architect

TOP FUTURE SKILLS REQUESTED ⓘ

Skills	5-Year Projected Growth
Container Security	156%
Cloud Security	136%
Public Cloud Security	121%
Microservices Security	113%
SABSA	66%

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES ⓘ

- Securely Provision ⌄
- Protect and Defend ⌄
- Analyze ⌄
- Oversee and Govern ⌄

TOP CERTIFICATIONS REQUESTED ⓘ

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- IT Infrastructure Library (ITIL) Certification

TOP SKILLS REQUESTED ⓘ

1. Information Security
2. Network Security
3. Cryptography
4. Information Systems
5. Authentication
6. Linux
7. Software Development
8. Cisco
9. NIST Cybersecurity Framework

Source: https://www.cyberseek.org/pathway.html

How to become a competent and skilled Enterprise Security Architect

Source: https://www.cyberseek.org/pathway.html

It can be done
The Growth Mindset

Video: understanding mindset

Play Video
must be in 'Presentation Mode' to Play video

Fixed mindset:
ability is static

Leads to a desire to look smart and therefore a tendency to:

Give up easily

See failures as fruitless or worse

Ignore useful negative feedback

Feel threatened by the success of others

Avoid challenges

Growth mindset:
ability can be developed

Leads to a desire to learn and therefore a tendency to:

Persist in the face of setbacks

See failures as essential to mastery

Learn from criticism

Find lessons and inspiration in the success of others

Embrace challenges with agility

How do mindsets show up in us & others?

Our mindsets can be applied to any ability and are flexible depending on context.

Fixed Mindset:
ability is static

Growth Mindset:
Ability can be developed

What is one personal example of when I exercised a fixed mindset?

I tried public speaking once, but I think I'm just not a natural. I think even if I did it more, I'd never be good at it.

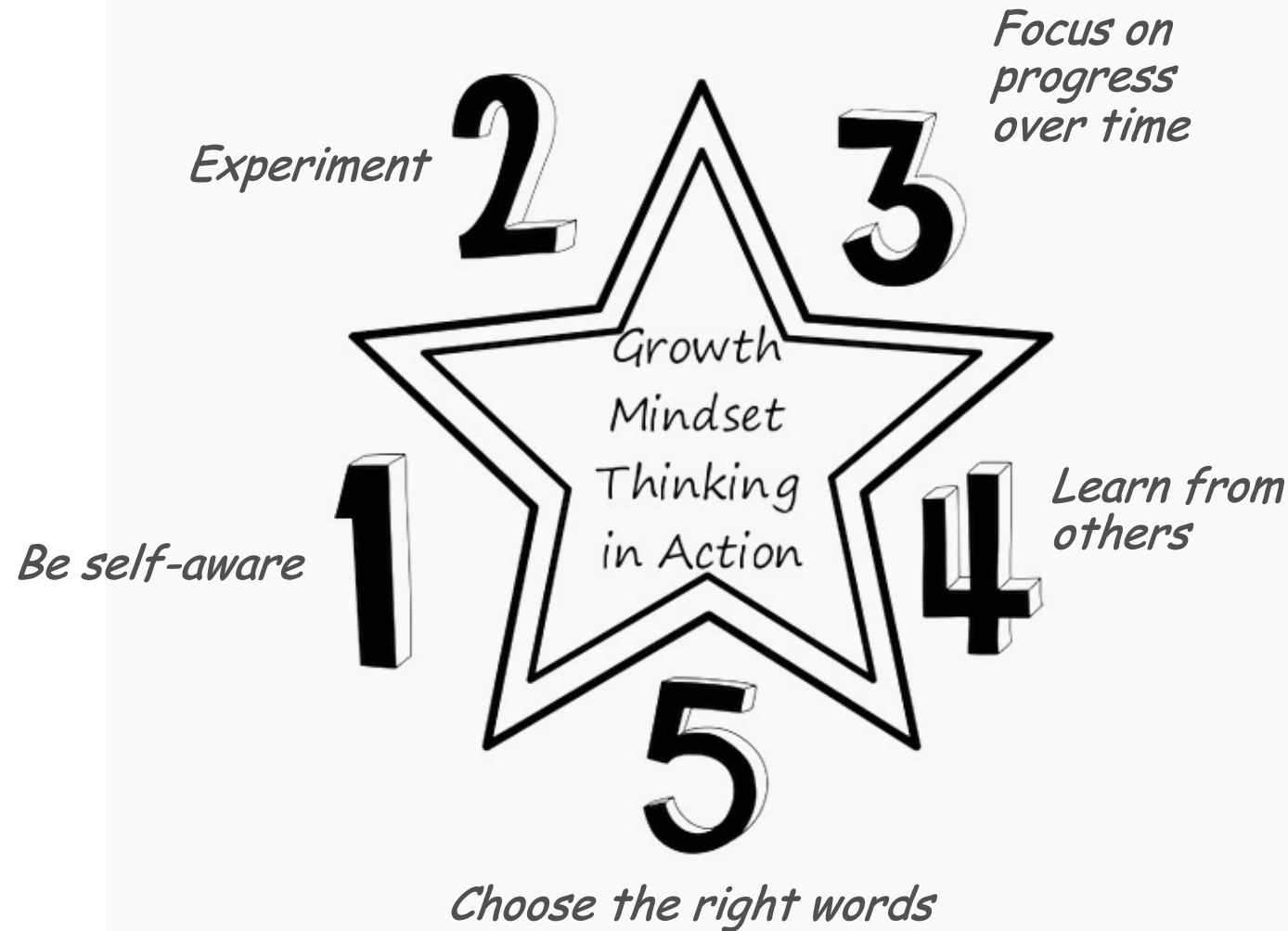**What is one personal example of when I exercised a growth mindset?**

I recently started working out; what a pain, at first! I knew if I kept it up, I'd get better. Now, I'm setting bigger goals!

Video: growth mindset thinking in action

Play Video
must be in 'Presentation Mode' to Play video

Experiment

Focus on progress over time

Be self-aware

Learn from others

Growth Mindset Thinking in Action

Choose the right words

2 3 1 4 5

Free resources

Free resources

- https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

    - 42 + free courses

    - Some recommended ones…
        - https://portswigger.net/web-security   - bug bounty hunting ☺
        - https://docs.microsoft.com/en-us/learn/browse/?term=security&terms=security   - Microsoft Azure etc
        - https://aws.amazon.com/training/   - AWS security

Speaker biography

Deven Gengan is an Enterprise Architect at Derivco concentrating on IT Security. He is very passionate about architecture frameworks and their applications in real world scenarios. He has been active in the cybersecurity community by reviewing conference submissions, trainings and exam certifications for OWASP and EC-Council.

Deven holds a HDE(UKZN), BSc(UNISA), BSc HONS(UNISA) and is currently busy with a MS in Cybersecurity Leadership. Deven is also a Certified Ethical Hacker and CISSP.

LinkedIn: https://www.linkedin.com/in/deven-g-7b054b17/
GitHub: https://github.com/DevenGengan