



Auditing and Remediation

Module 12

Module 12 Agenda

- Auditing
- Remediation
- Cyber Security Careers

Auditing

Auditing

- By definition, an audit is an inspection of an organization's systems or its individual's accounts.
- There are many different types of audits that can be performed. For example....
 - Internal audits
 - External audits
 - IRS tax audits
 - Financial audits
 - Operational audits
 - Pay audits
 - Compliance audits
 - Information Technology (IT) / cyber security audits
 - Payroll audits

Auditing

- As you may have guessed, we are going to focus on Information Technology/cyber security audits.
 - **Information Technology (IT) and cyber security audits** are performed in order to detect issues within computer systems and its software.
 - Audits help search computers for vulnerabilities that need to be patched.

*IT and cyber security audits differ from pen-tests because they are used to check what security controls are in place and if those said controls are working properly. Whereas pen-tests evaluate the entire risk level of the system.

Auditing

What is it:

- **IT/cyber security auditing** is the examination of a computer system to make sure everything is clean and up to date.
 - It is essentially a checklist to help systems evaluate if they have the proper security measures in place.

Auditing

Why:

- With the internet rapidly expanding, cyber threats/attacks are becoming increasingly prevalent
 - Auditing helps find holes within cyber security infrastructure
 - Auditing can help monitor network security
 - Audits help the user maintain updated software to protect itself

Auditing

How it works:

- IT/cyber security audits are most often conducted by third-parties.
- The computer system's encrypted data is sent to a auditing company to be evaluated.
 - It is compared to regulations and is given either a pass or fail report after completion
- The auditing company follows a security model to make sure data will not be exposed during the process.

Remediation

Remediation

Remediation is the process of taking some kind of action to prevent any further damage to an attacked system or to start the clean-up process after the damage has already been dealt.

What is it:

- For cyber security in particular, **remediation** is the process of stopping and treating a data breach.
- Detects and contains a breach before it grows and damages the entire system

Remediation

Why:

- Security breaches are a major threat for companies and business.
 - They can expose sensitive data concerning the company and its customers
- Failing to detect breaches can put companies at greater risk

How it works:

- Detects and evaluates the cause of the breach
- Determine how to stop the harmful activity and how to patch the damage

Remediation

Breaches:

On your own time throughout the week, find time to read this article about how breaches happen, how to detect them, and how to fix them. *This will be very helpful for the CDC*

How To Detect Data Breaches:

Article

Jobs in Cyber Security

Jobs in Cyber Security

Being a junior security auditor is actually a career that cyber security students can pursue. Watch the video below that explains the job! :)



https://youtu.be/iW7W_6stSh0

Jobs in Cyber Security

- Cyber security jobs are in high demand and offer competitive salaries
 - According to [cybercademy.org](https://www.cybercademy.org)
 - “3.5 million cyber security jobs are expected to open by this year”
 - “\$83,000 is the national average salary for entry-level cyber security analysts”
- Cyber security offers a variety of careers

Jobs in Cyber Security

Cyber security students have a lot of options for careers. Including those listed below...

- Penetration Tester
- Incident Responder
- Cyber security Analyst
- Security Specialist
- Vulnerability Assessor

We will be discovering what cyber security career is right for you in Activity 2

Jobs in Cyber Security

The best jobs in technology

Cybersecurity jobs: high-demand, high pay, fascinating work, while making a difference!

Can you qualify for the National Cyber Scholarship Competition?



Visit our website

Try CyberStart to see whether you like solving cybersecurity challenges by visiting cyberstartamerica.org



Can you make it to the Nationals?

Prove you have the ability to complete the challenges in CyberStart to take part in a two-day scholarship challenge



Win a scholarship!

Compete with others to qualify for recognition and one of **600 scholarships** to use at the college of your choice

**cyberstart
America**

Initial cyber jobs with lots of advancement opportunities

- Digital forensic analyst; investigator**
"The thrill of the hunt! It's CSI for cyber geeks! You never encounter the same crime twice."
You are the detective in the world of cybersecurity - searching computers and networks for evidence in the wake of an incident.
- Penetration tester for systems and networks**
"Be a hacker, but do it legally and get paid a lot of money!"
You look for security vulnerabilities in target systems and networks to help enterprises improve their security.
- Application pen tester**
"We desperately need more of this, application security has been such a black hole for so long."
You're a programming/security wizard; test applications before deployment so they don't present opportunities for intruders.
- Security operations centre (SOC) analyst**
"The fire ranger. Catch the initial blaze, or there goes the forest."
With an eye for detail and anomalies, you see things most others miss. Active prevention, active detection, active monitoring, active response.
- Cyber defender; security engineer (enterprise and ICS)**
"A leg up on your IT and engineering buddies; talk shop with them but you are saving the world from the bad guys, lol."
Implement/tune firewalls, IPS/IDS, patching, admin rights, monitoring application while using, more.

More advanced cyber jobs - open after a few years of great performance and specialized training

- Hunter, incident responder**
"The secret agent of geeksdom. You walk in and say 'Oh I'll take it from here.'"
While everyone else is running around shouting 'the system's dead!', you have the sense and skills to rationally figure out why.
- Security architect**
"You get to design the solution, and not just for the perimeter."
You are very creative, on top of the game technically and the business; you design and build defensible systems and are part of a team of very adept people.
- Secure software development manager**
"Coolest software developers."
You protect the whole development team from making errors that will allow hackers to penetrate your organization and steal data. You are a programmer, but a programmer with special powers.
- Malware analyst/reverse engineer**
"The technician elite! Only go here if you have been called. You know who you are."
Look deep inside malicious software to understand the nature of the threat - how it got in, what flaw it exploited, what it is trying to do or has done.
- Technical director/CISO**
"Making decisions making things happen. That's coolness."
Top of the tech ladder. Strategic thinking; hands-on involvement in solution design/deployment; you hold the keys to tech infrastructure and have the ability to contribute and influence.

Other great cyber jobs

- Cyber educators**, build the talent the nation needs
- Cybersecurity awareness coordinators**, protect users from themselves
- Cyber policy analysts**, define critical processes
- Cyber legal advisors**, help make sure everything is done legally
- Cyber project managers**, keep the team moving along
- Cyber intelligence analysts**, see out beyond the horizon ... and dozens more



You'll find these jobs in

- Government
- Oil and gas
- High tech
- Health care
- Manufacturing
- Finance
- Defense
- Intelligence and more!

What our students say about CyberStart America



I like all the different types of problem solving/programming solutions. Not only am I using Python but I'm decoding messages, which is really fun.



The novice level was so welcoming, I never felt over my head even though I knew nothing about computers or programming.



It was a great combination of fun and learning. I felt like I was in a movie or a real adventure.



I had no idea what I wanted to do with my life but thanks to CyberStart now I do. Thank you!



Don't miss out! Register at cyberstart.io/getstarted

Poster [Link](#)

Jobs in Cyber Security

As mentioned in the previous video, basic cyber security skills include...

- Knowledge of operating systems like Windows, Unix, and Linux
- Programming skills in C, C++, Java, PHP, and Python (you can learn more about programming by completing the Smart-IT venue of IT-Adventures)
- Elementary concepts (firewalls, access controls, malware, etc.)

Jobs in Cyber Security

Cyber security skills can be developed through...

- Online programs/certifications
- College degrees in:
 - Software Engineering
 - Computer Science
 - Computer Information Systems
 - Business Information Systems
 - Information Assurance

To Do

- ❑ Complete Module 12 Activity 1
- ❑ Complete Module 12 Activity 2
- ❑ Read the following article: [link](#)

End of Module 12!

What questions do you have?

Final Module Topic:

Physical Security & Social Engineering

Questions?

Contact IT-Adventures support staff!

email:

ita@iastate.edu