موسسه نورانت

NooraNet®
CyberSecurity Leadership

نام دوره : ArcSight ESM	مدت دوره : ۳۰ ساعت	اعتبار دهنده: HP

❖ توضیح دوره :

نصـــــب ، پیکر بندی و استقرار ابزار در دوره ArcSight ESMو نحوه راهبری مرکز عملیات امنیت به وســـــیله ArcSight ESMموضوعی است که در دوره ArcSight ESMارائه می گردد. شـــرکت ArcSightپس از اینکه توسـط HPخریداری شـد، بلافاصـــله به عنوان پرچمدار SIEMدر دنیا قرار گرفت و توانســـــت در مدت کوتاهی بسـیاری از ساختارهای استاندارد مرکز عملیات امنیت را پایه ریزی نماید. این ابزار یکی از پرکاربـردتـرین SIEM های دنیا است.

❖ پیش نیاز دوره

- تسلط بر مفاهیم TCP/IP و لایه های شبکه
- LPIC 1
- Microsoft Specialist
- آشنا به مفاهیم تحلیل Logو رویدادهای امنیتی
- CEH
- ArcSight SmartConnector Level 1

❖ مجوزها و اعتبارات

دارای مجوز رسمی از :

- شورای عالی انفورماتیک
- اداره کل نظام مدیریت امنیت اطلاعات
- سازمان نظام صنفی رایانه ای
- گواهی ISO9001

❖ امتیازات دوره :

- اساتید با تجربه (بالای ۱۲ سال سابقه)
- لابراتوارهای مجهز
- اعطای مدارک فارسی و انگلیسی با قابلت ترجمه و تایید قوه قضاییه
- مشاوره رایگان قبل و بعد از دوره
- دسترسی به پرتال اختصاصی noorasec

❖ مخاطبین دوره

مدیران و کارشناسان مرکز عملیات امنیت

آدرس: تهران-خیابان مطهری-خیابان کوه نور- کوچه دوم پلاک ۹ -طبقه اول
تلفن : ۸۸۱۷۵۵۶۰ - فکس : ۸۸۱۷۵۵۳۴

www.noorasec.com
Info@noorasec.com

NooraNet®
CyberSecurity Leadership

موسسه نورانت

سرفصل دوره ArcSight ESM

Introduction to ESM 6.5
Define ESM User Roles
List ArcSight Components, Interfaces, Information Resources

ArcSight Event Schema and Life Cycle
Describe ESM Event Schema and Schema Groups
Identify ArcSight Event Life Cycle Phases and Schema population

ArcSight ESM Install and Configuration
Describe Pre-Install Requirements
Identify Install Process (Wizards)
Describe reconfiguration

ArcSight ESM Console
Describe Login, user preference, and main tool bar facilities
Navigate resource tree, viewer and edit/inspect panels

ArcSight Command Center
Login, navigate main tab means
Access dashboards, event search, report, and workflow cases
Navigate administrative facilities for ESM system configuration, archive ,connectors status, and event storage

ArcSight Web Interface
Login to the home page
Access dashboards, reports, active channel ,notifications

Active Channels, Filters and Field Sets
Access active channels and modify filters and field sets
Use right-click means and event investigation facilities

ESM Rules and Lists
Differentiate simple vs join type rules, real-time vs scheduled rules
Edit rule attributes, including conditions, aggregation, actions, triggers
Explain the use of active lists and session lists

Dashboards and data monitors
Access dashboards the interpret data monitor display
Describe the benefits of using identity view
Explain drill down to active channels

Query viewers
Describe query viewer usage
Edit query viewers, establish baselines, define drilldowns

ESM Reports
Enter report runtime parameters, run,archive reports
Edit focused reports and delta reports
Established and manage report scheduling distribution

User Administration
Create ESM Users and User Groups
Explain the administration of ACLs
Password Policies

User Notifications
Describe notification functions and responses
Access, modify and configure notifications

Event search, filters and saved searches
Search events using the search builder/advanced search tools
Display search results and select output options

www.noorasec.com
Info@noorasec.com

آدرس: تهران-خیابان مطهری-خیابان کوه نور- کوچه دوم پلاک ۹ -طبقه اول
تلفن : ۸۸۱۷۵۵۶۰ - فکس : ۸۸۱۷۵۵۳۴