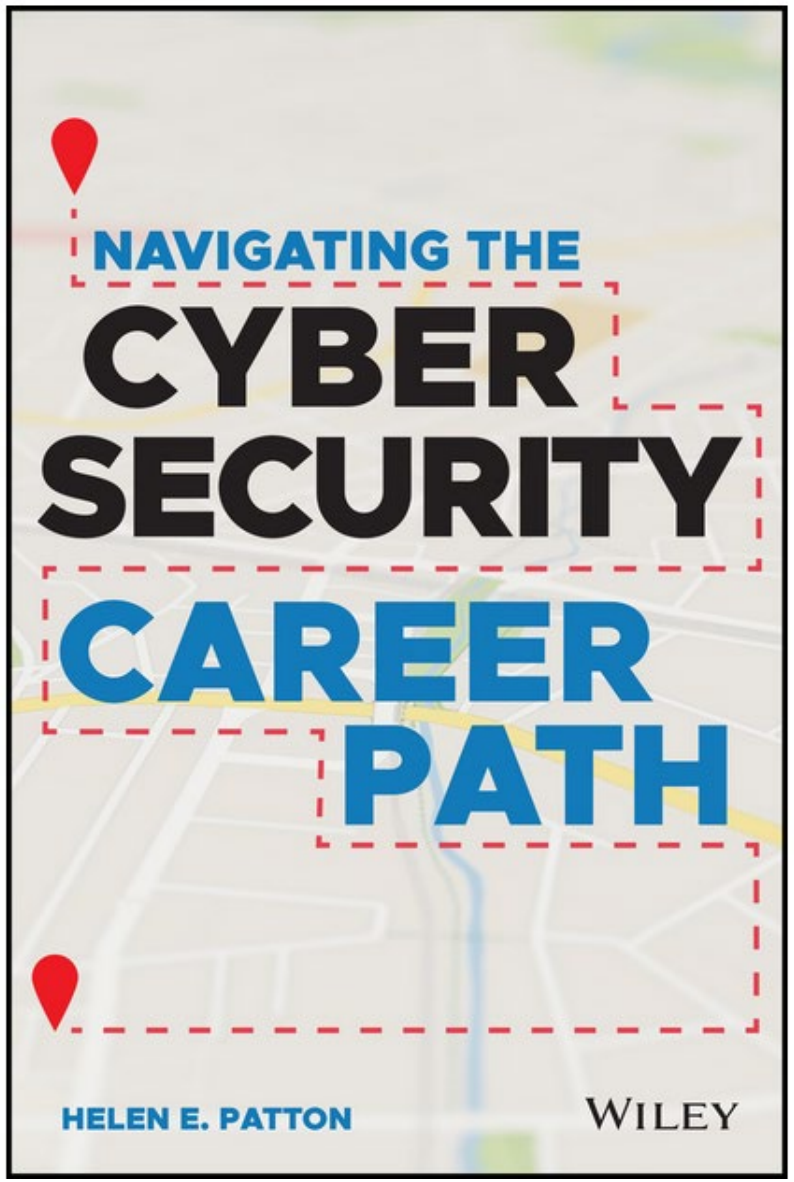
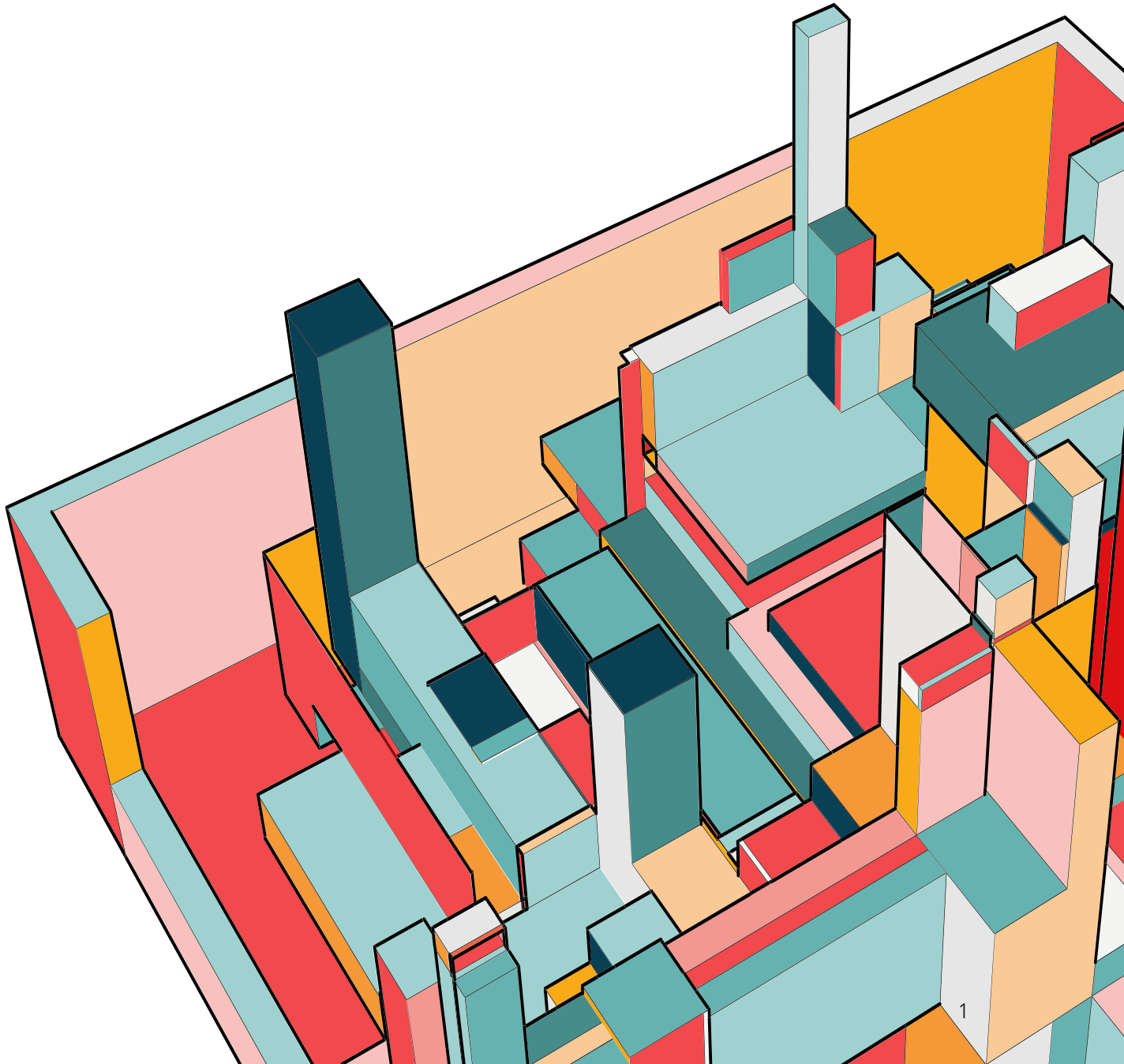

NAVIGATING THE
CYBER SECURITY
CAREER PATH
HELEN E. PATTON
WILEY



CYBERSECURITY 101

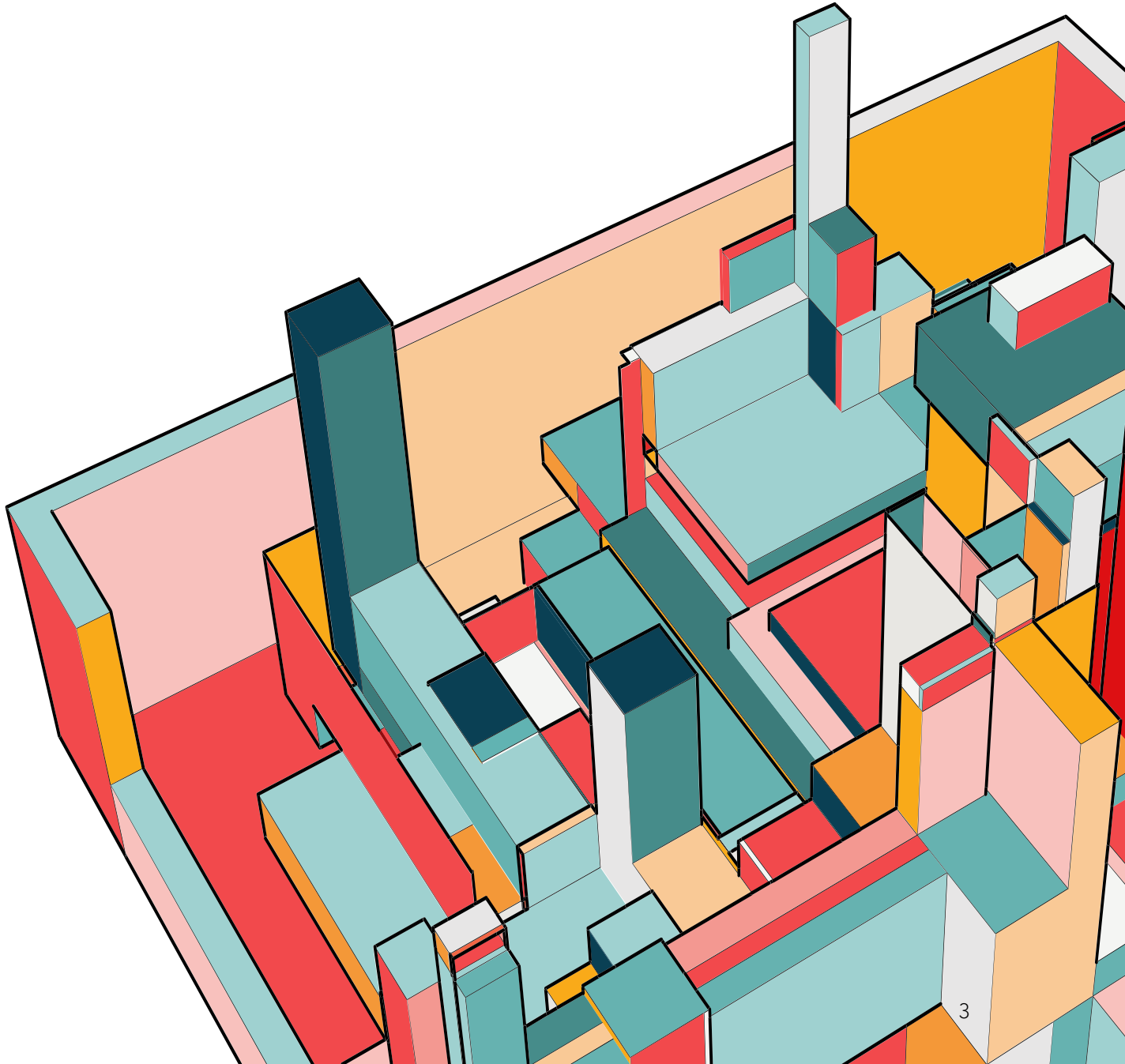
Ed Garcia – Info Tech/Cyber Warrior,
Success Coach - Strategist

ABOUT ED GARCIA

1. BS Degree in Computer Information Systems.
2. Minor in Computer Science
3. MS Degree Information Science
4. 20 years Info Tech at a Data Center HQ – 4 Mainframes @ $3-6 Million + 15,000 devices, across half of CA.
5. 22 years Teaching Info Tech/CyberSecurity Moorpark College

Current Goals:

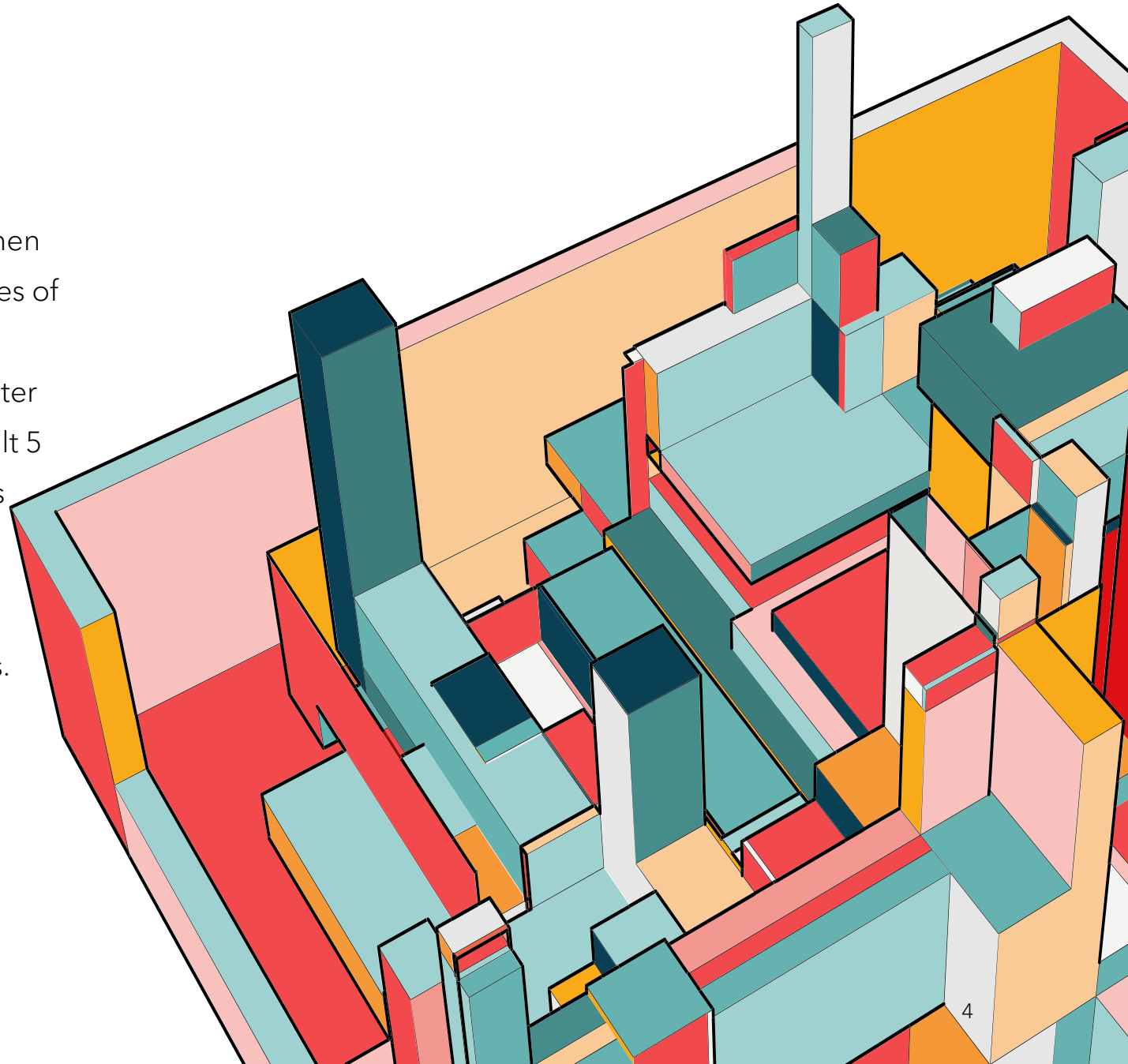
1. Developing Cloud knowledge
2. Developing Cyber Training Program
3. Coach for Student National Cyber League
4. Developing new programs, BS Degree Cyber.
5. Constantly learning…….



ABOUT MOORPARK COLLEGE

At Moorpark College - developed an A.S. Degree in Info Tech, then Developed a Cyber Security A.S. Degree Program with 15 courses of which 85% map to Professional Certification. We are also developing a Cybersecurity Bachelors Degree, applying for Center of Excellence in CyberSecurity thru NSA. Mr. Garcia has also built 5 Amazon Web Services courses, 2 Microsoft Azure courses, and is constantly updating new courses. Our newest areas of development are Cloud focused.

1. Students participate in National CyberLeague Competitions.
2. Projects include PFSense Firewalls, Network Ops in Lab env.
3. Exploring development of Cyber Ninja ranking system to further drive workplace innovation.



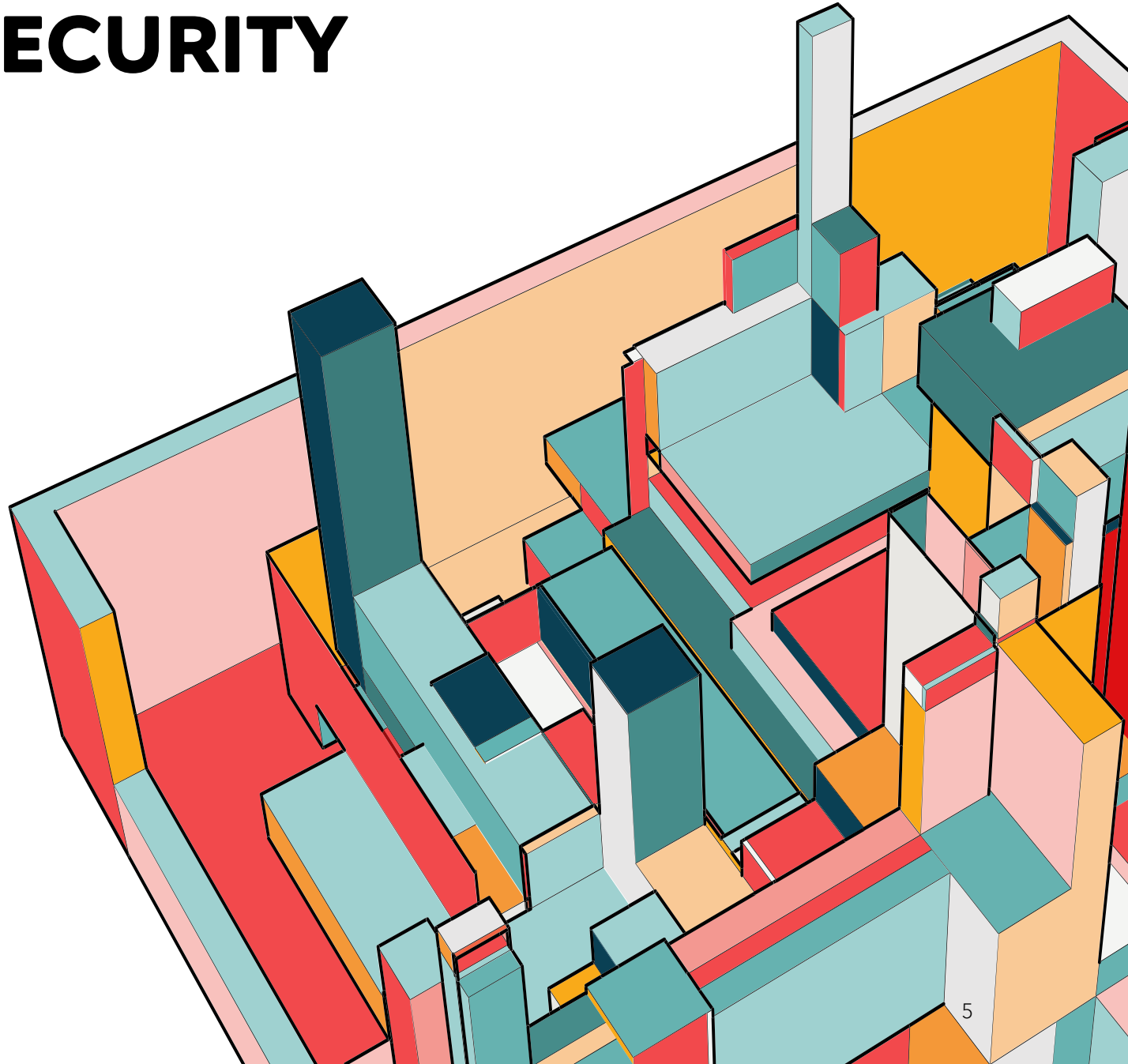
WHAT ARE CYBERSECURITY CHALLENGES –

STAY CONNECTED

https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1#areaheading-occ590

Microsoft 2021 Security Report

Internal Threats/IP Theft/Customer Lists/Vendors/software/processes/Info sharing



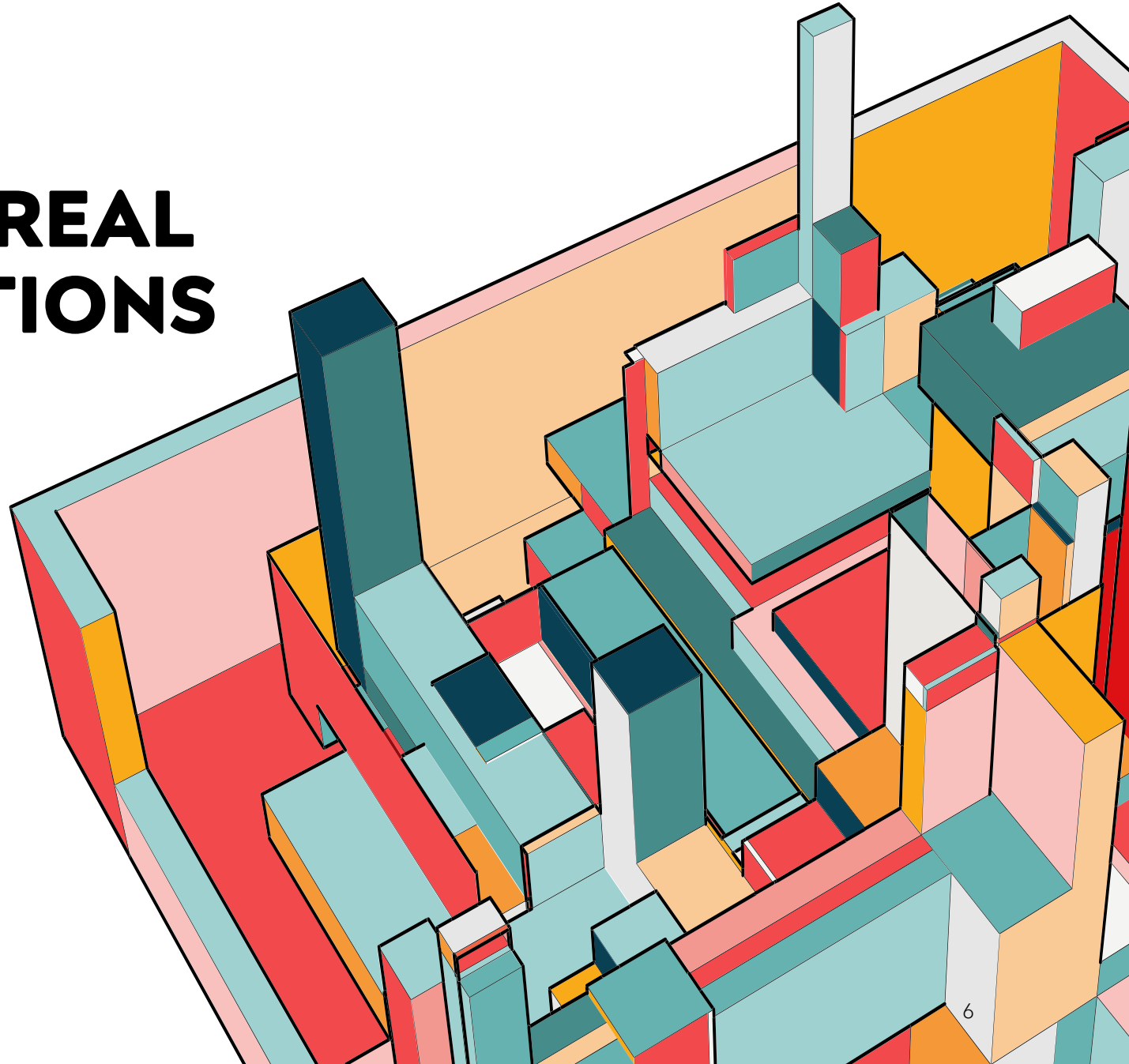
HIGH TARGETS → REAL ESTATE TRANSACTIONS

Escrow Office had a compromised email accounts.

Friend had Wire Transfer Instructions email being monitored….

Transfer Instructions sent 3 hours before real Transaction to a different account.

High Value Targets – Whale Phishing



HAVE YOUR STRATEGY FOR SUCCESS

1) Identify skills GAPs

1. Review Job Market, Employers?
2. Identify Certifications in demand – Pick one!
3. Identify Skills in Demand – Pick one!
4. Identify soft skills – Pick one!

2) Needs of Workplace/Job Market /Opportunities

1. Bosses biggest challenge
2. Morning Report
3. Web Based, DB, coworker support
4. Collaboration is key

3) Manage your time

Calendar, 8-5, Project Mgmt., weekly review,

4) Get training/network with others

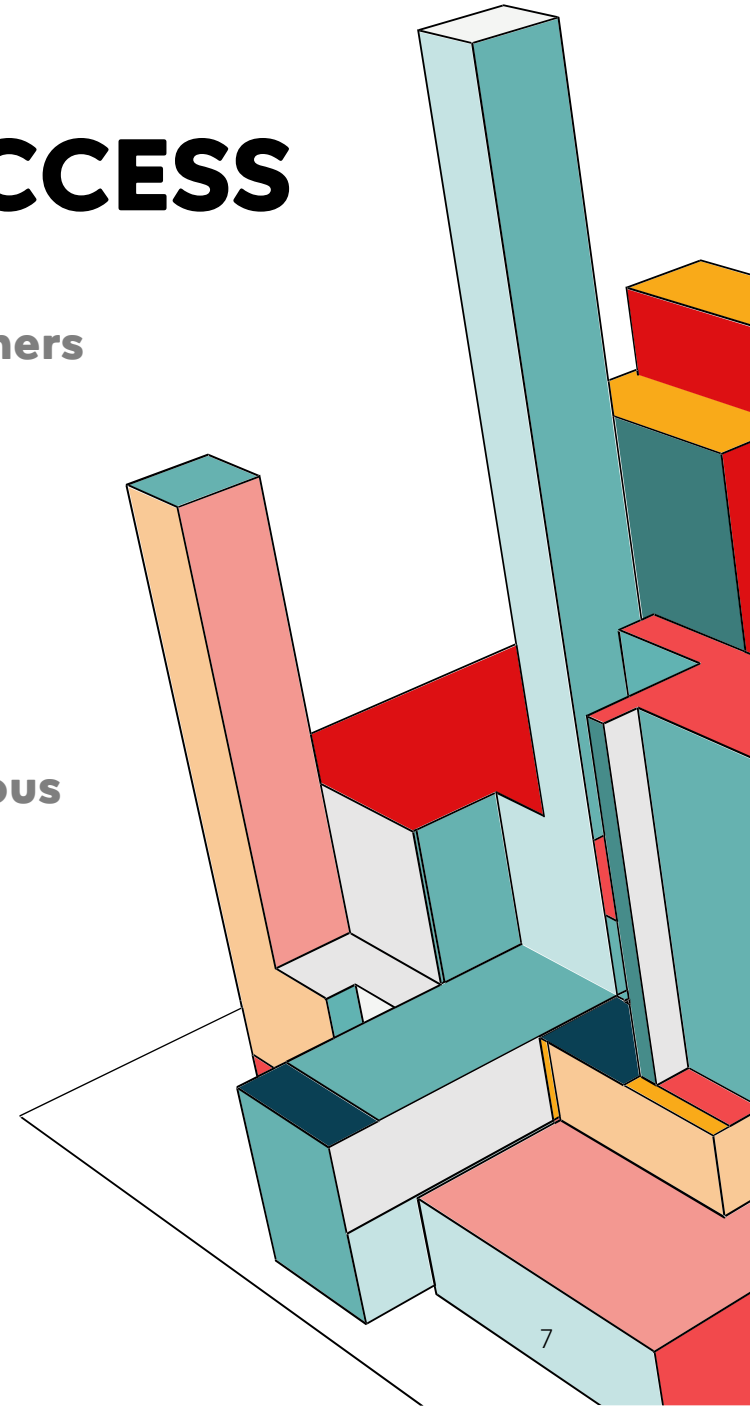
1. Onground training
2. Udemy, acloudguru, testout, aws, azure, safari oreilly, google, etc
3. Local, regional, state, national, ISSA VC, Secure the Village

5) Develop Hands On/Stay Curious

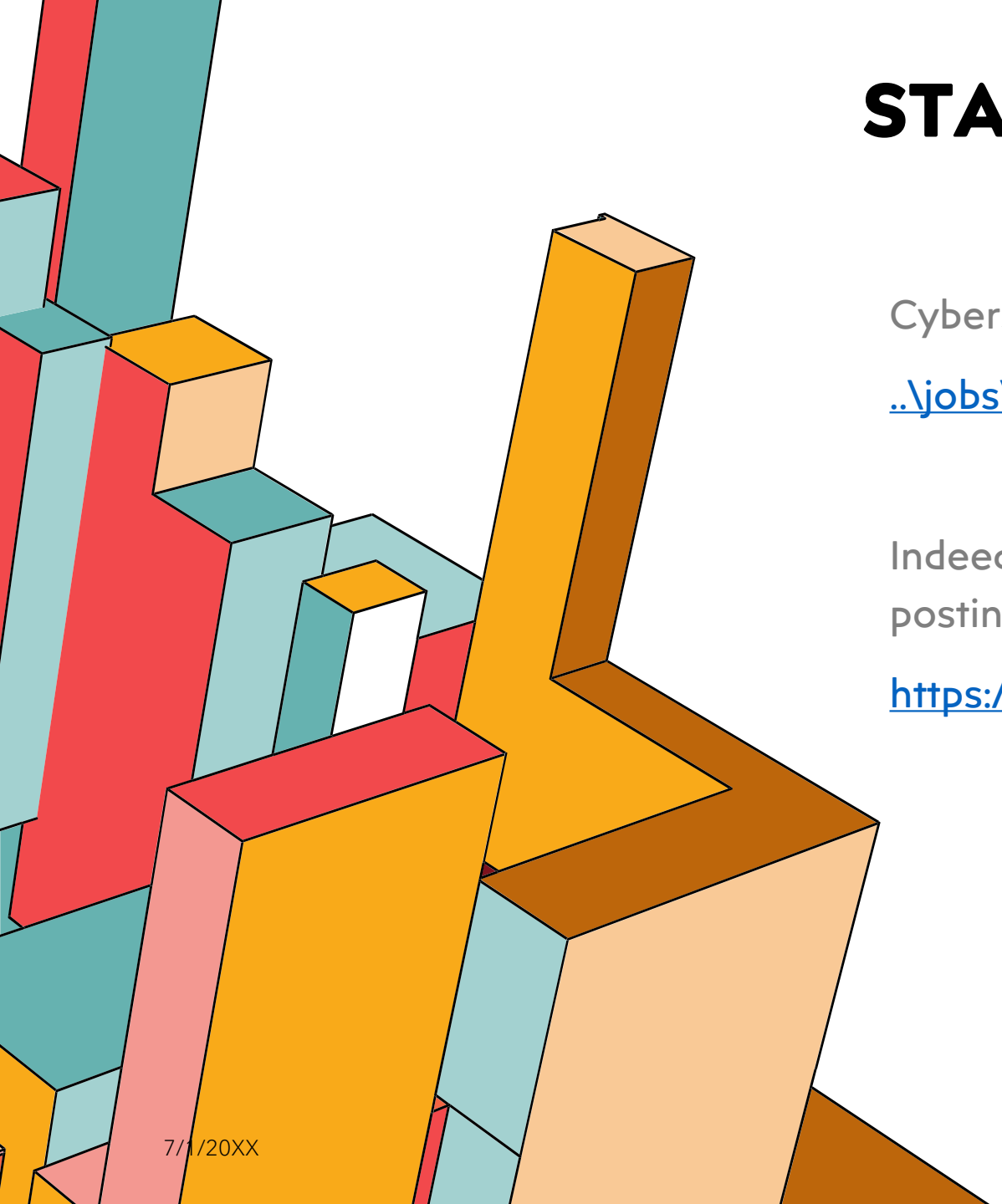
NDG, Testout, WASTC, AWS, Azure, etc
Linux ubuntu clone

Utilize Multi-Prong Approach!

1) Theory,
2) Hands-On,
3) Certification



STAY INFORMED –



Cyberseek.org – explore pathways

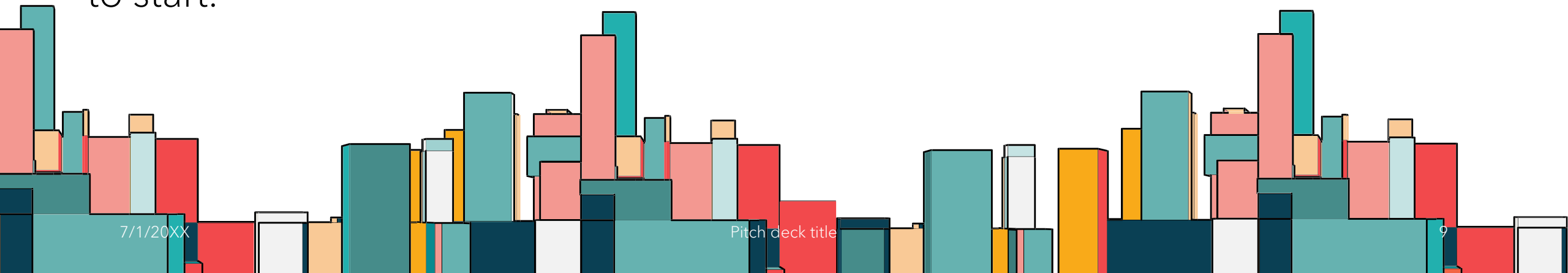
..\jobs\Security\Information_Security_Director.pdf

Indeed.com – know local/regional employers, review job postings, align YOUR training

https://www.cyberseek.org/

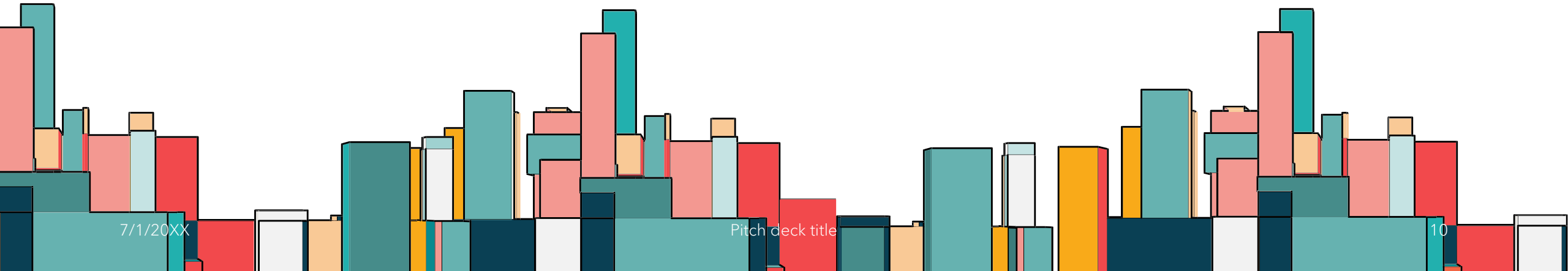
WHAT IS YOUR ROLE BLUE TEAM?

Blue teams are operational defenders of an organization. Blue team roles include incident responders and security engineers for endpoints, identity, application development, networks, cloud, forensics, threat intelligence, etc. Blue team technical roles can also include auditing and compliance, or they can include governance and policy. The role of blue teams is to create ways to protect the people, technology, and information being used by an organization. When looking for blue team jobs, look for terms like security operations, security architecture, risk assessment, or threat intelligence as a place to start.



WHAT IS YOUR ROLE RED TEAM?

Red teams discover system and process weaknesses. They might do testing to exploit those weaknesses and to help the organization improve its security controls. Penetration testers, vulnerability researchers, threat hunters, and others make up red teams that partner with blue teams. When searching for red team jobs, look for pentesting, ethical hacking, reverse engineering, and threat intelligence.

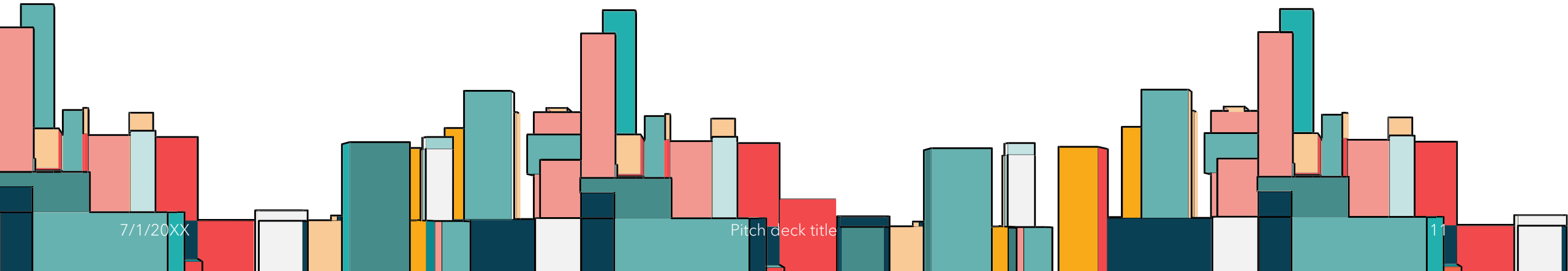


TRUST BUT VALIDATE MINDSET

PROJECT MANAGEMENT + DEPLOYMENT OVERSIGHT!

1. What is the process to determine something has broken? Device/Server not responding, where does info flow? Case Study Trend Application!
2. What is the process to determine something is working? Email performance, firewall blocking, etc Case Study – Moorpark College – IPv4
3. What is the process to identify whats Normal and an Anomaly? Case Study Omeggamon – Mainframe Performance
4. Do current Security Policies reflect current Business needs?

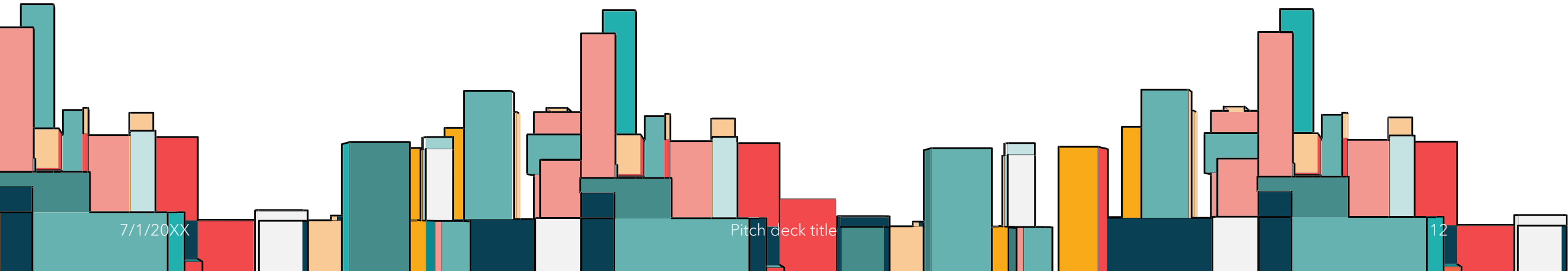
Example: Hybrid Workforce – 5 best practices for hybrid workplace model security



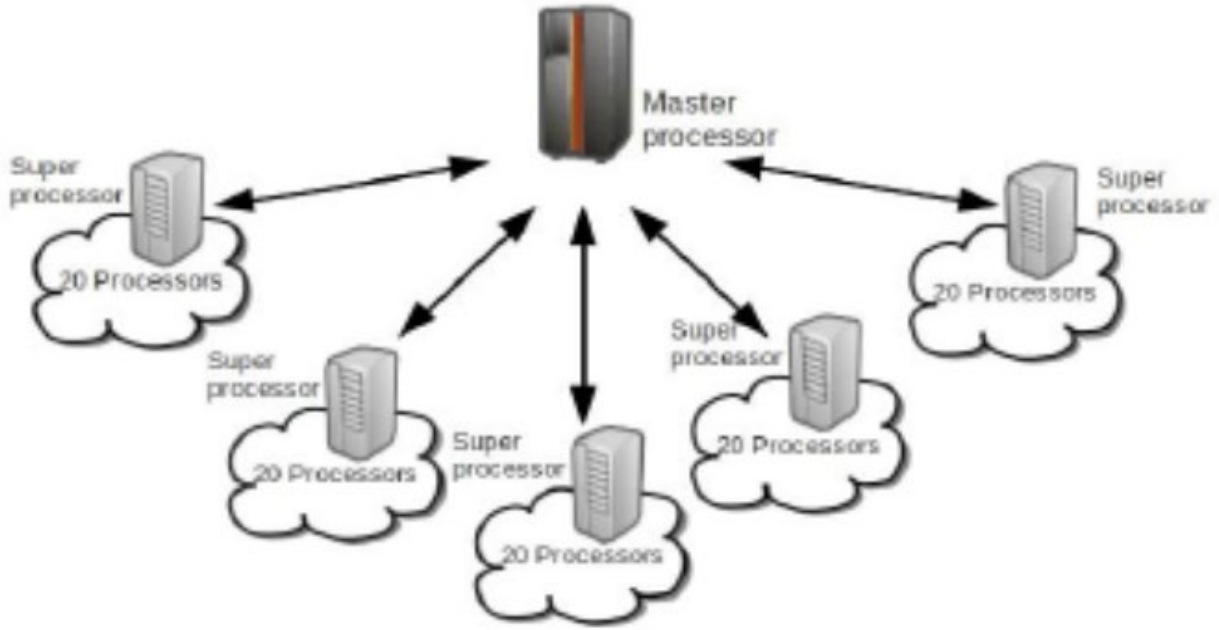
NSA MANAGEABLE NETWORK PLAN

NSA Manageable Network Plan PDF

CASE Study – $50M DataCenter Electrical Power Outage – Painting Crew!



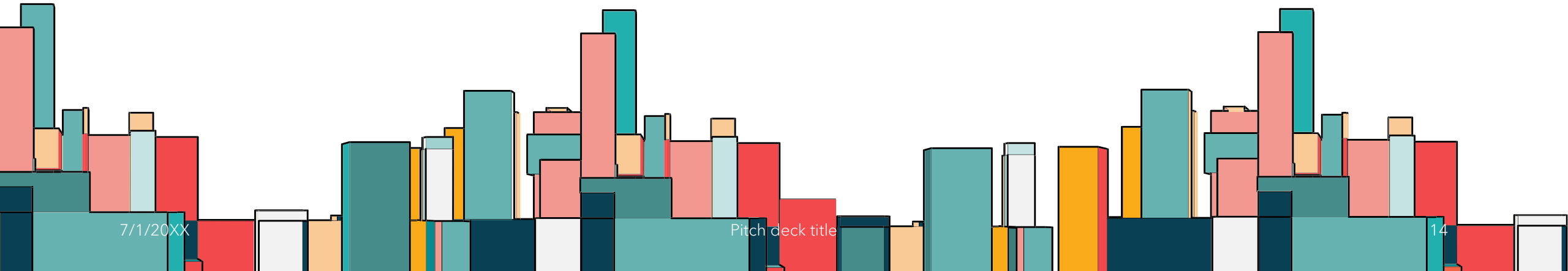
TREND – Enterprise Polling, DB, Web, Authentication, NOC Center



NATIONAL INITIATIVE FOR CYBERSECURITY FRAMEWORK?

In the United States, the federal government has created the National Initiative for Cybersecurity Education (NICE) framework (https://www.nist.gov/itl/applied-cybersecurity/nice).

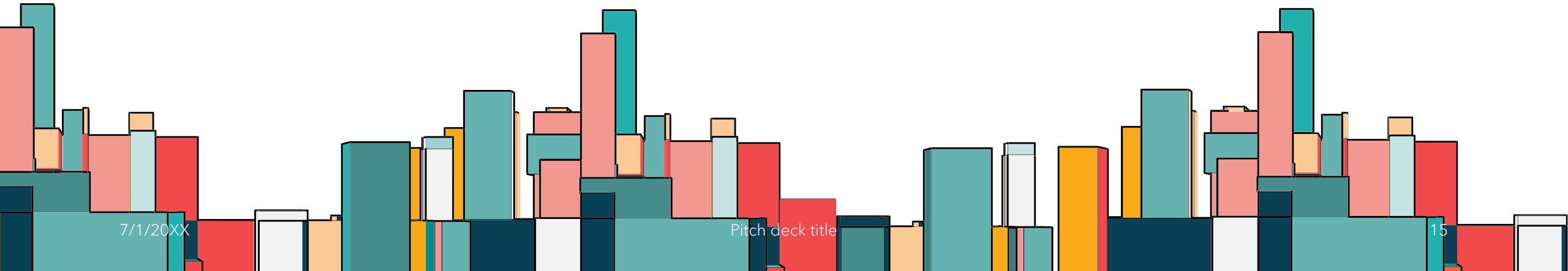
Workforce Frameswork



CYBERSECURITY MINDMAP?

A mindmap is simply a visualization of a concept. Cybersecurity mindmaps are a visualization of the functions that make up cybersecurity, usually presented in the format of a CISO organization or the roles a CISO must cover. Most people outside the Cybersecurity profession don't fully *realize and appreciate the complexity of a security professional's job*. CISO MindMap has been an effective educational tool and has enabled professionals to design and refine their security programs.

Rafeeq Rehman cybersecurity Mindmap

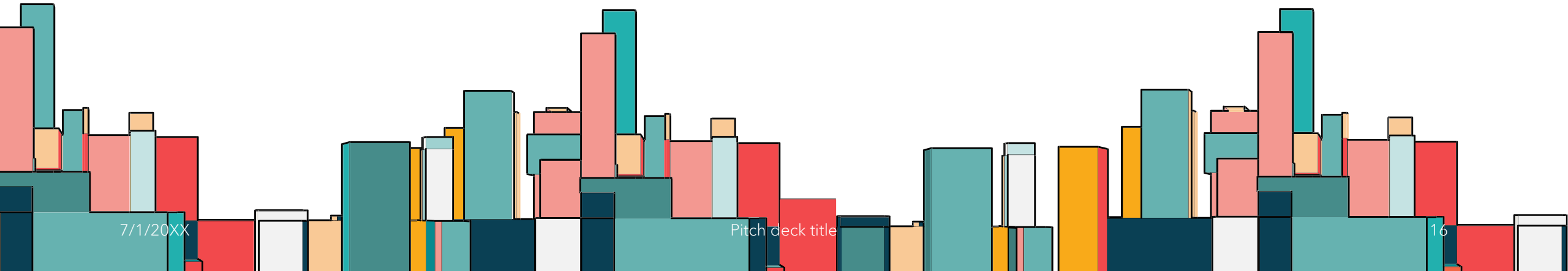


TAP CYBERSECURITY PROFESSIONALS

Interview Security People
A great place to start learning about security is by talking to people who work in the industry to get their stories. Go to a conference like a local BSides (http://www.securitybsides.com/w/page/12194156/FrontPage) or ISSA (www.issa.org) event.

You could also attend a local security meet-up, or use LinkedIn or social media contacts.

ISSA – see local chapters



CERTIFICATION BENEFITS

Requires a commitment and is achievable!

Creates opportunities for Job Interviews

Develops confidence + competency

Certifications

TRAINING/CERTIFICATION
SELF-DEVELOPMENT

Boot Camps
Home Labs
Projects
Portfolio

College Degrees

1. Self-paced training
2. Udemy
3. NCL
4. Over the wire
5. Hack the box
6. ETC

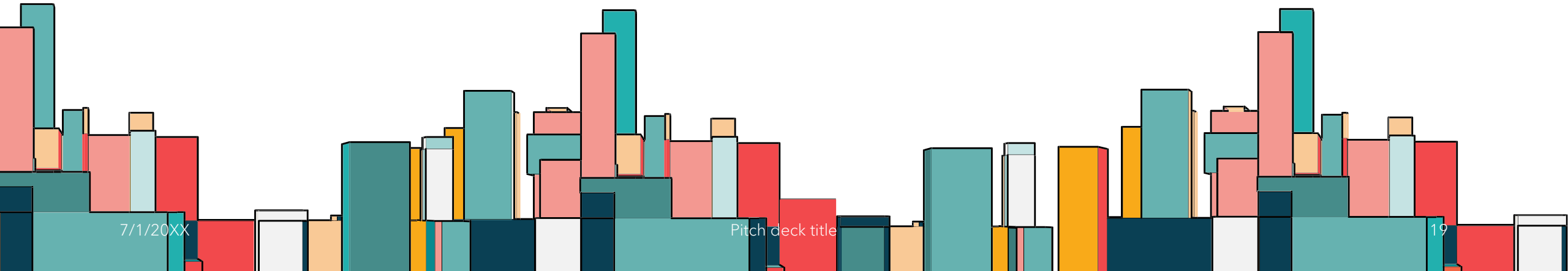
Internships

BLOGS

Also, check out these blogs: (Very informative)

Leslie Carhart, Starting an Infosec Career (https://tisiphone.net/2015/10/12/starting-an-infosec-career-the-megamix-chapters-1-3/)

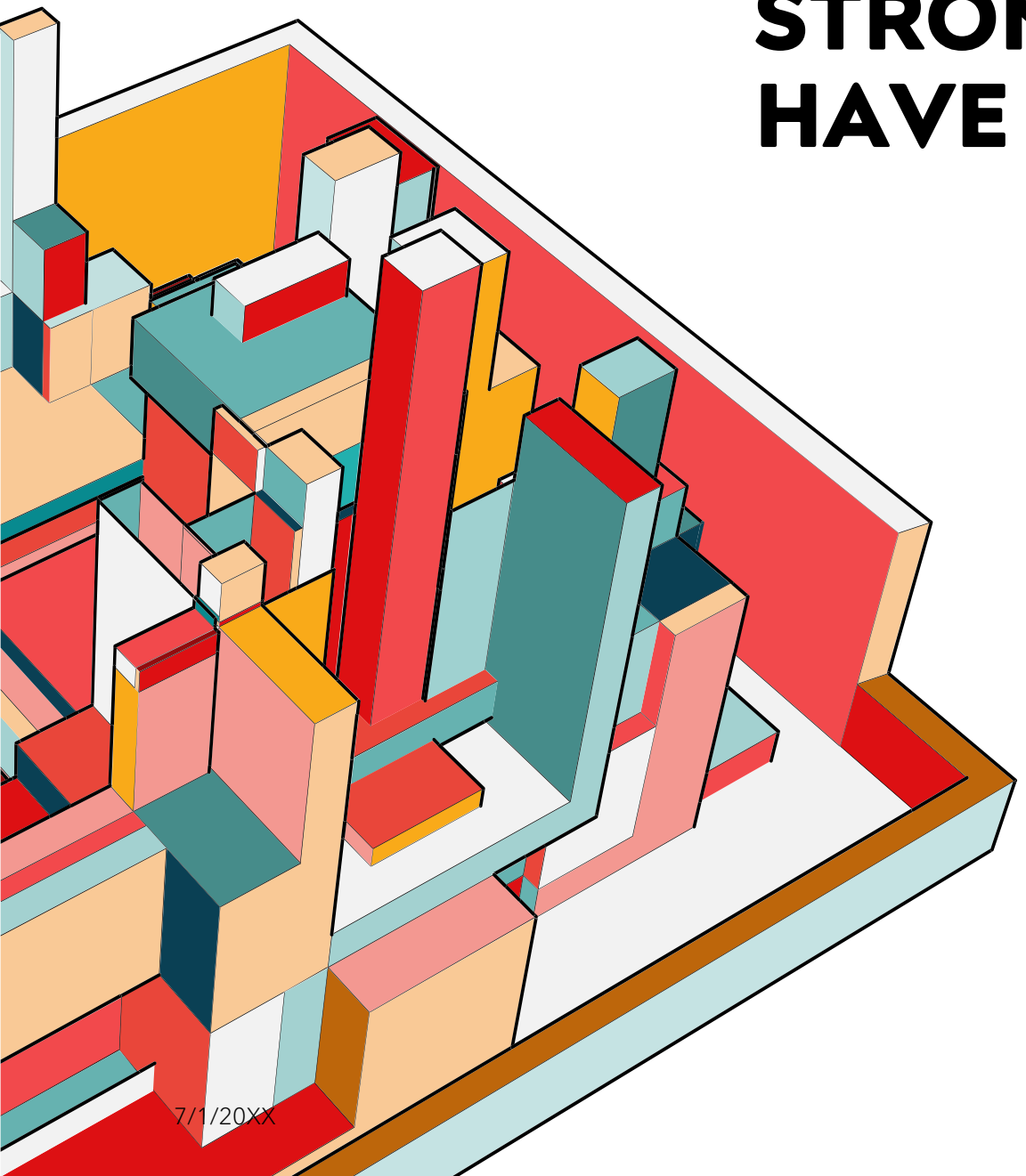
Daniel Miessler, How to Build a Cybersecurity Career (https://danielmiessler.com/blog/build-successful-infosec-career/



SOFT SKILLS – VERY IMPORTANT

Communication Skills

Communication skills fall into two categories: writing and talking.

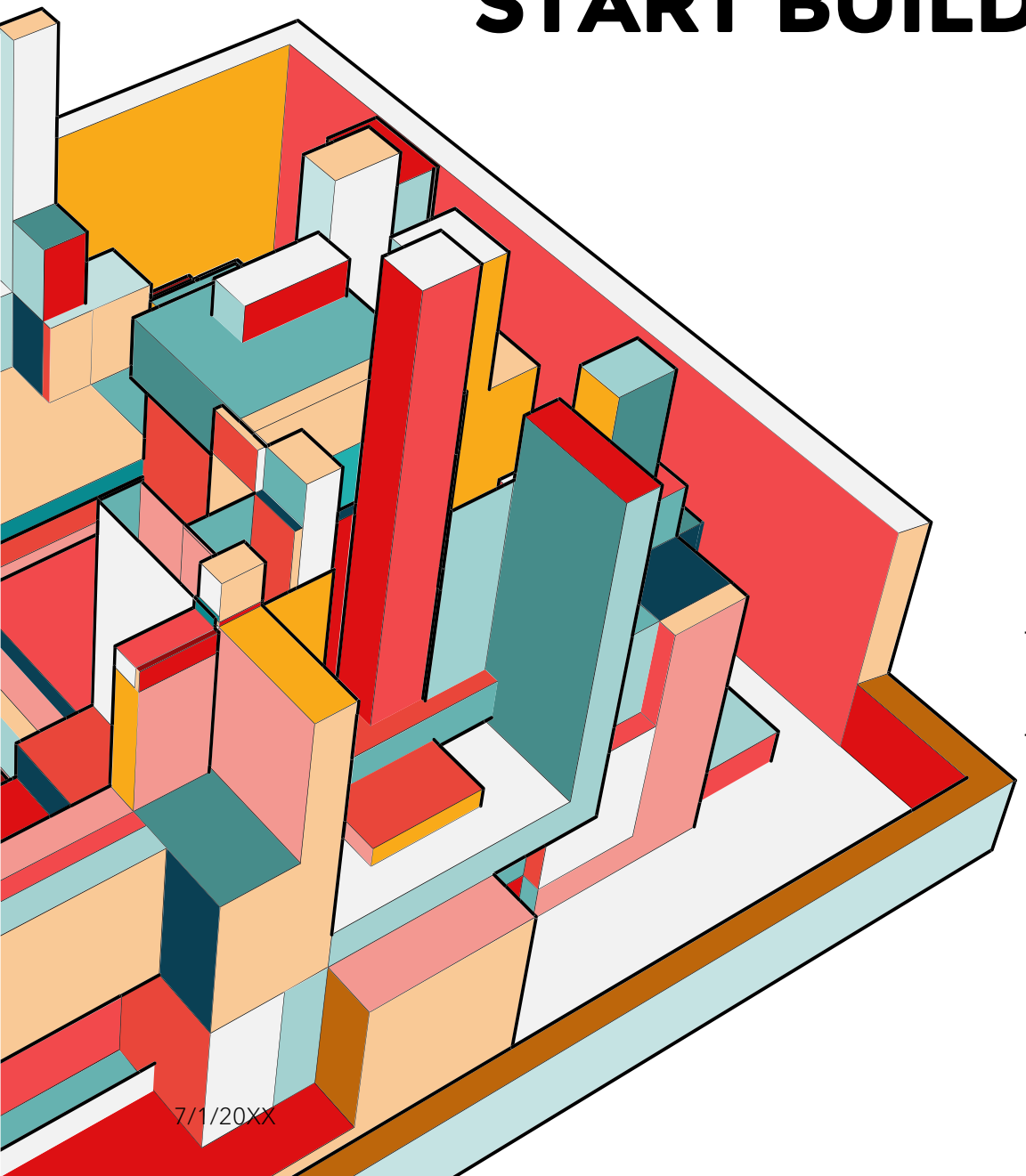


STRONG COMMUNICATION HAVE EXAMPLES

Being able to get your point across clearly and concisely is a required skill in many professions, particularly security. Portfolio of Documentation Examples at Job Interview

If you're not comfortable speaking in formal situations, there are plenty of public-speaking classes (such as Toastmasters) available – use them. Practice speaking in front of a mirror. Record yourself speaking and judge yourself critically. When you're ready, present to other people who will give you constructive criticism – and be ready to take it!

START BUILDING RESUME + PORTFOLIO



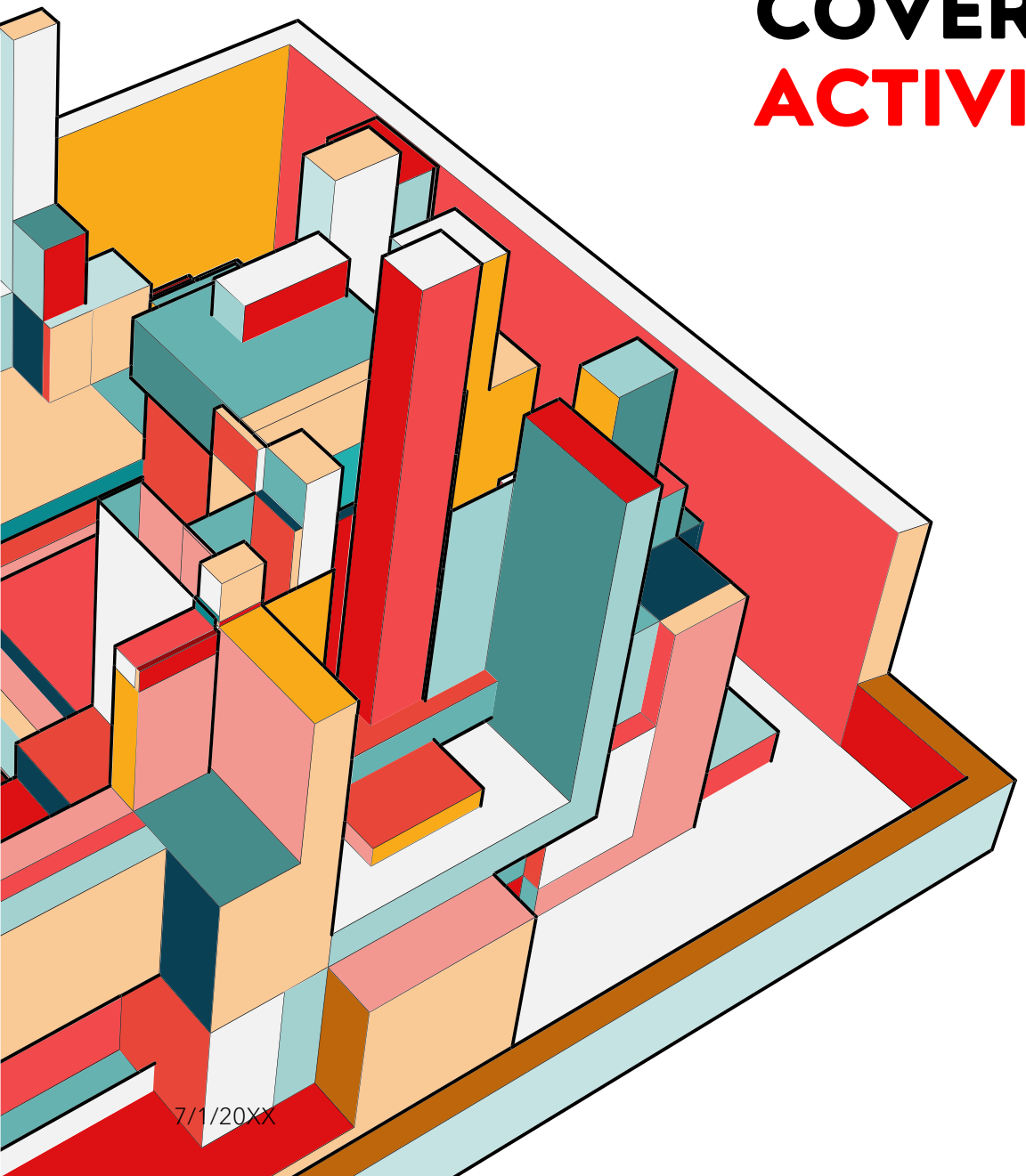
Homework on the company, the hiring manager, the industry, and the role itself. Be prepared for Interview!

What industry is the company in? Is it a highly regulated one? Is it a new industry? Is the industry established or struggling? Why would you want to work in this kind of industry?

What is the mission of this company? What do they care about? Profits? Community? Innovation? Why would you want to work in this kind of company?

Who is the hiring manager? What is their background? Are they a technologist or a compliance officer? First-time manager? Why would you want to work for this manager?

What is the role? Is it one of many roles at the company? Is it a new role for the company? Is the person who did the role still there? (Perhaps they are the hiring manager and are hiring their replacement.) Why are you applying for this role?

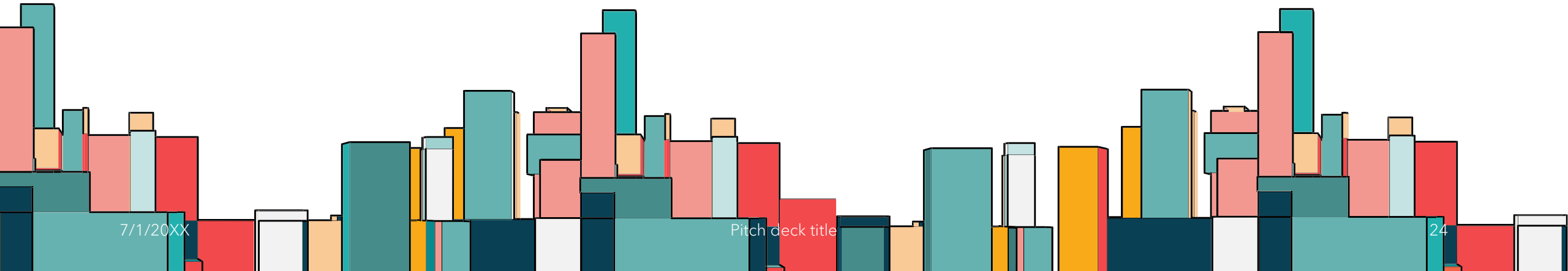


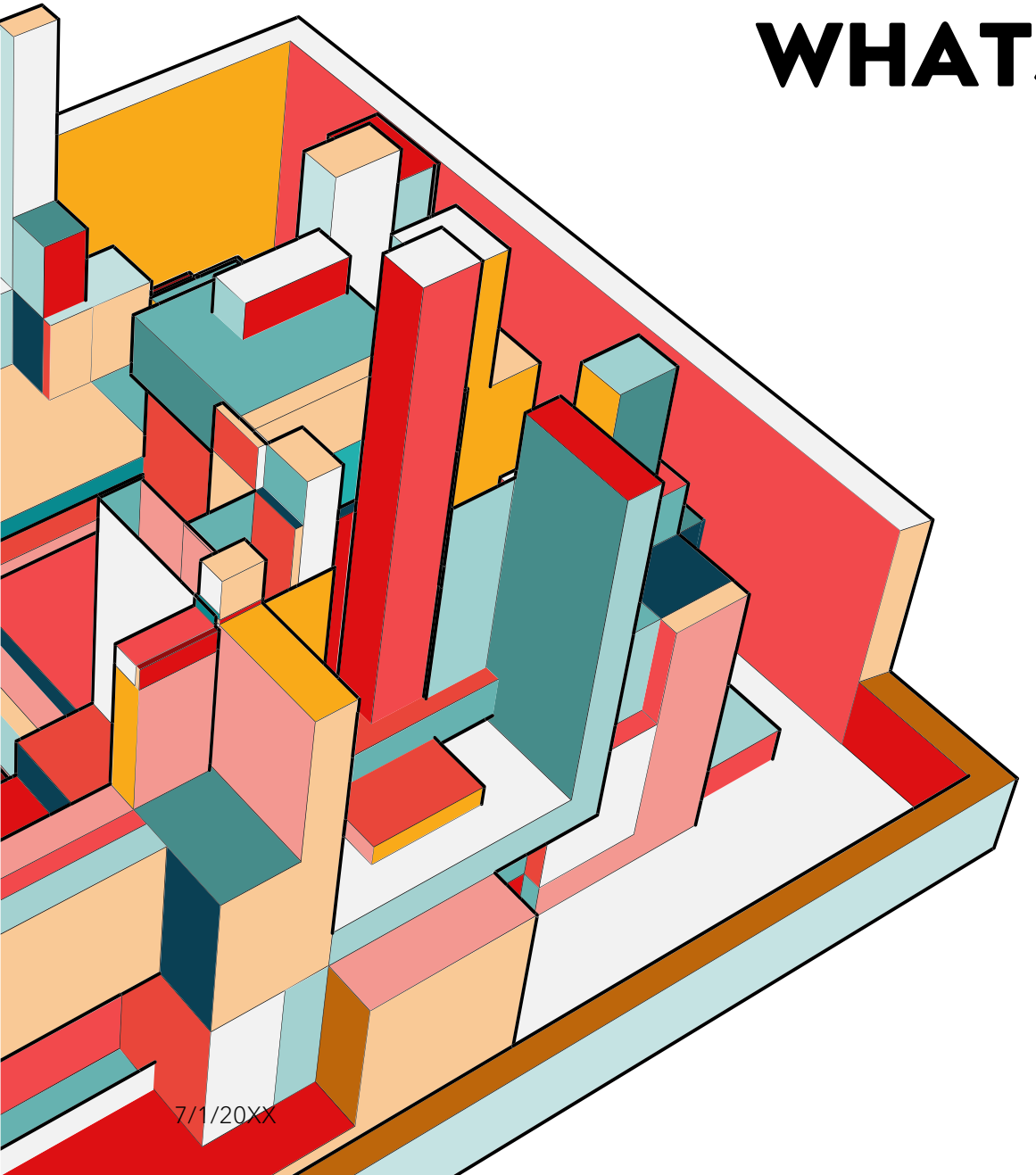
COVER LETTER + OUT OF BAND ACTIVITIES/ACCOMPLISHMENTS

1. Membership in a cyber club or professional organization
2. If you have a Kali/Linux server that you play around with
3. Participation in capture-the-flag (CTF) events or other training
4. Security conference attendance
5. Digital presence on LinkedIn, Facebook, etc
6. References

TRUST BUT VALIDATE MINDSET WORTH REPEATING!!!!!

1. What is the process to determine something has broken? Device/Server not responding, where does info flow? Enterprise Morning Report via Web, saw need so I built process to develop my skills.
2. What is the process to determine something is working? Email performance, firewall blocking, etc Case Study – Customer Billing – Log all activity, Flag Unauthorized Transactions.
3. What is the process to identify whats Normal and an Anomaly? Case Study - Deregulation – Who is accessing Customer Accounts?





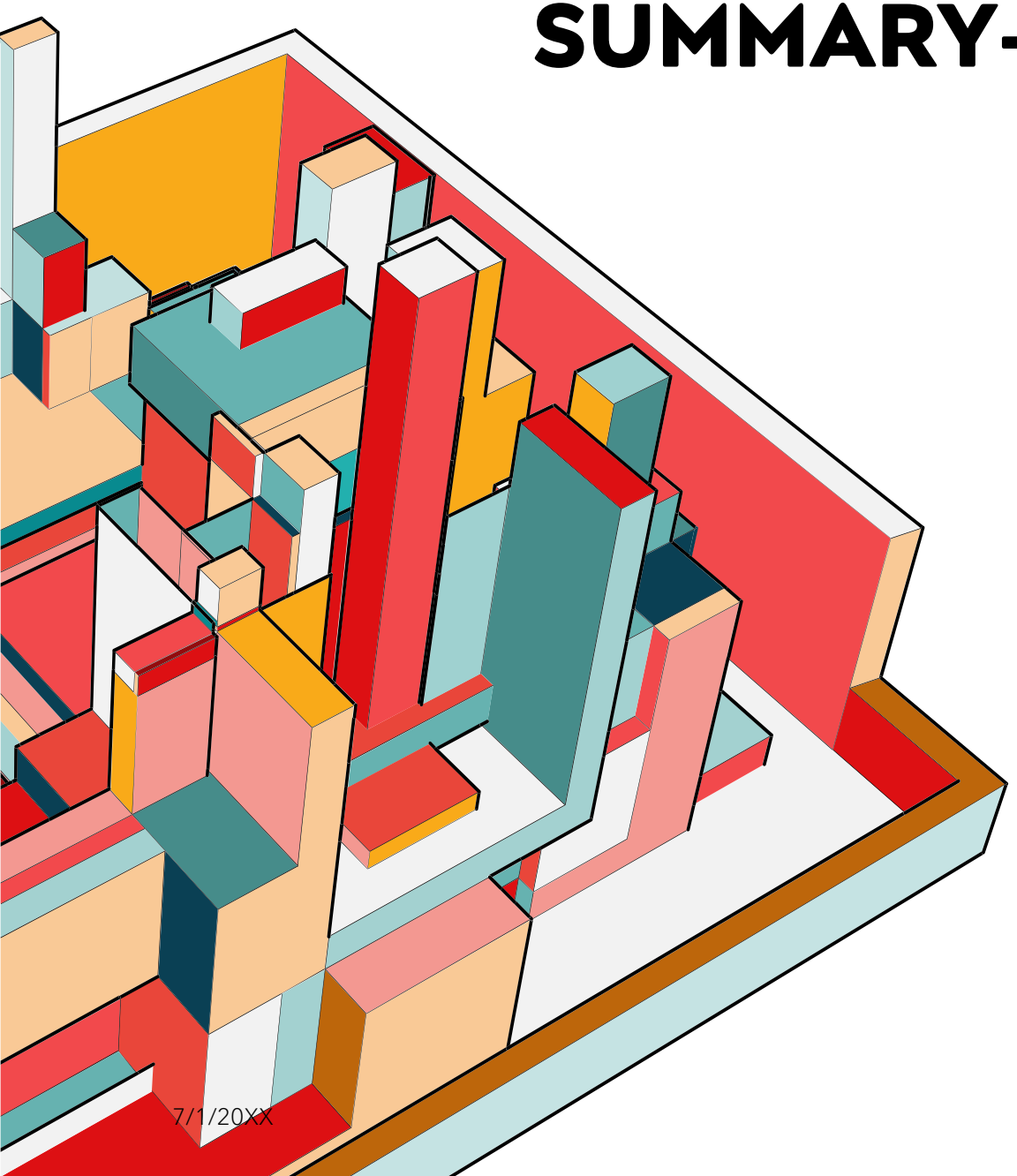
WHATS NEXT?

Create a generic security résumé for each type of job you hope to land.
Create a cover letter template that is ready to be modified for each job.

Update your LinkedIn profile. Make sure you're using it to actively engage with the security community and topics.

Consider other social media or online options and begin participating in those activities.
Share your draft résumé and social media profiles with security contacts and managers. Ask them for feedback and incorporate that into your résumé and online presence.
If you're ready to start using your résumé to search for jobs, prepare your references.

SUMMARY- GOING FORWARD



1. Have a Plan to Develop YOU.version.2.0.1
2. Education, Certification, Hands-On
3. Have a Growth Mindset
4. Networking/ no silo's allowed!
5. Get started every day, How do you climb a Mountain?
6. Develop your Time Management skills!
7. Out of sight – Out of mind!
8. Q&A

THANK YOU

Ed Garcia

Moorpark College

Cybersecurity, Cloud, InfoTech Program

egarcia@vccccd.edu