Zoom testing

Portland State
Computer Science

Zoom testing

- So we're all on the same page…
  - Send a message into the chat
  - Raise hand in chat
  - Unmute via "Alt-A", say hello, and Mute via "Alt-A"
  - Screenshare your desktop showing the Google Slide presentation I shared with you
  - Sit tight until 2:15pm

CS 576: Computer Security Research Seminar

Portland State

Computer Science

Prior courses

- Focus on technical foundations and skill development
  - CS 585: Cryptography
  - CS 591: Introduction to Computer Security
  - CS 592: Malware Reverse Engineering
  - CS 595: Web and Cloud Security
  - CS 596: Network Security
  - CS 510: Blockchain Development & Security
  - CS 530: Internet, Web, & Cloud Systems

Prior courses

- Focus on technical foundations and skill development
  - CS 585: Cryptography
  - CS 591: Introduction to Computer Security
  - CS 592: Malware Reverse Engineering
  - CS 595: Web and Cloud Security
  - CS 596: Network Security
  - CS 510: Blockchain Development & Security
  - CS 530: Internet, Web, & Cloud Systems

This course

- Career-focused
- Broad look at what is happening currently within the discipline
  - Industry
  - Academia
  - Policy
- Soft skills development
  - Critical reading
  - Presenting

Logistics

- Synchronous class meetings over Zoom
  - Initial lectures
  - Podcast discussions
  - Rotating student presentations
- Attendance and participation graded on Zoom and Slack channel

Format

- Podcasts (every week)
- Presentation #1: Techniques in Mitre Attack matrix (Weeks 2-6)
- Presentation #2: Academic research paper (Weeks 6-10)
- Final presentation screencast (Uploaded during finals week)
- Final open-note exam (Finals week)

Podcasts (weekly)

- Weekly assignments to listen to podcasts covering a range of policy and industry topics
- Shared Google Doc with instructor with questions to answer for each podcast (mostly to encourage intentional listening)
  - See this week's
- Due Sunday
- Discussion of podcasts in Zoom class the following week
  - Take notes for open-note final

Presentation #1: Mitre Attack (Weeks 2-6)

- Mitre Attack matrix
  - Enumeration of attacker methods
  - Lecture on Thursday
  - Discussion of Mitre Attack podcasts (Tu 4/7)
- Student presentations covering tactics
  - Covering a subset of the techniques within a tactic in ~20 minute presentation describing…
    - Technical details of each technique's use, the vulnerability it leverages, the difficulty in using it, and case studies of how it has been used
    - Description of CIS control and specific counter-measures that can mitigate each technique, their ease of deployment, and their effectiveness in prevention.
  - Done via a shared Google Slide presentation
- Students not presenting
  - Take notes for open note final
  - Questions and comments via Zoom chat for discussion after presentation is over

Schedule so far

- Week 2: Th 4/9: Initial access (Ted), Execution (Alex D)
- Week 3: Tu 4/14, Th 4/16 (volunteers sought)
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Send a Zoom chat msg now or Slack message after class
- Otherwise will tactic will be assigned to you by next class

Presentation #2: Research paper (Weeks 6-10)

- Select research paper to cover from list of papers linked on web site
  - Send a message to reserve a paper to present over Slack by next Tuesday
  - Become the class expert on the paper
- Present the paper to the class over Zoom
  - Include in second section of your shared Google Slide presentation as before.
  - Presentation should run ~20 minutes and address questions in slides
  - Background and Motivation (1-2 slides)
  - Proposed Approach (4-10 slides)
  - Evaluation (2-5 slides)
  - Analysis (2-6 slides)
- Students not presenting
  - Take notes for open note final
  - Questions and comments via Zoom chat for discussion after presentation is over

Final presentation

- Select research paper to cover from list of papers linked on web site
- Repeat process from previous research paper presentation
  - Include in second section of your shared Google Slide presentation as before
- Present the paper to the class over a screencast uploaded to MediaSpace
  - The presentation should run about 20 minutes and cover
  - Background and Motivation (1-2 slides)
  - Proposed Approach (4-10 slides)
  - Evaluation (2-5 slides)
  - Analysis (2-6 slides)
  - See shared Google Slide presentation for questions to address

(Open-note) final quiz

- Covering presentation and podcast material as given in class
- Short answers
- Done via Google Docs/Forms on scheduled final exam timeslot

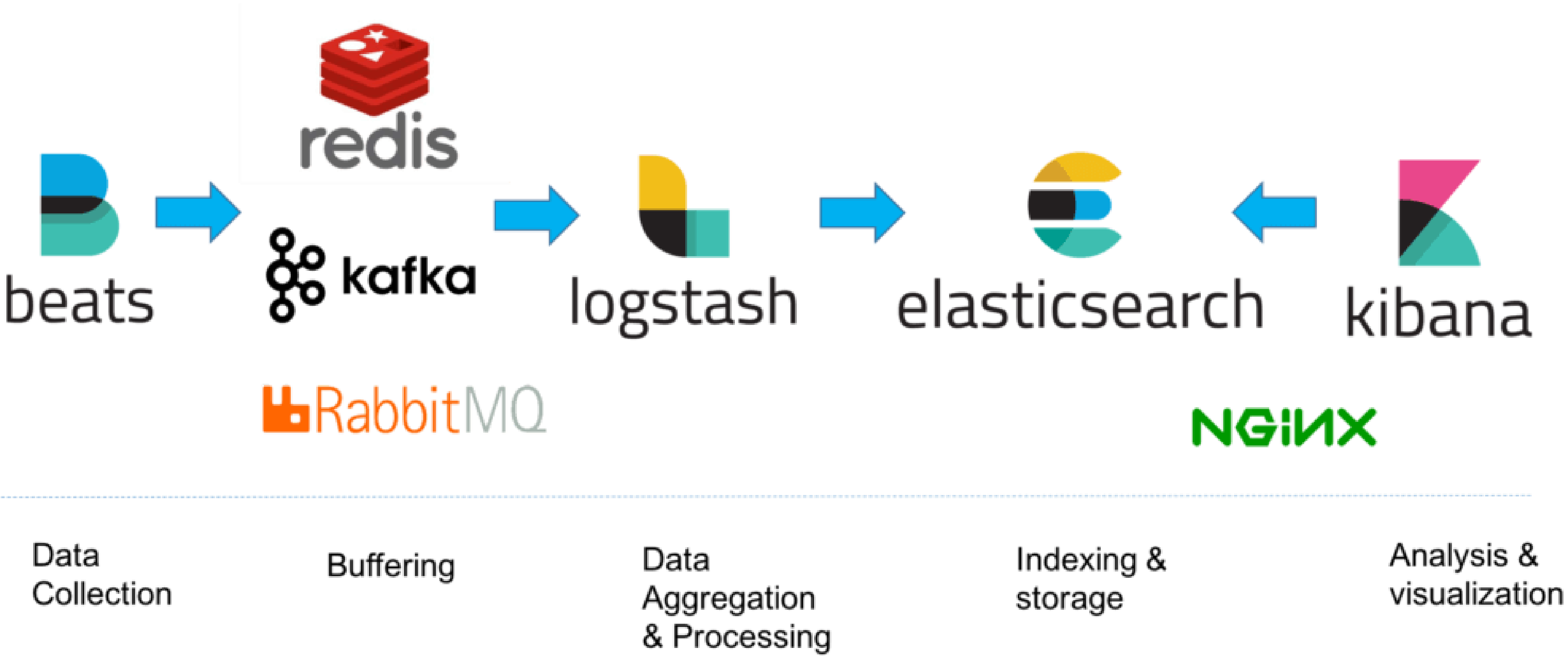
Podcast terminology

Portland State
Computer Science

Week #1: Mitre Attack

- IDS/IPS
  - Intrusion detection system
  - Intrusion prevention system
- EDR/EPR
  - Endpoint detection and response
  - Endpoint protection and response
- DLP
  - Data loss prevention

- SIEM
  - Security information event management system
  - Splunk, ELK (Elasticsearch, Logstash, Kibana) stack



Data Collection

Buffering

Data Aggregation & Processing

Indexing & storage

Analysis & visualization

- SOC
  - Security operations center

Week #2: BeyondCorp/ZeroTrust

- 3270 client (terminal)
- Microsegmentation=>mutually distrusting machines in network ->isolating their allowed traffic from each other especially for legacy applications
- CASB
  - Cloud Access Security Broker
  - on-premises or cloud-based **security** policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise **security** policies as cloud-based resources are accessed.
- RDP
  - Remote Desktop Protocol (e.g. xterm for Windows)
- MDM
  - Mobile device management
- OTT
  - Over the top video delivery (e.g. Netflix, HBO, Disney+)

Cloud, serverless, DevOps

- Serverless => servers on demand
- WAF = Web Application Firewall
- RASP = Runtime Application Self-Protection (friction, performance, modifies app at run-time!, needs language support)