mimecast | education

Mimecast Education Courses and Certification Tracks

Table of Contents - Courses

* To be released second half of 2021

Mimecast Education Course Offering by Product

Product	Course	Duration	Certification track
Secure Email Gateway (SEG)	Set up and Administration Fundamentals	5 hours	Warrior
	Security Policy Fundamentals	2 hours	Warrior
	Email Continuity	1 hour	Warrior
	Advanced Email Hygiene & Security Best Practices	3 hours	Gladiator
	Advanced Message Center	2 hours	Gladiator
	Advanced Targeted Threat Protection	2 hours	Gladiator
	Advanced Information Protection	2 hours	Gladiator
	Advanced Internal Email Protect and Threat Remediation	1 hour	Gladiator
	Cybergraph Fundamentals (video)	1 hour	Gladiator
Cloud Archive	Fundamentals	2 hours	Stand-alone
	Compliance*	1.5 hours	Stand-alone *
	Management*	1.5 hours	Stand-alone *
API	Fundamentals	23 min (video)	Stand-alone
DMARC Analyzer	Fundamentals	1 hour	Stand-alone
Brand Exploit Protect	Fundamentals	1 hour (video)	Stand-alone
Awareness Training	Fundamentals	1 hour	Stand-alone
Web Security	Fundamentals	2 hours	Stand-alone

See full certification program here

* To be released second half of 2021

Course Name	Course Level	Prerequisites	Description	Learning Objectives
[2] Secure Email Gateway: Set up and Administration Fundamentals	**Level 1**	**Prerequisites:** N/A	**Description:** This course is designed to help you get started with Mimecast by learning how to set up and navigate the Mimecast Administration Console, which provides central administrative control for all your security policies. You will also learn about how to access reports, as well as the Service Monitor and Status pages.	**Learning Objectives:** Following the course, you should be able to: • Navigate and understand the functionalities of the Administration Console • Understand where the Service Status page is located • Explain what configurations are available in the Account Settings • Set up Mimecast services and setup mail flow • Create and manage Mimecast administrators • Synchronize your organization's directory and manage your users and groups • Control user access to end-user apps and the limits within • Schedule and read reports • Explain the service monitor features and create alert notifications along • Troubleshoot email delivery in Message Center
[3] Secure Email Gateway: Security Policy Fundamentals	**Level 1**	**Prerequisites:** SEG: Setup and Administration + Analytics	**Description:** This course is designed to help you understand the basics of the Mimecast Secure Email Gateway capabilities and how Mimecast multi-layered detection engines and intelligence protect organizations from phishing, malware, spam and zero-day attacks. Focusing on spam scanning and malware protection, this course ensures administrators have the knowledge necessary to effectively protect their organization's email with Mimecast. Also covered is a high-level overview of the Targeted Threat Protection configurations.	**Learning Objectives:** Following this course, you should be able to: • Understand the Mimecast Email Inspection Funnel and what checks are performed on emails by Mimecast • Understand the way email security policies are organised, scoped, and applied • Explain common email security policies and their uses • Overview of our Targeted Threat Protection configurations
[5] Email Continuity: Fundamentals	**Level 1**	**Prerequisites:** SEG: Setup and Administration Fundamentals	**Description:** The course is designed to help administrators to prepare their Mimecast environment for continuity events and the communications to coincide with those events.	**Learning Objectives:** Following this course, you should be able to: • Create continuity events and continuity monitors • Establish a server connection for continuity monitoring • Respond to a continuity monitor alert • Build an SMS response to continuity events

* To be released second half of 2021

Course Name	Course Level	Prerequisites	Description	Learning Objectives
[6] Secure Email Gateway: Email Hygiene & Security Best Practices	**Level 2**	**Prerequisites:** Warrior Certified	**Description:** This course is designed to provide you with knowledge and skills needed to effectively protect your organization's email with Mimecast. Focusing on basic email security policy configuration and discussion of best practices, this course will help you stop spam and malware before it reaches your email system.	**Learning Objectives:** Following this course, you should be able to: • Understand the default security policy configurations • Scope and customize email security policies based on the needs of your organization • Understand best practices for security policy configuration
[7] Secure Email Gateway: Advanced Message Center	**Level 2**	**Prerequisites:** Warrior Certified	**Description:** This course is designed to equip Mimecast administrators with the skills needed to investigate delivered and blocked emails with our robust message tracking and analysis tools. With the help of common scenarios and use cases, you will learn how to troubleshoot message delivery and respond to queries from your users (e.g., when they ask about specific emails) as well as inspect suspicious messages that may be false positives.	**Learning Objectives:** Following this course, you should be able to: • Understand best practices for security policy configuration • Effectively monitor email flows and the different message queues • Search across multiple queues • Analyze information provided in logs • Effectively deal with most common queries from users • Troubleshoot message delivery
[8] Secure Email Gateway: Advanced Internal Email Protect and Threat Remediation	**Level 2**	**Prerequisites:** Warrior Certified	**Description:** This course will provide use cases for configuring Internal Email Protect to protect your internal, outbound, and delivered messages from malware and sensitive content. It will also help you understand how you can use threat remediation to remove dangerous content from your users' mailboxes if discovered after delivery.	**Learning Objectives:** Following this course, you should be able to: • Configure Internal Email Protect for URL Protect, Attachment Protect and Content Examination to conduct additional security checks on both internal journaled and outbound email. • Automatic remediation of any newly found, zero-day attachment-based malware detected in your user's mailboxes"
[9] Secure Email Gateway: Advanced Targeted Threat Protection	**Level 2**	**Prerequisites:** Warrior Certified	**Description:** This course is designed to provide you with the skills and knowledge needed to effectively implement Targeted Threat Protection in your organization. Focusing on configuration best practices for all TTP Suite products, this course ensures you can customise policies based on your organization's needs and remediate against both internal and external threats.	**Learning Objectives:** Following this course, you should be able to: • Understand the default TTP policy configurations and customize for your organization • Configure TTP end-user awareness • Apply TTP best practices • Enable device enrollment • Configure Browser Isolation for email • Remediate against internal threats using Threat Remediation • Monitor and analyze TTP dashboards and logs

* To be released second half of 2021

Course Name	Course Level	Prerequisites	Description	Learning Objectives
[10] Secure Email Gateway: Advanced Information Protection	**Level 2**	**Prerequisites:** Warrior Certified SEG: Email Hygiene & Security Best Practices	**Description:** This course will equip you with practical skills and knowledge needed to prevent sensitive information from falling into the wrong hands with Mimecast comprehensive data loss prevention (DLP) solution. Focusing on common configurations and best practices of DLP policies, Secure Messaging and Large File Send, this course will provide you with a deep understanding of capabilities to protect sensitive information as it travels via email.	**Learning Objectives:** Following this course, you should be able to: • Enable and manage real-time protection against outbound data leaks (DLP) with customized Content Examination policies • Configure Content Examination policy and explain when and how it is triggered • Configure Large File Send for your organization • Enable and configure Secure Messaging service • Use LFS and Secure Messaging to send sensitive information securely
[11] Secure Email Gateway: Cybergraph Fundamentals	**Level 2**	**Prerequisites:** N/A	**Description:** This course will equip you with practical skills and knowledge needed to prevent sensitive information from falling into the wrong hands	**Learning Objectives:** Following this course, you should be able to: • Enable and manage real-time protection against outbound data leaks (DLP) with customized Content Examination policies
[12] Cloud Archive: Fundamentals	**Level 1**	**Prerequisites:** SEG: Setup and Administration Fundamentals	**Description:** This course is designed to help you understand the basics of the Mimecast Cloud Archive capabilities.	**Learning Objectives:** Following the course, you should be able to: • Search the email archive in the Mimecast Administration Console and end-user apps • Save and export Archive Searches • Export archived message data and monitor exports • Work with Archive View and Search Logs • Create and use smart tags • Create and manage eDiscovery Cases in the Case Review Application • Adjust data retention periods and expire emails from the Mimecast Archive • Know how to configure Mimecast Synchronization Engine (MSE) and work with Archive Power Tools
[13] Cloud Archive: Compliance*	**Level 2**	**Prerequisites:** Cloud Archive: Fundamentals	**Description:** This course is designed to provide you with knowledge and skills needed to effectively install, configure, and use the Mimecast Archive compliance tools. Focusing on real life scenarios, this course will assist you in effectively utilizing the tools within the Archive product set to help you meet all your compliance needs.	**Learning Objectives:** Following this course, you should be able to: • Set up and use eDiscovery, Reviewer, and Supervision • Leverage use cases for eDiscovery, Reviewer, Supervision and Compliance Protect to effectively carry out archive compliance tasks in your environment

* To be released second half of 2021

Course Name	Course Level	Prerequisites	Description	Learning Objectives
[14] Cloud Archive: Management*	**Level 2**	**Prerequisites:** Cloud Archive: Fundamentals Cloud Archive: Compliance	**Description:** This course is designed to provide you with the knowledge and skills needed to effectively install, configure, and use Mimecast Archive management tools. Focusing on real life scenarios, this course will also help you to effectively utilize the tools within the Archive product set to help you meet all your email management needs.	**Learning Objectives:** Following this course, you should be able to: • Install and configure the Mimecast Synchronization Engine (MSE) • Leverage use cases MSE and Sync & Recover tools to effectively carry out archive management tasks in your environment
[15] DMARC Analyzer: Fundamentals	**Level 1**	**Prerequisites:** N/A	**Description:** This course is designed to help administrators understand the basics of DMARC and related email authentication methods and how Mimecast DMARC Analyzer platform can help protect their organization's domains from spoofing and abuse.	**Learning Objectives:** Following this course, you should be able to: • Understand what is DMARC and explain how it works • Understand Identifier Alignment in DMARC • Know how DMARC record looks like and explain its components • Describe and compare three different DMARC policy levels and how they affect the way email is handled • Understand the different types of DMARC reports • Navigate the DMARC Analyzer dashboard and read report data
[16] Brand Exploit Protect: Fundamentals (Video)	**Level 1**	**Prerequisites:** N/A	**Description:** This course is designed to help you understand the basics of the Mimecast Brand Exploit Protect (BEP) capabilities and the BEP platform. The course will help ensure that the administrators have the knowledge and skills necessary to effectively protect their brand against exploitation by the domains the organization does not own.	**Learning Objectives:** Following this course, you should be able to: • Understand the threat landscape related to domain / brand impersonation and how brands/domains are used for phishing attacks • Explain how BEP performs web scanning, how it detects and remediates against threats • Understand and analyse information provided in the BEP dashboards and take appropriate action based on that information • Know how to configure BEP integration with Email and Web security solutions • Explain the process of taking down an attack with BEP using an example case

* To be released second half of 2021

Course Name	Course Level	Prerequisites	Description	Learning Objectives
[17] API: Fundamentals (Video)	**Level 1**	**Prerequisites:** N/A	**Description:** This course is designed to help you understand the basics of Mimecast's APIs and how they work in integrations. You will also gain a better understanding of some of the security tools in your ecosystem.	**Learning Objectives:** Following the course, you should be able to: • Understand the challenges IT / security operations teams face • Know what an Ecosystem is comprised of • Understand what an API is and the value it can bring to an organization • Explain how Mimecast's APIs can be used to share data and functionality • Know how an integration works, the benefits and the different types of integrations • Understand what SIEM, SOAR, IT Help / Service Desk and Endpoint systems are and Mimecast integration use cases for them • Explain the importance of sharing threats between your security platforms
[19] Awareness Training: Fundamentals	**Level 1**	**Prerequisites:** N/A	**Description:** This course is designed to help you learn how to configure and manage the Mimecast Awareness Training product.	**Learning Objectives:** Following this course, you should be able to: • Understand what Awareness Training provides for a company • Synchronize your directory • Configure your settings • Schedule training from the Queue and Launch a Campaign • Know what the end user experience looks like • Manage Reminder and Watchlist Notifications • Effectively leverage information from the Dashboard and Reports • Monitor achievements and areas where users need improvement • Send out a Phishing Campaign and view the results
[20] Web Security: Fundamentals	**Level 1**	**Prerequisites:** SEG: Setup and Administration SEG: Targeted Threat Protection	**Description:** This course is designed to provide the administrators with the skills and knowledge needed to set up Mimecast's Web Security product from pre-deployment to post-deployment.	**Learning Objectives:** Following this course, you should be able to: • Understand Mimecast's Web Security capabilities • Understand Network Level Protection • Explain how the Mimecast Security Agent works • List the pre-deployment activities • Know how to deploy Web Security to networked and roaming devices • Know how to create Web Security policies • Understand the post-Deployment activities • Know how to read Web Security dashboards • Access and interpret report data

* To be released second half of 2021