State Information Technology Systems Division (SITSD)

JAMES ZITO

CISSP-ISSAP, GCFE, SECURITY+, NETWORK+, A+, ZTX-I

SECURITY ARCHITECT

jzito@mt.gov

LinkedIn:
https://www.linkedin.com/in/jameszito

Department of Administration - SITSD

As the Department of Administration, we provide hosting services and cloud support to all agencies within the state who are providing public services to our citizens. Services such as law enforcement, child support, mental health, tax filing, hunting and fishing licenses, natural resources, road conditions, and a lot more!

Cybersecurity is important for our agency as we are responsible for securing the infrastructure the agencies use to store their sensitive citizen data. Typical tasks would include:

- Assessing risk of information systems using vulnerability and configuration compliance scanning.
- Threat hunting for indicators of compromise (IOC's) in the environment.
- Responding to security incidents.
- Architecting new security solutions or requesting changes to current infrastructure to enhance our security posture and reduce our threat exposure.

An average day in the life of a Cybersecurity professional

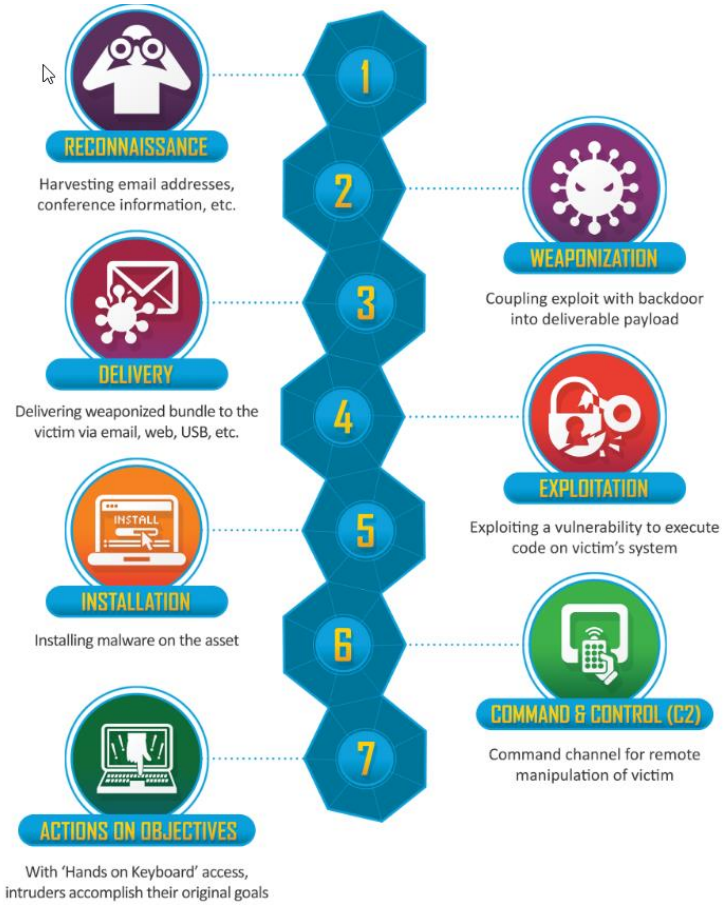
Varies depending on the specialty the individual is responsible.

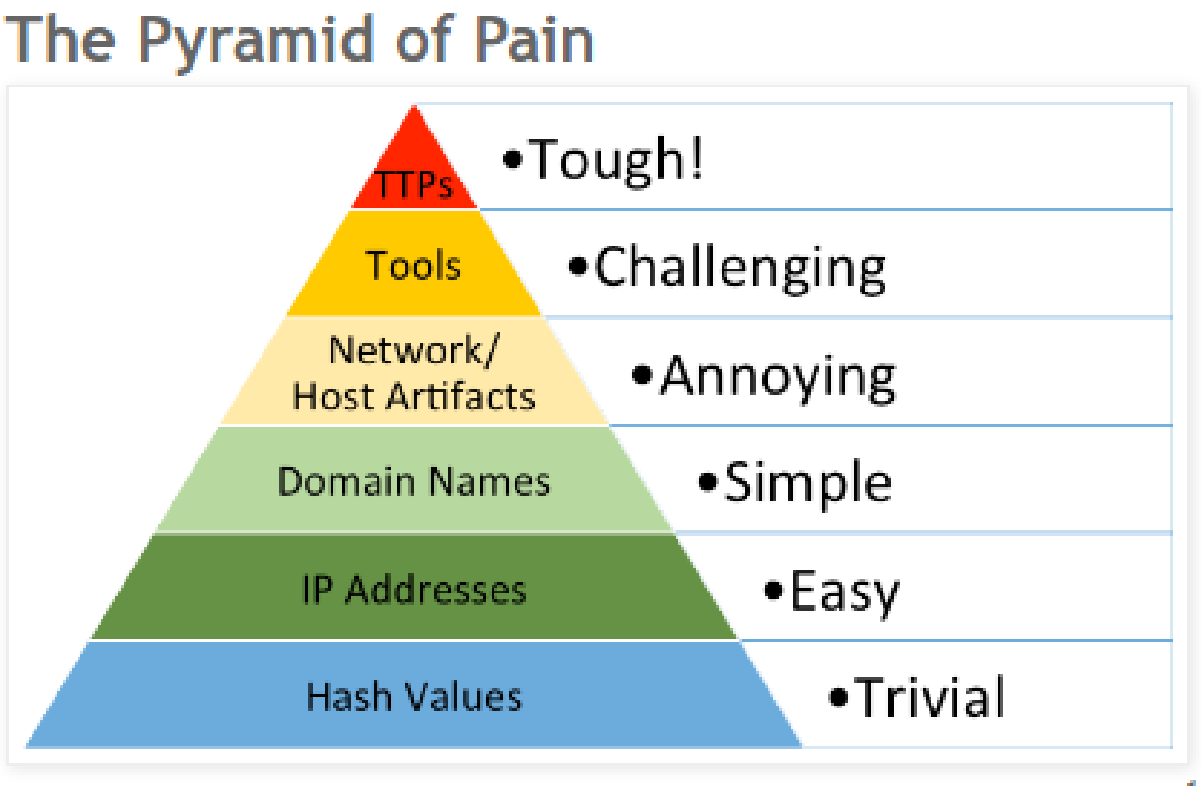
- Incident responders are like firefighters. They respond to reported security incidents but, in their downtime, must maintain their tools and be more proactive in performing threat hunting.
- Risk Management groups evaluate systems by doing risk assessments and help to make sure IT operations are within compliance of our security policies and regulatory bodies such as the IRS, HIPPA, and more.
- Security Architecture performs daily reviews of firewall requests making sure the least amount of access is approved. I help determine the security needs of the enterprise, design architecture, research solutions, drive assessment of those solutions in proof of concepts, and drive technology deployment projects from to meet our needs from a security perspective.

Tips/Advice for students pursuing career in Cybersecurity

- Get as much experience as you possibly can in the information technology field even if it’s an entry level administrator role.
- Develop an attention to detail as that is a critical skillset.
- Stay up to date with the latest cybersecurity news.
- Try to get core entry level certifications like CompTIA Network+, Security+, or CySA.
- Learn how information systems perform logging and how to filter logs.
- If you can, try to use technical examples in interviews.
- Learn what the “Cyber Kill Chain” and the “Pyramid of Pain” is and think like a hacker when asked questions you're not sure about in interviews.
- Have a passion for security.

Cyber Kill Chain & Pyramid of Pain





https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Cybersecurity Information Resources

- https://www.cisa.gov/
- https://www.darkreading.com/
- https://krebsonsecurity.com/
- https://cyberscoop.com/
- https://www.csoonline.com/
- https://thehackernews.com/

Cybersecurity Training Resources

- FedVTE – https://fedvte.usalearning.gov/public_fedvte.php
- SANS.org - https://www.sans.org/webcasts/?msc=main-nav
- ISC2 - https://www.isc2.org/News-and-Events/Webinars
- BrightTALK - https://www.brighttalk.com/topic/cyber-security/
- Cybrary - https://www.cybrary.it/

Typical interview questions for cybersecurity

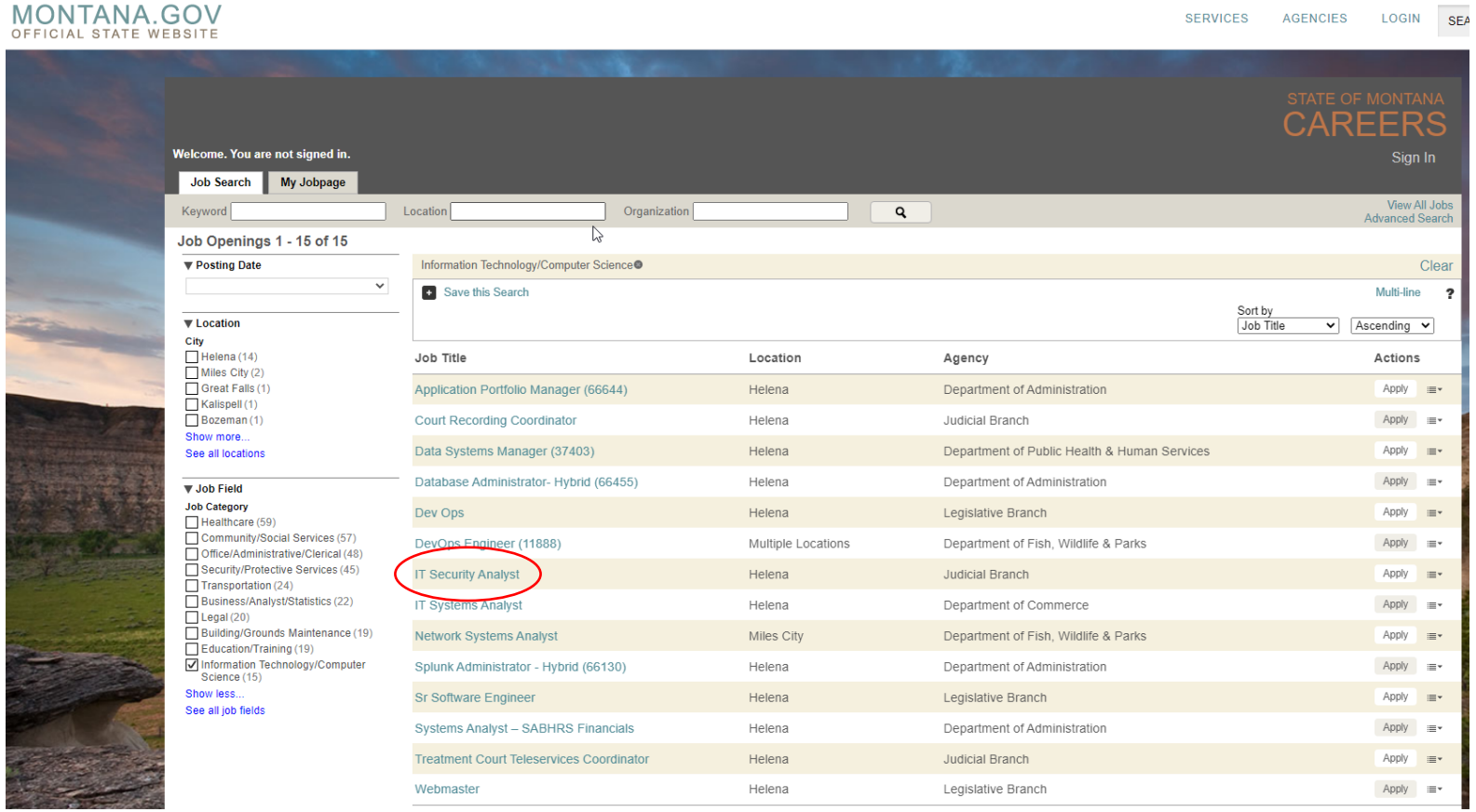
- **Can you tell us what the difference between a risk, vulnerability, and an exploit is?**
  - Risk – the potential for loss and damage when the threat occurs.
  - Vulnerability - exposes the organization to a threat.
  - Exploit – code to take advantage of a vulnerability.
- **If you were to focus your cybersecurity efforts on mitigation vulnerabilities or threats, what would it be and why?**
  - Vulnerabilities because those are things you can control. Threats you cannot.
- **What is your understanding of cybersecurity, and what do you think are the biggest threats to organizations today?**
- **What steps might you take to contain and mitigate an incident?**
- **Can you describe a time when you detected and responded to a security incident? Or if recent graduate, can you describe how your classes taught you to detect and responded to a security incidents?**

Cybersecurity Job Postings for Montana State Government

MONTANA.GOV > Employment > State Careers

CAREER OPPORTUNITIES

- Career Section (View or apply for state jobs)



Questions?

State Information Technology Systems Division (SITSD)

JAMES ZITO

CISSP-ISSAP, GCFE, SECURITY+, NETWORK+, A+, ZTX-I

SECURITY ARCHITECT

jzito@mt.gov

LinkedIn: https://www.linkedin.com/in/jameszito