The goal of this course is to learn how to set up enterprise-scale systems to be resistant to attacks -- covering concepts from networking, operating systems, data analysis, and malware (malicious software).

Note: syllabus is subject to minor changes.

Module 1: Basics of networking

TCP/IP, DNS, packet analysis and security tools.

Module 2: Operating systems

Linux containers, firewalls, Security-Enhanced Linux (SELinux), Kubernetes-based container orchestration, control- and data-plane (e.g., Istio- and Envoy), identity and secrets management, Open Policy Agent.

Module 4: Malware in web-services

"OWASP" attacks like SQL- and command-injection, analysis of Equifax and CapOne incidents, long-term threats ('advanced persistent threats')

Module 4: Data analysis

Clustering, classification, and anomaly detection

Module 5: Open-ended

Compete across teams to set up defense- and attacks, work on projects that extend Kubernetes with new security policies.