کدکارگاه	WR1507
عنوان کارگاه	**آشنایی عملی با فرآیند و مکانیزمهای همبسته سازی هشدار در سامانه OSSIM و نقاط قوت و ضعف آن**
چکیده	در جریان یک حمله توسط ابزارهای تشخیص دهنده و ناظر سطح میزبان و شبکه، هشدارهایی تولید می شوند. با جمع آوری این هشدارها در یک مرکز عملیات امنیت و اعمال الگوریتم هایی روی آنها، ابتدا هشدارها و رویدادهایی که در نتیجه یک حمله یکسان به وجود آمده اند با یکدیگر تجمیع شده و سپس سناریو حملات چندگامی که مهاجم اجرا کرده استخراج می شوند. در این زمینه پژوهش های علمی و فنی صورت گرفته که نتیجه آنها مقالات پژوهشی و ابزارهای امنیتی بوده است. آشنایی با ابزارهای امنیتی، پیاده سازی و استفاده از آنها در کنار پژوهش های علمی به فهم بهتر مطالب کمک کرده و زمینه ساز انجام پژوهش های علمی واقعی تر و خلق ایده های موثرتر می شود. در این کارگاه با معرفی مرکز عملیات امنیت و مؤلفه های آن به بررسی پژوهش های صورت گرفته در زمینه یکی از مولفه های آن یعنی همبسته سازی هشدار می پردازیم. سپس سامانه OSSIM یکی از ابزارهایی که در این زمینه توسعه داده شده است را معرفی کرده و قابلیت های آن را در زمینه تجمیع و همبسته سازی هشدار در مقایسه با تحقیقات علمی بیان کرده و طی سناریوهای عملی نحوه استفاده از این سامانه را با جزئیات تشریح می کنیم. در انتها راهکاری برای رفع چالش تجمیع هشدارهای سطح شبکه و ماشین میزبان و همبسته سازی آنها ارائه می شود.
زبان ارائه کارگاه	فارسی
زمان برگزاری	یک شنبه ۱۰ اسفند ۱۳۹۳ – ساعت ۸ الی ۱۸ – (۸ ساعت)
مخاطبان	شرکت های امنیتی، دانشجویان، کارشناسان فناوری اطلاعات سازمان ها
ارائه‌دهندگان	دانشگاه صنعتی مالک اشتر دکتر علیرضا نوروزی– مهندس مهدیه صفرزاده
پیش‌نیازهای کارگاه	شبکه های کامپیوتری ، مفاهیم پایه ای شبکه
هزینه	۱۰۰۰۰۰۰ ریال
توضیحات	گواهی‌نامه حضور در کارگاه برای شرکت‌کنندگان صادر می‌شود.

سرفصل کارگاه:

- معرفی مرکز عملیات امنیت و مؤلفه های آن و مروری بر پژوهش های صورت گرفته در زمینه همبسته سازی هشدار
- معرفی سامانه متن باز و رایگان OSSIM و بیان قابلیت های آن در مقایسه با تحقیقات علمی
- اجرای چند سناریو عملی در زمینه کاربری سامانه OSSIM و نمایش قابلیت های آن در زمینه همبسته سازی
- ارائه راهکاری برای تجمیع و همبسته سازی هشدارهای سطح شبکه و ماشین میزبان
- نتیجه گیری و بیان نقاط ضعف و قوت