controlplane

G-Cloud 14

Service Definition

Kubernetes, Security and Cloud Native Training

Lot 3 Cloud Support

Delivering world-leading consulting solutions
to secure cloud, Kubernetes, and software supply chains.
Secure-by-design and secure-by-default are in our DNA.

1. Introduction

Company Overview

Trusted by the world's most secure organisations to build and assure mission-critical platforms, we are a focused team of cloud native security experts with a passion for open source and a commitment to culture and collaboration.

We have industry-leading expertise in designing, delivering, and securing hardened, zero trust platforms for regulated industries. This deep understanding of secure-by-design and secure-by-default principles across cloud, Kubernetes, and supply chain security enables us to develop human-centric systems guided by precise and usable threat models. Our approach enhances delivery efficacy and surpasses industry standards.

From multinational banks and major public clouds to critical national infrastructure programs and government projects, startups and scale-ups to global healthcare and insurance providers, ControlPlane has secured a diverse portfolio of renowned customers.

Who Are We?

- Specialists in **Secure-by-Design** and **Secure-by-Default** architectures, tailoring solutions to fit the unique needs of our clients
- Highly skilled **consultants, implementers, and trainers**, excelling in bridging the communication gap between engineers and executives
- Experts with **deep industry knowledge** in **highly regulated** environments and a comprehensive understanding of **open source software** in **strategic programmes**
- Proudly serving a diverse range of clients, from the world's **largest banks** to **public sector entities** and **open-source R&D labs**
- Enablers of **team and organisational transformation** through adaptable Agile practices designed to enhance efficiency and innovation

- Renowned for **unparalleled customer satisfaction** and retention, thanks to our **deep expertise and flexibility** in navigating technical and regulatory domains

2. The Service

Kubernetes, Security and Cloud Native Training

ControlPlane's best-practice driven Kubernetes curriculum consists of instructor-led hands-on labs, practical examples, and real-world scenarios. These courses are informed by our wealth of experience deploying and supporting secure, high compliance, mission-critical distributed systems for some of the world's biggest brands.

All content is regularly updated to reflect the latest Kubernetes release and is informed by extensive community feedback and enterprise engagements.

Courses

Kubernetes Fundamentals

Specification

Course Length: two days

Class size: 5-30

Delivery method: Instructor-led classroom training, in-person or remote

Course Description

This course introduces participants to container orchestration with Kubernetes. Attendees will master the foundational concepts of Kubernetes in development and production through a combination of presentations, demos, and hands-on labs, including building and deploying Kubernetes applications, cloud native Continuous Delivery, and cluster monitoring and debugging. This course also covers system components, core resources, and the requirements for minimum viable cluster security.

Course Outline

- What real-world problems does Kubernetes solve?
- Kubernetes in historical context
- Container basics: Linux cgroups and namespaces
- Core resources and kubectl
- Kubernetes system components
- Container networking

- Developer workflow
- Deploying an application: CI pipeline, containerisation, testing, secure configuration, liveness & readiness probes, and useful kubectl tips
- Interactive cluster debugging

Who should attend?

This course is designed for those who are new to Kubernetes and containers, as well as those who have had exposure but would like to gain a deeper understanding. No prior knowledge of Kubernetes is required. This course is suitable for developers, operations, architects and anyone seeking to gain a strong foundation in modern, cloud native software delivery.

Kubernetes Operations

Specification

Course Length: two days

Class size: 5-30

Delivery method: Instructor-led classroom training, in-person or remote

Course Description

This course builds on Kubernetes Fundamentals by digging deeper into how Kubernetes works. It covers advanced features and use-cases to prepare engineers for the day-to-day reality of creating, maintaining and debugging Kubernetes clusters in production.

Course Outline

- Installing, upgrading, and maintaining Kubernetes
- Cluster architecture and topologies
- Advanced features: networking, storage and ingress
- Zero-downtime deployments and secrets management
- Maintaining etcd
- Enterprise RBAC and authentication
- Testing cluster security
- Interactive production cluster debugging
- Vendor and tooling landscape
- Comparison of cloud-provider Kubernetes offerings
- Self-service, multi-tenant Kubernetes platforms for enterprises

Who should attend?

This course is designed for anyone with a basic understanding of Kubernetes, and prepares attendees to run production Kubernetes clusters. The course is also suitable for technical managers who want a better understanding of an SRE's role in cloud native application delivery.

Kubernetes for Developers

Specification

Course Length: two days

Class size: 5-30

Delivery method: Instructor-led classroom training, in-person or remote

Course Description

This course builds on Kubernetes Fundamentals by going "under the hood" and examining the relationship between application workloads and the Kubernetes orchestrator. It details how to take advantage of Kubernetes features to deploy fault-tolerant autoscaling applications, release new versions with zero downtime, and debug failures.

Course Outline

- What's different about applications in Kubernetes
- How to containerise anything quickly and securely
- Development and test pipelines for containerised applications
- Communicating developer intent to the orchestrator
- How to compose an application in Kubernetes
- Secrets management, identity, and zero trust
- Observability, logging and telemetry for Kubernetes workloads
- Zero-downtime deployment options
- Top-down troubleshooting for each layer of the stack
- Demystifying container networking and cloud native firewalls
- Where, when, and why to persist the application state
- Container security 101
- Interactive production cluster debugging

Who should attend?

This course is designed for anyone with a basic understanding of Kubernetes and prepares attendees to run write applications for Kubernetes. The course is also

suitable for technical managers who want a better understanding of a developer's changing roles and responsibilities in cloud native application delivery.

Kubernetes and Container Security

Specification

Course Length: one day

Class size: 5-30

Delivery method: Instructor-led classroom training, in-person or remote

Course Description

The course guides attendees through Linux container security in general, and progresses to advanced Kubernetes cluster security. It emphasises pragmatic threat modelling and risk assessment based on an understanding of the tools and primitives available.

Course Outline

- How to attack containerised workloads
- Enhanced container security
- How to attack Kubernetes
- Interactive production cluster hacking
- Hardening Kubernetes
- Locking down applications
- Automated security testing and DevSecOps workflows
- Intrusion detection and breach analysis
- Security tooling and vendor landscape

Who should attend?

This course is suitable for developers, operations, and security engineers. It covers basic to advanced container and Kubernetes security for those that want to strengthen their security understanding. It is particularly beneficial for those operating Kubernetes in a high-compliance domain, or for established security professionals looking to update their skills for the cloud native world.

Advanced Kubernetes Security: Learn By Hacking

Specification

Course Length: Three Days (or Four Days with Capture the Flag scenarios)

Class size: 5-30

Delivery method: Instructor-led classroom training, in-person only

Course Description

This unique, industry-leading course takes attendees through the architecture, security, and delivery of Kubernetes systems for security-conscious organisations, using the best of current and next generation tooling. It is written by Hacking Kubernetes author and SANS instructor Andrew Martin.

Combining Red Team (offensive) and Blue Team (defensive) approaches, information security professionals and engineers will gain an understanding of the attack surface of a cloud native system: from building applications into containers and appraising supply chain vulnerabilities, through runtime detection and monitoring, to evading the system's defences and popping shells, this course gives you the tools you need to understand how to attack and defend against present and future threat actors. Attendees will gain hands-on experience building, exploring, and securing real-world systems through an offensive lens.

Attendees have access to cloud-hosted clusters and will examine methods of compromise, play attack scenarios against real infrastructure, and then shift their focus to defending and remediating infrastructure services. This includes hardening the Kubernetes orchestrator and workload configuration, deploying security testing and monitoring software in pipelines and clusters, attacking and defending container supply chains, cryptographically signing images and build pipelines, exploring intrusion detection and monitoring, applying AppArmor and Seccomp profiles to defeat attacks, and understanding next-generation runtimes.

The course leverages threat modelling to apply realistic attack vectors and define test driven security controls. These are applied at multiple stages throughout the pipeline to enhance engineers' productivity and feedback loops.

- Wargame custom scenarios against real clusters on production infrastructure
- Use real-world exploits to target key application deployment components
- Explore vulnerabilities to cloud native deployments through authentication, pipeline, and supply chain exploits
- Understand the risks involved in running cloud native infrastructure
- Threat model and remediate threats with optimal defensive controls

- Exploit and then secure application deployments via Docker and Kubernetes

Course Outline

- Container exploitation by example
- Kubernetes attack surface
- Kubernetes deployment pipelines
- Source control signing and verification
- Container image vulnerability scanning
- Circumventing pipeline controls
- Image signing with Cosign and Notary
- Pipeline metadata collection and enforcement
- Supply-chain verification with in-toto and Tekton Chains
- Kubernetes & container security testing
- Secure GitOps deployments with Flux
- Users, identity, and RBAC
- Runtime security and intrusion detection
- Network policy and lockdown
- Service meshes and workload identity
- Advanced container isolation

Who should attend?

This course is suitable for intermediate to advanced Kubernetes development, operations, and security teams, penetration testers, vulnerability assessors, and hands-on SOC analysts. Operational knowledge of Linux, Docker or Podman is a prerequisite and Kubernetes experience is essential. It is particularly beneficial for those operating Kubernetes in a high-compliance domain, and for established security professionals looking to update their skills for the cloud native world.

Threat Modelling Kubernetes

Specification

Course Length: one day

Class size: 5-30

Delivery method: Instructor-led classroom training, in-person or remote

Course Description

Traditional on-premise systems rely heavily on perimeter and firewall security: Kubernetes and cloud native systems present new threat profiles. Cloud technologies change rapidly as vendors introduce new managed services, and users evolve their usage of an ever-expanding toolset. Kubernetes moves fast and security must keep up with the speed of innovation.

Secure Kubernetes usage requires a thorough understanding of the system, its information assets, and any threats or risks posed by its use. In this course, we introduce modern and lightweight threat modelling. These techniques are designed for evolving cloud systems, to help security and engineering teams increase the security and velocity of system delivery.

Course Outline

- Introduction to the basic principles of threat modelling in a Kubernetes context:
- What are we building?
    - Business impact assessments for data
    - Data flow diagrams and information flow matrices
    - Understanding threat landscapes and adversaries
    - Kubernetes technical overview
    - Introduction to an example architecture to threat model
    - Information flow matrix lab
- What can go wrong?
    - Gathering techniques and threat sources
    - Modelling techniques
        - STRIDE
        - Attack Trees
    - Building Attack Trees as code
    - Key differences between cloud native and on-prem
    - Key Kubernetes threats to workloads, storage, networking and the control plane

    - STRIDE brainstorming lab
- What are we going to do about that?
    - Risk management techniques
    - Key Kubernetes security controls
    - Lab on selecting proportionate controls
- Did we do a good enough job?
    - Iterative threat modelling
    - Scaling the threat modelling process
    - Testing security controls in a hands-on lab

Who should attend?

This course is designed for anyone with a basic understanding of Kubernetes and cloud infrastructure who is interested in investigating formal threat modelling in a cloud native context. It is suitable for security architects and developers, and anyone who aspires to become a Security Champion, driving decisions with a sound understanding of the threats in your organisation's business environment.

GRC Threat Modelling with Cloud Native

Specification

Course Length: one day

Class size: 5-30

Delivery method: Instructor-led classroom training, in-person or remote

Course Description

This course builds on Threat Modelling Kubernetes by diving deeper into how formal threat modelling can be used to prove compliance with GRC requirements. The course is backed by a full reference Kubernetes Threat Model, linked to controls from industry frameworks and standards. It highlights how these controls can be implemented in practice using popular open source technologies. Attendees will leave with the practical knowledge and tools needed to design or audit secure-by-default Kubernetes-based systems, within highly regulated environments.

Course Outline

- Half-day "Threat Modelling Kubernetes" courseware delivery to introduce the fundamentals of Threat Modelling

- Attendees will then use the fundamental Threat Modelling techniques learned in the first half of the course to build up a complete, generic Kubernetes Threat Model
- Deep dive into applicable compliance frameworks
- Integration examples of popular open source technology into governance, risk management, and compliance frameworks, and demonstrations of how these technologies can help organisations meet compliance requirements
- Further hands-on scenario-focused threat modelling based on real customer needs and “straw man” architectures presented by attendees to update the initial generic Threat Model

Who should attend?

This course is designed for audit and regulatory teams that may have had some exposure to Kubernetes, but who are not well acquainted with how to meet strict GRC requirements for rapidly evolving, cloud native systems. By working through a complete Kubernetes Threat Model, fully mapped to key compliance standards, attendees will leave with the confidence needed to run, audit and assure Kubernetes clusters in highly regulated contexts.

3. Provision of the Service

Customer Responsibilities

ControlPlane will inform the customer of any device or network requirements which must be met for attendees to successfully complete the course. It is the customer’s responsibility to ensure that attendees have access to compliant devices. ControlPlane is able to provide a classroom and arrange logistics if needed. This will be charged as per our T&Cs and the agreed Statement of Work.

After-Sales Account Management

As part of ControlPlane’s account management, we ensure that attendees are sent a post-training survey to provide feedback on their experience. This survey allows ControlPlane to deliver training more suited to your preferences in future and discuss opportunities for further collaboration or support.

4. Our Experience

Case Studies

We deliver our unique, hands-on cloud native security training at KubeCons and conferences, and under licence for O'Reilly Online ("Attacking and Defending Kubernetes" and "Threat Modelling Kubernetes"), and authored the SANS SEC584 Kubernetes course.

ControlPlane CEO Andrew Martin co-authored the O'Reilly book "Hacking Kubernetes".

ControlPlane orchestrated the creation of the Cloud Native Security Associate (KCSA) Exam for the Linux Foundation (LF). In addition, we authored two zero trust security courses for LF: LFS183x, a free e-learning course entitled "Introduction to Zero Trust", and LFS482, a three day, instructor-led course on "Zero Trust Security with SPIFFE and SPIRE".

Clients

From multinational banks and major public clouds to critical national infrastructure programs and government projects, startups and scale-ups to global healthcare and insurance providers, ControlPlane has secured a diverse portfolio of renowned customers.

What our clients say about us

"

You deliver and set standards in a way that others struggle to match.

Director - Cloud Security, Multinational Bank

"

I cannot ask for better people: they are driven to improve, help and collaborate.

Director - Cloud Security, Multinational Bank

"

Assistance in supporting our Agile team has proved invaluable.

Senior VP - Cloud Security, Multinational Bank

Accreditations

GKE Benchmarks	Hacking Kubernetes	SEC-584
Chosen by Google to audit and author the CIS Benchmarks for Google Kubernetes Engine (GKE)	Authored the technical attack and defense guide Hacking Kubernetes for O'Reilly	Authors of SANS SEC-584: Cloud Native Security: Defending Containers and Kubernetes

Core Competencies

Consulting	Training & Events	Community Engagement
• Cloud Native **transformations** • Kubernetes, container, and cloud **security** • **Zero-Trust** architecture design and assurance • **DevSecOps** infrastructure and application delivery • Secure SDLC and continuous delivery **pipelines** • Hardened **supply chain** build and automation • Cloud Native **SOC integration** • **Pentest, Red, Blue, Purple Team** • **Products** and **platforms security audit and review**	• **CNCF** Official Training Partner • **SANS** and **O'Reilly** authors and trainers • Secure Kubernetes **Operations, Application Delivery**, and **Advanced Pentesting** courses • **Advanced Kubernetes Security: Learn By Hacking** (former SANS SEC584) • **Capture The Flag (CTF)** events held at **KubeCon** (3 years running), and privately for developers, operations, and **red/blue** teams • Original **Docker** trainers • Original **Hashicorp** trainers	• Prolific **international** and community **public speakers** • **Conference** and meetup **organisers and volunteers** • **Free hands-on workshops**, teaching hacking, debugging, and security, at **local and international** events • **CFP reviewers** for largest container and **Kubernetes industry events** (KubeCon, Cloud Native SecuityCon) • Container Camp **curators and volunteers** for all 7 events (London to San Francisco)

G-Cloud Offerings

ControlPlane offers the following services on the G-Cloud Framework

Lot 2

- ControlPlane Enterprise for Flux CD

Lot 3

- Penetration Testing
- Security Assessments and Threat Modelling
- Security Architecture and Security Engineering
- Agile Delivery Services for Cloud Native Security
- Kubernetes, Security and Cloud Native Training

Contact Details

For more information or to speak with an account manager, please get in touch:

solutions@control-plane.io

https://control-plane.io/