magentai

Integrated Cybersecurity Workshop

Magentai presents its modular Integrated Cybersecurity Workshop - a customizable engaging, interactive event focused on helping you dive into Secured hybrid- cloud architectures, essential services, design-patterns, and application evolution.

Customers will get an overview of current techniques and practices with comparisons to current methods, and tool-sets. This interactive workshop includes use cases, presentations, and demonstrations that will get you and your team quicklly up to speed on the latest in Modern Cybersecurity.

Engagement Overview

In this interactive session, Magentai will highlight key aspects of AI-driven zero trust, segmentation, multi-cloud user access control, secured user access, hybrid mesh firewall, security methodologies, and popular use cases. To gain a better understanding we will explore 1 or 2 real-world case studies relevant to the modules being presented.

Course Details

Delivery Method

- Instructor-Led Training conducted by Modern Cybersecurity Architects with real-world experience designing and implementing
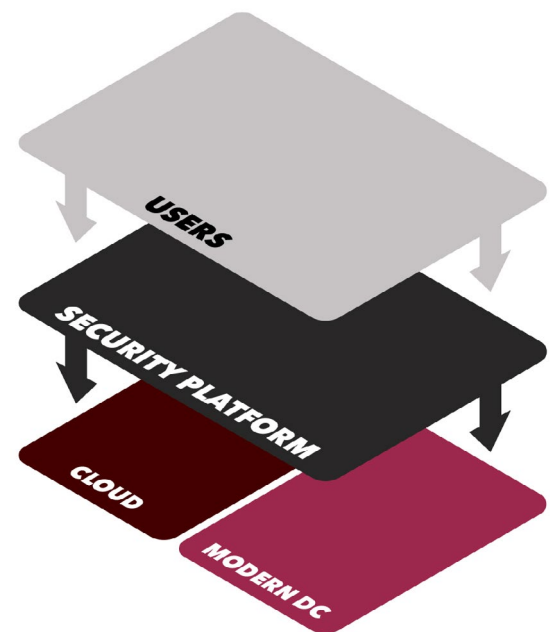
Time Commitment

- 2-4 hours

Suggest Audience

- Security Architects

- Security Operations

- Network Architects

- Governance & Compliance

- IT Stakeholders

Prerequisites

- Understanding of rudimentary concepts of private and public cloud networking and modern security terminology.

A Unified Approach

Deliverables

Customized Materials: Magentai will provide workshop slides presented

Findings and Next Steps: A package consisting of a handout with customer findings will be created and delivered via a 1-hour follow-up session.

magentai

Magentai is a world-class Cybersecurity services provider, dedicated to implement, integrate and operate the most resilient Cybersecurity platforms using proven state-of-the-art technologies. With a team of seasoned experts and cutting-edge technology, we deliver comprehensive solutions tailored to our clients' unique needs, ensuring their digital assets remain secure in an increasingly complex cyber landscape.

For more information or to engage our services, please contact us at info@magentai.com or visit https://magentai.com

Integrated Cybersecurity Workshop

The following is a list of potential modules presented during the Workshop. The final agenda will be customized based on requirements or per special request. Choose up to 2 modules.

Zero Trust Strategies

The border has dissolved and now people, applications, and data reside in multiple places. With a growing number of security solutions, Magentai offers an overview to make sense of the security landscape and how the pieces come together to create a zero-trust strategy.

Cybersecurity & AI

Explore how AI is transforming cybersecurity, moving beyond a buzzword to become a critical tool in combating sophisticated threats. We'll cover key trends, real-world applications, and discuss both the benefits and challenges of integrating AI into cybersecurity strategies.

Segmentation

Discuss advanced segmentation mechanisms that secure the network with ease of control. Discuss how application and workload protection can be accomplished with integrated firewall, identity services and segmentation capabilities.

Product Deep Dive

Pick one ot two of these Cisco products to get a technical deep dive of functionality, architecture, and use cases associated with the solution: Secure Workload, Secure Access, Identity Services Engine, Secure Firewall, XDR, Security Cloud Control.

Secure Access

Explore modern Secure Access best practices that encompass keeping a data center secure from threats, attacks, and unauthorized access. Understand how access controls work together to prevent breaches.

Breach Detection and Mitigation

Breach detection tools can help identify threats inside your network. Learn about the pillars and support mechanisms needed to be put in place alongside the tools to recognizing active threats and alerting relevant security staff.

Cybersecurity Architectures

The security model has evolved as we move from traditional data-centers to cloud-centric targets and the border has dissolved. Understand changes to key threats and new security models as you build your security strategy.

Identity Management and Protection

Leveraging identity and stolen credentials is still a main threat vector outside and within the organization. Learn about the controls in this space from identity to privilege access management and other controls in this space.

Cloud Security Controls

Cloud security leverage different patterns than those in the datacenter. Explore foundational patterns in the cloud security space with a focus on leveraging cloud-native controls.

Creating a Modern Cyber Framework

Compliance frameworks exist to help customers measure their security strategy against a rubrick. Learn about popular frameworks like NIST and FAIR and how best to apply them to your organization.

Security Visibility (FSO)

Visibility exists in organizations but rarely with a security context. Furthermore translating visibility to security policy is challenging. Learn how to derive visibility, score assets, and translate that visibility to policy.

Hybrid Mesh Firewall

Review a unified security platform designed to protect diverse IT environments, including corporate networks, cloud infrastructure, and remote workers, by providing centralized management for consistent policy enforcement and threat mitigation

Security Operations: XDR/MDR

Learn about the pillars of security operations that are becoming more of a requirement for security platforms. Explore the operational models in place today in most enterprises to keep ahead of attackers.

Layered Network Security: Firewall/Network/uSeg/DNS

Leveraging identity and stolen credentials is still a main threat vector outside and within the organization. Learn about the controls in this space from identity to privilege access management and other controls in this space.

Vulnerability Management

Learn about techniques for managing and remediating cyber vulnerabilities across endpoints, workloads, and systems. Score assets based exposure to CVE's and map that against popular attacks in the wild to create an approach to managing vulnerabilities.

SECURITY MODULES: **STRATEGIC**   **TECHNOLOGY**