CERTIFIED SOC ANALYST (CSA) EĞİTİMİ

5 GÜN

Digital Vizyon Akademi

www.digitalvizyon.net

İçindekiler

Eğitim Hakkında

Certified SOC Analyst (CSA) Eğitimi, güvenlik operasyonları merkezi (SOC) analisti olmayı hedefleyen profesyonellere yönelik kapsamlı bir sertifikasyon programıdır. Bu eğitim, katılımcılara bilgisayar ağlarında güvenlik olaylarını tespit etme, analiz etme ve yönetme konularında derinlemesine bilgi ve beceriler kazandırmayı amaçlamaktadır.

CSA eğitimi, SOC analistinin rolünü ve sorumluluklarını anlamak için gerekli olan temel bilgileri sunmaktadır. Ayrıca, güvenlik olaylarına hızlı ve etkili bir şekilde müdahale etme yeteneklerini geliştirme konusunda katılımcılara yardımcı olur. Böylece, ağ güvenliğini artırmak için proaktif önlemler almayı öğrenirler.

Eğitim sürecinde, katılımcılar güvenlik olaylarını tespit etmek ve analiz etmek için kullanılan araçlar ve teknikler hakkında kapsamlı bir bilgi sahibi olurlar. Özellikle, Güvenlik Bilgisi ve Olay Yönetimi (SIEM), log analizi, tehdit istihbaratı ve olay yanıtı gibi konulara odaklanılır. Bu sayede, katılımcılar güvenlik olaylarını etkili bir şekilde tanımlama, analiz etme ve yönetme becerilerini geliştirirler.

CSA eğitimi aynı zamanda saldırıları tanımlama ve sınıflandırma becerilerini geliştirmeyi hedefler. Katılımcılar, zararlı yazılım analizi, ağ trafiği izleme ve tehdit istihbaratı kullanarak saldırıları tespit etme ve saldırıya uğrayan sistemlerin analizini yapma konusunda yetkinlik kazanırlar.

Eğitim programı, SOC analistinin iletişim ve raporlama becerilerini de önemsemektedir. Bu doğrultuda, katılımcılar güvenlik olaylarını ve analiz sonuçlarını yöneticilere, ekip üyelerine ve ilgili paydaşlara etkili bir şekilde iletebilmeyi öğrenirler. Böylece, güvenlik operasyonları merkezlerinde etkin bir iletişim ağı kurulabilir.

CSA sertifikası, katılımcıların SOC analisti olarak çalışma yeteneklerini ve uzmanlıklarını kanıtlar. İşverenler, bu sertifikayı güvenlik operasyonları merkezlerinde çalışacak profesyonellerin niteliklerini değerlendirmede önemli bir kriter olarak kabul etmektedir. CSA sertifikalı profesyoneller, güvenlik olaylarını etkin bir şekilde yönetme ve organizasyonların ağ güvenliğini sağlama konusunda güçlü bir yetkinlik sergilemektedir.

Sonuç olarak,Certified SOC Analyst (CSA) Eğitimi, güvenlik operasyonları merkezlerinde çalışmak isteyen profesyonellerin güvenlik olaylarını tespit etme, analiz etme ve yönetme becerilerini geliştirmelerini sağlar. Bu eğitim sayesinde katılımcılar, organizasyonların ağ güvenliğini güçlendirerek, siber saldırılara karşı daha etkili bir şekilde korunma sağlayabilirler. Ayrıca, geçiş cümlelerini daha etkin bir şekilde kullanarak paragraf akışını daha da iyileştirmek mümkündür.

Neler Öğreneceksiniz?

Certified SOC Analyst (CSA) eğitimi sırasında aşağıdaki konuları öğrenebilirsiniz:

- Güvenlik Olayları Analizi: Güvenlik olaylarını tespit etme ve analiz etme becerilerinizi geliştirirsiniz. Olayların kökenini belirleme, olayları sınıflandırma, olaylara yanıt verme ve sorunları analiz etme konularını öğrenirsiniz.
- Tehdit İstihbaratı ve Tehdit Değerlendirmesi: Tehdit istihbaratını kullanarak güvenlik olaylarını değerlendirme becerilerinizi geliştirirsiniz. Tehdit istihbaratı kaynaklarına erişim, tehdit aktörlerini takip etme, saldırı yöntemlerini analiz etme ve tehdit istihbaratının SOC operasyonlarına entegrasyonunu öğrenirsiniz.
- Sistem ve Ağ İzleme: Sistem ve ağ izleme tekniklerini ve araçlarını öğrenirsiniz. Log analizi, ağ trafiği izleme, saldırı tespiti sistemleri gibi araçları kullanarak olayları izleme ve tehditleri tespit etme yeteneklerinizi geliştirirsiniz.
- Olay Yanıtı ve İzleme: Olaylara hızlı ve etkili bir şekilde yanıt verme ve izleme becerilerinizi geliştirirsiniz. Olaylara müdahale etme süreçlerini ve izleme tekniklerini öğrenirsiniz. Saldırıları durdurma, etkisini azaltma ve sistemleri yeniden yapılandırma konularında uzmanlaşırsınız.
- Olay Yönetimi ve Raporlama: Olay yönetimi süreçlerini ve raporlama becerilerini geliştirirsiniz. Olayların kaydedilmesi, sınıflandırılması, takibi ve raporlanması için kullanılan yöntemleri ve araçları kullanmayı öğrenirsiniz.

CSA eğitimi, güvenlik olaylarını daha etkin bir şekilde analiz etmek ve güvenlik tehditlerine karşı etkili bir şekilde yanıt vermek için gerekli bilgi ve becerileri sağlar. Olayları tespit etme, analiz etme, yanıtlama, izleme ve raporlama konularında uzmanlaşarak organizasyonun güvenlik durumunu iyileştirebilirsiniz. CSA sertifikası, güvenlik olaylarına profesyonel bir yaklaşım sergilediğinizi ve SOC operasyonlarında başarılı olabileceğinizi gösterir.

Ön Koşullar

Certified SOC Analyst (CSA) eğitimine katılmadan önce belirli bir ön koşul bulunmamaktadır. Ancak, aşağıdaki bilgi ve deneyimler, eğitimi daha iyi anlamanıza ve başarılı bir şekilde tamamlamanıza yardımcı olabilir:

- Bilgi Güvenliği Temelleri: Bilgi güvenliği konularında temel bir anlayışa sahip olmanız önerilir. Güvenlik prensipleri, saldırı türleri, güvenlik kontrolleri ve güvenlik tehditleri hakkında genel bir bilgiye sahip olmak, eğitim sürecini daha verimli hale getirebilir.
- Ağ ve Sistem Güvenliği: Ağ ve sistem güvenliği konularında bir temel bilgiye sahip olmak faydalı olacaktır. Ağ yapılandırması, ağ protokolleri, güvenlik duvarları, saldırı tespit sistemleri gibi temel ağ güvenliği kavramlarına aşina olmak, SOC operasyonlarını daha iyi anlamanıza yardımcı olabilir.
- Olay İzleme ve Log Analizi: Olay izleme ve log analizi süreçleri hakkında bilgi ve deneyim sahibi olmak faydalıdır. Olayları izleme araçlarını kullanma, log kayıtlarını analiz etme ve

saldırıları tespit etme konularında deneyim kazanmış olmak, eğitimi daha iyi anlamanıza yardımcı olabilir.

Bu ön bilgi ve deneyimler, CSA eğitimine katılmadan önce size avantaj sağlayabilir, ancak kesin bir ön koşul değildir. Eğitimi sağlayan kuruluşun belirlediği spesifik ön koşulları kontrol etmek önemlidir, çünkü gereksinimler farklı kuruluşlar arasında değişebilir. Eğitim sağlayıcının belirlediği ön koşulları karşıladığınızdan emin olmanız önerilir.

Kimler Katılmalı

Certified SOC Analyst (CSA) eğitimi aşağıdaki profesyoneller için uygun olabilir:

- SOC Operasyonları Personeli: Güvenlik Operasyon Merkezi (SOC) ekiplerinde çalışanlar, güvenlik olaylarını analiz etme, tehditleri tespit etme ve müdahale etme becerilerini geliştirmek için CSA eğitimine katılabilirler. Bu eğitim, SOC operasyonlarında etkin bir şekilde çalışmalarına yardımcı olur.
- Güvenlik Analistleri: Güvenlik analistleri, güvenlik olaylarını tespit etme, analiz etme ve yanıtlama konularında bilgi ve beceri kazanmak isteyebilirler. CSA eğitimi, güvenlik analistlerinin olayları etkin bir şekilde yönetmelerine ve organizasyonun güvenlik savunmasını güçlendirmelerine yardımcı olur.
- Olay Yanıtı Ekipleri: Olay yanıtı ekipleri, güvenlik olaylarına hızlı ve etkili bir şekilde yanıt vermekle görevlidir. CSA eğitimi, bu ekiplerin olayları yönetme, analiz etme ve müdahale etme becerilerini geliştirmelerine yardımcı olur.
- Sistem ve Ağ Yöneticileri: Sistem ve ağ yöneticileri, organizasyonun ağ altyapısının güvenliğini sağlamak ve güvenlik olaylarını yönetmekle sorumludur. CSA eğitimi, bu yöneticilere güvenlik olaylarını tespit etme, analiz etme ve yanıtlama konularında bilgi ve beceri kazandırır.
- Güvenlik Danışmanları ve Denetçiler: Güvenlik danışmanları ve denetçiler, müşterilere güvenlik operasyonları ve olay yönetimi konularında rehberlik etmek isteyebilirler. CSA eğitimi, danışmanlık ve denetim süreçlerinde güvenlik olaylarını etkili bir şekilde yönetme yeteneklerini geliştirmek için uygundur.

Yukarıdaki gruplar, CSA eğitimine katılmak için uygun olabilecek örneklerdir. Ancak, herhangi biri, güvenlik olaylarına ilgi ve motivasyona sahipse, bu eğitime katılarak bilgi ve becerilerini geliştirebilirler. SOC operasyonlarına katılmak, güvenlik analizi yapmak veya güvenlik olaylarını yönetmek isteyen herkes, CSA eğitimine katılabilir.

Outline

Module 01: Security Operations and Management

Module 02: Understanding Cyber Threats, IoCs, and Attack Methodology

Module 03: Incidents, Events, and Logging

Module 04: Incident Detection with Security Information and Event Management (SIEM)

Module 05: Enhanced Incident Detection with Threat Intelligence

Module 06: Incident Response