Евгений АФОНИН
архитектор решений информационной безопасности Micro Focus

Виктор СЕРДЮК
генеральный директор АО «ДиалогНаука»

SOC НЕ РАВЕН SIEM

ОПЫТ КОМПАНИИ MICRO FOCUS В ПОСТРОЕНИИ СИТУАЦИОННЫХ ЦЕНТРОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В 2017 году исполнилось 10 лет, как первые решения Micro Focus ArcSight[1] были внедрены в российских компаниях. За эти годы более 400 компаний доверили сбор и анализ информации о событиях безопасности этой платформе.

УНИКАЛЬНЫЙ ОПЫТ

Одна из важнейших задач, стоящих перед Micro Focus и отечественными компаниями-интеграторами — перенос лучших практик зарубежного опыта. И тут простого технологического лидерства недостаточно, поскольку успех в данном случае зависит, в том числе, от зрелости и мастерства людей, которые занимаются установкой, настройкой и последующей эксплуатацией продукта Micro Focus ArcSight. За 10 лет был накоплен уникальный опыт в установке и эксплуатации продукта, его проектировании, а самое важное — понимании того, как на базе Micro Focus ArcSight построить процессы управления инцидентами информационной безопасности.

[1] 1 сентября 2017 г. компания Hewlett Packard Enterprise выделила подразделение HPE Software и объединила его с компанией Micro Focus

НЕТРИВИАЛЬНАЯ ЗАДАЧА

Сегодня одним из наиболее эффективных средств мониторинга и реагирования на инциденты ИБ является создание SOC (Security Operations Center). Общепринятого определения SOC все еще нет, но мы будем понимать под ним выделенную организационно-штатную структуру, ответственную за обработку инцидентов ИБ и располагающую необходимым техническим обеспечением. Деятельность SOC должна быть строго регламентирована внутренними нормативными документами, описывающими все этапы процесса управления инцидентами — от их регистрации до устранения их последствий и последующего расследования.

Эффективность работы SOC обеспечивается конвейерным подходом в организации работы, строгой специализацией ответственных сотрудников, автоматизацией рутинных задач и тесным взаимодействием с остальными подразделениями предприятия — как в части реагирования на инциденты, так и в части определения актуальных задач информационной безопасности. Такая организация позволяет обеспечить стабильное качество работы сотрудников по выявлению и реагированию на инциденты ИБ, четко понимать структуру инвестиционных и операционных затрат с учетом заданного уровня качества, а также иметь возможность их обоснования перед руководством организации. В качестве базовой платформы для организации SOC, как правило, выступает система мониторинга событий ИБ (SIEM), при этом необходимо понимать, что SOC не равен SIEM.

Организация эффективного SOC является нетривиальной задачей, которая к тому же находится на пересечении трех различных составляющих: кадры, технологии и регламенты взаимодействия-эксплуатации. Как поставщик платформы ArcSight, Hewlett Packard Enterprise, ныне Micro Focus, сталкивался с задачами построения SOC достаточно часто, чтобы создать в 2007 году выделенное подразделение по созданию SOC с нуля или аудиту уже существующих SOC. За время работы созданного подразделения Security Intelligence & Operations Consulting (ранее HPE SIOC, ныне Micro Focus SIOC) силами этой международной команды из 50 специалистов было создано более 50 SOC и проведено более 120 аудитов по всему миру.

САМЫЙ БОЛЬШОЙ SOC

Три года назад Micro Focus SIOC (ранее HPE SIOC) создал внутренний SOC компании Hewlett Packard, который обрабатывает события аудита, поступающие со всей ИТ-инфраструктуры, обеспечивающей повседневную работу более 300 тыс. сотрудников компании по всему миру. С целью своевременного выявления инцидентов ИБ каждую секунду в реальном времени коррелируется более 3 млрд событий ежедневно. Команда Micro Focus SOC состоит из трех смен аналитиков первичного реагирования, которые обеспечивают мониторинг выявленных инцидентов круглосуточно, отдельной команды по выполнению расследований подтвержденных инцидентов ИБ, двух инженеров Micro Focus ArcSight и, самое важное, руководителя SOC, отвечающего за вопросы контроля качества, управления персоналом, развития SOC и взаимодействия с остальными подразделениями Micro Focus.

Проектирование и создание Micro Focus SOC заняло порядка 8–10 месяцев и включало в себя создание и развертывание отказоустойчивой инфраструктуры по автоматическому сбору, хранению и корреляции событий аудита на базе платформы Micro Focus ArcSight, формулирование требований и прием персонала с привязкой к специфике номенклатуры инцидентов ИБ Micro Focus, создания необходимых правил корреляции событий, инструментальных панелей мониторинга и отчетов по показателям повседневной работы команды SOC, а также регламентов реагирования на инциденты и взаимодействия с остальными подразделениями Micro Focus. Процесс создания SOC был разделен на три этапа: защита периметра, защита внутренних приложений и защита бизнес-процессов, что позволило существенно приблизить дату начала работы в режиме реального времени.

ПРОЦЕСС СОЗДАНИЯ SOC БЫЛ РАЗДЕЛЕН НА ТРИ ЭТАПА: ЗАЩИТА ПЕРИМЕТРА, ЗАЩИТА ВНУТРЕННИХ ПРИЛОЖЕНИЙ И ЗАЩИТА БИЗНЕС-ПРОЦЕССОВ, ЧТО ПОЗВОЛИЛО СУЩЕСТВЕННО ПРИБЛИЗИТЬ ДАТУ НАЧАЛА РАБОТЫ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Из наиболее важных выводов по итогам данного проекта стоит выделить следующие: костяк группы аналитиков SOC должен обладать опытом выявления и реагирования на инциденты; необходимый опыт инженера по обслуживанию ИТ-инфраструктуры должен быть не менее двух лет; в целях снижения текучки персонала в SOC необходимо предусмотреть план развития сотрудников; при организации круглосуточного мониторинга обязательно необходимо обеспечивать передачу опыта между сменами; карта компетенций каждой функциональной группы специалистов должна быть актуализирована относительно утвержденной номенклатуры инцидентов и учитывать неизбежную ротацию специалистов SOC.

Метрики работы SOC

Идентификатор	Метрика	Текущий период			Динамика	Статус
		За день, среднее	За день, максимальное	За день, минимальное		
TM-002	Инциденты, содержащие достаточное количество исходной информации	86%	100%	75%	↑	2
	Дополнительные затраты (чч), связанные с недостатком исходной информации	8.2	9.1	0	↓	2
TM-003	Количество событий на аналитика в час	11.1	132.1	2.1	↑	1
TM-004	Инциденты с уникальным текстом описания	83%	95%	76%	—	2
TM-005	Инциденты, потребовавшие изменения уровня влияния аналитиком	17%	19%	7%	↓	3
TM-006	Ошибки 2 рода с группировкой по сценариям	11%	15%	0%	↓	3
TM-007	Уведомления с эскалацией до 2го уровня	15%	30%	10%	↓	1
	Уведомления с эскалацией до 3го уровня	7%	10%	0%	↓	2

Рисунок 1. Пример внутренних метрик работы SOC

СОГЛАСНО ОТЧЕТУ «STATE OF SECURITY OPERATIONS 2016: REPORT OF CAPABILITIES AND MATURITY OF CYBER DEFENSE ORGANIZATIONS», КОТОРЫЙ БЫЛ ОПУБЛИКОВАН HPE SIOC, СРЕДНИЙ УРОВЕНЬ ЗРЕЛОСТИ SOC ПО МИРУ НЕ ПОДНИМАЛСЯ ВЫШЕ 1.5, ПРИ МИНИМАЛЬНОМ ПОКАЗАТЕЛЕ 0.59 И МАКСИМАЛЬНОМ 3.34

Более подробную информацию о работе SOC Micro Focus можно узнать из публикаций на профильных конференциях и тематических печатных изданиях. Сам SOC территориально расположен в Пало-Альто и является хорошей площадкой для демонстрации возможностей технологий безопасности Micro Focus.

ДАЛЬНЕЙШЕЕ РАЗВИТИЕ

Дальнейшее развитие SOC на предприятии является не менее ответственной и комплексной задачей, чем его развертывание. Команда Micro Focus Security Intelligence & Operations Consulting при формировании оценки зрелости SOC и рекомендаций по его развитию использует модель CMMI с разделением на следующие уровни: Incomplete, Performed, Managed, Defined, Measured. Более того, используя статистику предыдущих аудитов, индексная оценка зрелости SOC по шкале от 0 до 5 по каждому из показателей разделов Business, People, Process, Technology может быть оценена относительно среднего наблюдаемого уровня зрелости заказчика в его вертикали — телеком, банки, ритейл и пр. Такой подход позволяет сформировать долгосрочные цели развития SOC на 2–3 года вперед и подготовить календарный план мероприятий для их достижения, как в части технологий, так и в части персонала и процессов их организовывающих.

ЧТО ПОЧИТАТЬ?

Ежегодно Micro Focus SIOC публикует на своей странице *https://software.microfocus.com/en-us/software/security-operations-center* аналитические материалы по различным актуальным проблемам построения SOC.

Наиболее интересной для отечественного рынка, на наш взгляд, может являться информация об управлении персоналом SOC, начиная от определения ролей и обязанностей, оценки уровня компетенций, подготовки плана развития сотрудников и организации сменной работы до преодоления проблем, связанных с ротацией специалистов. Полезные рекомендации, полученные из реального опыта, также можно найти в документе «Growing the Security Analyst: Hiring, training, and retention (Как вырастить аналитика по безопасности: Найм, обучение и удержание)».

Согласно отчету «State of Security Operations 2016: report of capabilities and

Описание	Отдел архитектуры и стратегического развития	Руководитель SOC	Аналитик уровня 2	Аналитик уровня 1	Аналитика угроз	Отдел сервисов SOC	Отдел сопровождения	Владелец системы	Отдел системного администрирования	Отдел реагирования на инциденты	Отдел персонала	Отдел связей с общественностью	Юридический отдел	Отдел соответствия и аудита
Обнаружение угроз с помощью мониторинга и анализа событий	C	A	R	R	R	I	C	C	R	C	C	C	C	I
Постоянный мониторинг исторических данных для выявления подозрительной активности	C	A	C	C	R	I	C	C	C	C	C	C	C	I
Предоставление отчетов для аудита	C	I	R	R		I	R	Y	R	R				A
Создание правил/отчетов SIEM	C	I	I	I	I	I	A	C	I	I	I	I	I	I

Рисунок 2. Пример матрицы распределения ответственности по модели RACI

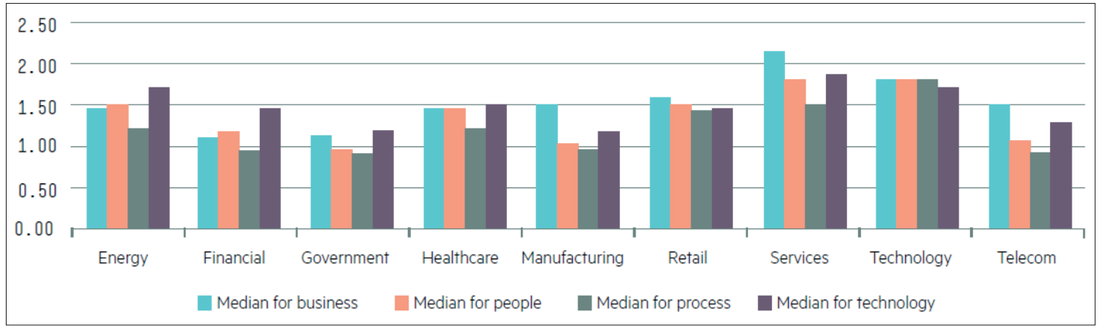

Рисунок 3. Распределение среднего уровня зрелости SOC по вертикалям за последние 5 лет

maturity of cyber defense organizations», который был опубликован Micro Focus SIOC, средний уровень зрелости SOC по миру не поднимался выше 1.5, при минимальном показателе 0.59 и максимальном 3.34. Повышение уровня зрелости SOC не должно быть самоцелью, а его границы, как правило, определяются бюджетом, согласованным в рамках бизнес-кейса, привязанного к актуальным задачам обеспечения ИБ организации. Ключевыми трендами прошлого года стали более широкое использование аутсорсинга для замещения — масштабирования аналитиков первичного реагирования, появление новой роли data scientist для работы с большими данными и поведенческими профилями, а также растущая популярность средств автоматизации реагирования на инциденты ИБ.

ПЯТЬ ОШИБОК

Интересна и статистика из прошлых отчетов Micro Focus SIOC, которая показывает, что только 25% проектов создания SOC добились выполнения поставленных целей. При этом, если привести пять наиболее часто встречающихся ошибок, то можно увидеть следующее: а) недостаток поддержки. SOC не подвешен в вакууме. Его сотрудникам приходится каждый день взаимодействовать с большинством подразделений организации. Без поддержки руководства и четко определенной цели обеспечить эффективную работу по расследованию инцидентов невозможно; б) упор на технические решения. Наиболее частой причиной проблем является перекос бюджетов в сторону внедрений технических решений, что приводит к недостаточной квалификации и количеству специалистов. Большинство современных угроз требует серьезной квалификации аналитика, а также высокого уровня организации работы по расследованию инцидентов; в) нарушение принципа «от простого к сложному». Проблемы с решением базовых задач ИБ обязательно приводят к затруднениям при решении задач более высокого уровня. Управление информационными активами, корреляция кадровой информации, категоризация информационных активов — вся эта информация является ключевой при расследовании инцидентов; г) отсутствие фокуса. Решение несвойственных, второстепенных задач оказывает существенное негативное влияние на результаты работы ситуационного центра; д) работа «ради галочки». К сожалению, решение задач по обеспечению формального соответствия требованиям регуляторов или стандартам не всегда приводит к существенному повышению уровня защищенности; е) отсутствие процессного подхода. Финансирование ситуационных центров зачастую заканчивается на этапе внедрения. Обеспечение ресурсами их повседневной работы зачастую крайне недостаточно, однако совершенно необходимо для их эффективной работы.

НЕМНОГО РЕКЛАМЫ

В заключение хотелось бы сказать, что на отечественном рынке ИБ находятся все составляющие успеха для построения эффективного SOC: 1) проверенные технологии — на российском рынке представлено много промышленных систем класса SIEM, одной из которых является Micro Focus ArcSight. Пользователями Micro Focus ArcSight в РФ являются все основные провайдеры мобильной связи, один из крупнейших телекоммуникационных операторов проводной связи, один из крупнейших поставщиков услуг по железнодорожным перевозкам в РФ, крупнейшие российские банки, а также многие другие организации, имеющие подразделения по всей территории нашей страны; 2) необходимые компетенции — за эти годы появилось множество специалистов по продуктам SIEM, которые обладают многолетним опытом работы по реагированию и расследованию инцидентов ИБ, администрированию, проектированию, внедрению и развитию данной платформы; 3) понимание процессов и задач SOC — активная работа Micro Focus Enterprise Security, отечественных интеграторов по обобщению отечественного и зарубежного опыта и организации процессов SOC, проведение регулярных тематических конференций по профилю SOC, наличие отечественных компаний, предлагающих услуги аутсорсинга по мониторингу и расследованию инцидентов ИБ.

* * *

Все перечисленное позволяет нам с уверенностью сказать, что те компании и предприятия, которые выбирают организацию собственного SOC, принимают правильное решение, позволяющее существенно повысить уровень защищенности предприятия как от внешних, так и внутренних угроз.