- Filename: eccouncil-ceh31250-v11-19-4-1-cloud-security-controls.md
- Show Name: CEHv11 (312-50)
- Topic Name: Cloud Computing - Cloud Computing
- Episode Name: Cloud Security Controls
==

Cloud Security Controls

Objectives:

- Standard Security Controls

    - SDLC
    - Patches/Updates
    - Change Defaults
    - Firewall/IDS/IPS/WAF
    - Logging/Monitoring
    - Anti-DoS/DDoS
    - Encryption
    - AV/Endpoint Protection

- Cloud Specific

    - Secure Your S3 Buckets

        - IAM user policies

            - public/everyone = just say no!

                - https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_examples.html

        - Other Policies

            - search for this with Google or the aws docs

                - Block public access for s3 (on by default)
                - Enable encryption (also on by default)
                - Bucket versioning (like volume shadow copy for S3)

    - Docker

        - Use trusted Docker images
        - https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html

    - Kubernetes

        - https://www.bluematador.com/blog/kubernetes-security-essentials

- Cloud, Container, and Kubernetes Security Tools

    - Qualys Cloud Platform

        - https://www.qualys.com/cloud-platform

    - Prisma Cloud

        - https://www.paloaltonetworks.com/prisma/cloud

    - Aqua

        - https://www.aquasec.com

            - Docker and Kubernetes (and basically everything else)

- Tenable Container Security
    - https://www.tenable.com/products/tenable-io/container-security
- Kube-bench
    - https://github.com/aquasecurity/kube-bench
- Sumo Logic
    - https://www.sumologic.com
-