Система моделирования киберугроз и ликвидации инцидентов безопасности в информационных инфраструктурах «Cyber Range»

Функциональные характеристики

Система моделирования киберугроз и ликвидации инцидентов безопасности в информационных инфраструктурах «Cyber Range» позволяет:

– проводить обучения команд Security Operation Center (SOC) и Blue Team по предотвращению, обнаружению, реагированию, расследованию и устранению последствий инцидентов;

– моделировать виртуальные IT инфраструктуры (сети) организации, белый трафик сети, сервисы и средства защиты информации;

– имитировать в автоматизированном режиме по заданным сценариям компьютерные атаки на тестируемую IT инфраструктуру;

– развертывать виртуальные рабочие места специалистов по информационной безопасности для отработки навыков обнаружения атак и реагирования на инциденты;

– анализировать безопасность моделируемой сети, не затрагивая «боевой» контур;

– подключить проприетарные решения заказчика, в том числе: WAF (Imperva, Wallarm, F5, Barracuda, Fortinet); FW (Palo Alto, Cisco, Fortinet, Checkpoint, Juniper); Antivirus (Kaspersky, McAfee, Trend Micro); IDS/IPS (Trend Micro, Cisco, McAfee); SIEM (ArcSight, QRadar).