Съдържание

УПРАВЛЕНИЕ НА ЗАПЛАХИТЕ 7
Предизвикателства пред сигурността на инфраструктурата 7
Предизвикателства пред бизнеса 10
Защита от заплахите към инфраструктурата 14
Изисквания към виртуализацията на сигурността 16
Базирани в облака решения за сигурност 18

СИГУРНОСТ НА ВГРАДЕНИТЕ СИСТЕМИ 20
Предизвикателства пред сигурността в По-умната планета 20
По-умната планета 20
Съображения за сигурност в Умната електропреносна система 23
Инфраструктура на напредничавото замерване 28
Сигурност в По-умната планета 31
Какви са проблемите с доверието 31

МОБИЛНА СИГУРНОСТ 33
Еволюция на мобилния свят 33
Уникалност на мобилните устройства 35
Предизвикателства пред сигурността в предприятието 35
Характеристики и бизнес нужди за мобилна сигурност 36
Решения за мобилната сигурност на IBM 38
Решението за сигурност на приложенията IBM WorkLight 41
Сигурност на приложенията с AppScan 41
IBM Security Access Manager 42
Сигурна свързаност с IBM Mobile Connect 44
Сигурност на устройствата с IBM Endpoint Manager for Mobile 44
Разузнаване на мобилната сигурност с QRadar 45

ЗАЩИТА НА КРАЙНАТА ТОЧКА 47
Заплахи за крайната точка 47
Оценка на уязвимостта на крайната точка 51

СИГУРНОСТ В ОБЛАКА И КРАЙНАТА ТОЧКА 57
Болките на клиента 57
Влиянието на облака 58
Управление на сигурността и съответствието в облака 59
Управление на крайните точки от IBM 60
IBM Smart Cloud Foundation 63

РАЗУЗНАВАНЕ НА СИГУРНОСТТА 66
Терминология 66
Разузнаване на сигурността и SIEM 67

ИНДУСТРИАЛНИ СРЕДИ ... 70
Разузнаване на сигурността по примера на продуктите от IBM ... 75
Табло за подозрителните сървъри ... 76
Отчет от разузнаването на IP адресите ... 76
Корелация и портфолио ... 77
Какво е глобално разузнаване ... 78
MSS (Managed Security Services) разузнаване на сигурността ... 79
Сценарии на употреба ... 80

ВОДЕНЕ НА СИГУРНОСТТА ... 83
Обзор на водене, риск и съответствие ... 83
Реализация на GRC ... 84
Необходимостта от GRC практики ... 85
Водене на информационните технологии ... 88
Пример за структура на водене ... 96

КОМПЮТЪРНА КРИМИНАЛИСТИКА ... 105
Процес на обработка на цифровите доказателства ... 105
Видове доказателства ... 106
MITRE ATT&CK ... 107
Cyber Kill Chain ... 108
Диамантният модел ... 110
Създаване на способности за реагиране на инциденти
(отговор на инциденти) ... 114