MOORE

ІНФОРМАЦІЙНА БЕЗПЕКА

РІШЕННЯ ДЛЯ ВАШОГО БІЗНЕСУ

ЗМІСТ

ІНФОРМАЦІЙНА БЕЗПЕКА	**4**
Портфель послуг та рішень	4
ПОРТФЕЛЬ РІШЕНЬ З КОНТРОЛЮ ДОСТУПУ	5
Контроль доступу до мережі	5
Управління мобільністю підприємства	5
Багатофакторна автентифікація	5
Оновлювані бази загроз	5
ПОРТФЕЛЬ РІШЕНЬ ЩОДО ЗАХИСТУ МЕРЕЖІ І ЗАСТОСУНКІВ	**6**
Захист від мережевих атак	6
Глибокий аналіз файлів	6
Управління фаєрволами	6
Захист веб-додатків	6
Аналіз мережевого трафіку	6
Використання помилкових цілей	7
Безпечний віддалений доступ	7
Мережеві екрани наступного покоління	7
ПОРТФЕЛЬ РІШЕНЬ ЩОДО ЗАХИСТУ КІНЦЕВИХ ТОЧОК	**8**
Контроль додатків	8
Контроль пристроїв	8
Антивіруси	8
Шифрування	8
Виявлення та реагування на загрози на кінцевих точках	9
ПОРТФЕЛЬ РІШЕНЬ ЩОДО ЗАХИСТУ ДАНИХ ТА ОБЛІКОВИХ ЗАПИСІВ	**10**
Контроль привілейованих облікових записів	10
Запобігання витоку даних	10
Захист і моніторинг баз даних	11
Бекапування і відновлення дата центрів	11
Управління обліковими записами і доступом	11
Моніторинг та управління подіями безпеки	11
Управління оновленнями	11
Моніторинг підпільних джерел	11
ПОРТФЕЛЬ РІШЕНЬ З ОПТИМІЗАЦІЇ	**12**
Портфель рішень з оптимізації застосунків	12
НАША КОМАНДА	**13**
НАШІ ПАРТНЕРИ	**14**

ІНФОРМАЦІЙНА БЕЗПЕКА

Піклуємось про бізнес клієнта сьогодні та у майбутньому

Застосовуючи багатий досвід роботи з локальними та іноземними компаніями, Moore надає комплект послуг відповідно до індивідуальних потреб клієнтів.

Далі подано перелік рішень інформаційної безпеки, за якими наша компанія може надати повний спектр послуг. Пакет «впровадження під ключ» містить: підбір відповідного рішення ІБ, формування проєктної документації, впровадження і конфігурація рішення, формування внутрішньої документації, навчання персоналу та подальша локальна технічна підтримка від наших сертифікованих фахівців.

Члени нашої команди зможуть задовольнити ваші найвимогливіші потреби у сфері впровадження комплексних рішень, створення проєктної документації або інших послуг галузі інформаційної безпеки.

ПОРТФЕЛЬ ПОСЛУГ ТА РІШЕНЬ

ПОСЛУГИ ТА КОНСАЛТИНГ:

- Впровадження рішень ІБ і ІТ;
- Перша лінія технічної підтримки;
- Розробка проєктної документації;
- Навчання за авторськими і сертифікованими методиками;
- Тестування на проникнення;
- Розробка ПЗ;
- ІТ та ІБ аудит.

Наша місія – допомогти нашим клієнтам в успішному розвитку їх бізнесу, надаючи якісні та надійні рішення.

АПАРАТНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ:

Вендорське програмне забезпечення;

Вендорські апаратні рішення;

Мережеве обладнання:

- Комутатори різних типів і конфігурацій;
- Маршрутизатори різних типів і конфігурацій;
- Багатофункціональні масштабовані мережеві пристрої;
- Точки бездротового доступу;
- Бездротові мости;
- Контролери бездротових мереж.

Серверне обладнання:

- Апаратні і віртуалізовані сервери;
- Мейнфрейми.

Системи резервування та зберігання даних;

Робочі місця;

Периферійне обладнання.

ПОРТФЕЛЬ РІШЕНЬ З КОНТРОЛЮ ДОСТУПУ

Захист на передовому рубежі

КОНТРОЛЬ ДОСТУПУ ДО МЕРЕЖІ (NETWORK ACCESS CONTROL)

Функціональним завданням NAC є збір інформації про будь-які пристрої, які підключаються до мережі (ноутбук, принтер, IP-телефон, БФП...) з будь-якої точки і будь-яким способом (Ethernet, Wi-Fi, VPN ...), і в автоматичному режимі пустити / не пустити / пустити з обмеженнями даний пристрій або користувача.

Результатом впровадження такого рішення буде повна видимість Вашої мережі з контролем доступу та відповідністю регуляторним вимогам. Повна та постійна видимість мережі надає контроль над будь-якими змінами.

УПРАВЛІННЯ МОБІЛЬНІСТЮ ПІДПРИЄМСТВА (UNIFIED ENDPOINT MANAGEMENT)

Рішення цього класу являють собою єдину консоль управління мобільними пристроями організації (ноутбуки, планшети, смартфони ...). Серед функціональних можливостей цих рішень є набір технологій, процесів і політик для управління і забезпечення безпеки корпоративних і особистих мобільних пристроїв. Це здійснюється шляхом управління параметрами як самих пристроїв, так і корпоративних додатків.

Використання таких систем дозволяє вирішити проблему розмитого периметра організації та скоротити фінансові та репутаційні ризики, що пов'язані з кінцевими пристроями (особистими або корпоративними).

БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ (MULTI-FACTOR AUTHENTICATION)

Сутністю впровадження таких рішень є використання комбінації паролів і додаткових факторів. Комбінація цих даних являє собою: 1) фактор володіння (те, що в мене є): коди з смс, e-mail, мобільних додатків, USB-ключі та інше; 2) фактор властивості (те, чим я є): відбитки пальців, райдужна оболонка ока.

Сучасні рішення пропонують безліч технологій для реалізації багатофакторної автентифікації, зокрема й з використанням штучного інтелекту. Це дозволить додатково захистити Вашу організацію від зломів і крадіжок даних, а також оптимізувати процес автентифікації Ваших співробітників.

ОНОВЛЮВАНІ БАЗИ ЗАГРОЗ (THREAT INTELLIGENCE)

Рішення Threat Intelligence виконують роль кіберрозвідки, головним завданням якої є отримання і аналіз даних про актуальні загрози з метою прогнозування можливих атак і їх запобігання. Етапи проведення розвідки: збір і акумуляція даних про загрози з різних джерел в єдину систему, їх збагачення, аналіз і застосування отриманих знань.

Підвищення компетенції співробітників завдяки подібним джерелам сприяє їх ефективності, а також надає Вам захист від нових загроз.

ПОРТФЕЛЬ РІШЕНЬ ЩОДО ЗАХИСТУ МЕРЕЖІ І ЗАСТОСУНКІВ

Захист, оптимізація і аналіз наземної і/або віртуалізованої інфраструктур

ЗАХИСТ ВІД МЕРЕЖЕВИХ АТАК (DDOS PROTECTION)

Все більша кількість організацій піддається розподіленим атакам, і вони неухильно призводять до збитків. Передові рішення, які швидко і чітко визначають злоякісний трафік, надають захист від таких атак. Їх алгоритми захистять як від простих об'ємних атак, так і від комплексних та таких, що складно визначити.

Забезпечення безперервності сервісу є одним з головних пріоритетів багатьох компаній. Захист від DDoS є одним з рішень, що здатні забезпечити цілодобовий доступ до Ваших сервісів.

ГЛИБОКИЙ АНАЛІЗ ФАЙЛІВ (SANDBOX)

Цільові атаки натепер можуть ховатися в різного типу файлах, які надсилаються у вигляді поштових вкладень, або ж у файлах оновлень. Їх виявлення вимагає проведення глибокого аналізу в ізольованому середовищі. Проведення такого аналізу виконують «пісочниці», які запускають підозрілі файли всередині ізольованого оточення.

Необхідність в наявності подібних рішень викликана тим, що одне відкрите поштове вкладення неуважним співробітником або інсайдером здатне призвести до повної зупинки бізнес процесів.

УПРАВЛІННЯ ФАЄРВОЛАМИ (FIREWALL POLICY MANAGER)

Разом із зростанням інфраструктури спостерігається і нагромадження більшої кількості мережевих екранів. У конфігурації кожного з них присутні правила, які можуть конфліктувати між собою і згодом перешкоджати доступу пристроїв і додатків між собою.

Рішенням буде отримання рекомендацій з конфігурації мережевих екранів. В результаті ви отримаєте оптимізовану конфігурацію і інфраструктуру.

ЗАХИСТ ВЕБ-ДОДАТКІВ (WEB APPLICATION FIREWALL)

На відміну від класичних мережевих екранів, виконується детальний аналіз трафіку прикладного рівня. Результатом такого аналізу буде виявлення аномальних або шкідливих запитів до додатка і запобігання атак прикладного рівня. За рахунок блокування шкідливих запитів зменшується навантаження на сервера і забезпечується безпека застосунків. Перевагою таких рішень є забезпечення захищеності без необхідності зміни коду додатків.

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ (NETWORK PERFORMANCE MONITORING AND DIAGNOSTICS)

Використовуючи спеціалізовані рішення для виявлення причин деградації сервісу, команди можуть економити як час, так і кошти бюджету. У великих мережевих середовищах нерідко можна зіткнутися з різними проблемами, наприклад низька швидкість передачі трафіку між окремими вузлами мережі. Рішенням може бути виявлення вузьких місць (bottleneck), неоптимального використання мережевого каналу і аномалій трафіку. Все це виконується за допомогою аналізу статистичних даних, що одержуються через IPFIX або xFlow різних версій.

Використовуючи такі рішення, можна переглянути пріоритезацію трафіку, що передається, виявити і прискорити повільні застосунки. В результаті можна значно оптимізувати і прискорити архітектуру.

ВИКОРИСТАННЯ ПОМИЛКОВИХ ЦІЛЕЙ (DECEPTION)

Дозволяє прискорити процес виявлення присутності зловмисника в інфраструктурі до секунд / хвилин, уповільнити або повністю ізолювати атакуючого і зупинити атаку. Для цього використовуються приманки - пастки/ сенсори, які розгортаються в інфраструктурі за лічені хвилини. Зовні вразливі сутності дезінформують зловмисника і сигналізують про нелегітимну активність. Водночас відсутнє зайве навантаження на інфраструктуру і не створюються додаткові точки відмови.

БЕЗПЕЧНИЙ ВІДДАЛЕНИЙ ДОСТУП (SECURE REMOTE ACCESS)

Такі рішення допоможуть забезпечити безпечний доступ до корпоративних додатків незалежно від місця розташування користувачів. Віддаленим користувачам надається безпечне використання ресурсів через шифровані тунелі (VPN). Процес встановлення безпечного з'єднання може бути автоматизованим. Такі рішення можуть виконувати функцію єдиної точки входу (Single sign-on) і надавати детальну звітність.

У результаті віддалений доступ для співробітників стане контрольованим і безпечним. Відповідно виконання критичних робіт відбувається набагато оперативніше.

МЕРЕЖЕВІ ЕКРАНИ НАСТУПНОГО ПОКОЛІННЯ (NEXT-GENERATION FIREWALL)

Раз-у-раз виробники рішень інформаційної безпеки об'єднують функціонал декількох рішень в одному рішенні, таким чином створюючи рішення нового класу. Подібна ситуація відбулася з Firewall, IPS, Application control, які помістилися в NGFW.

Стислий перелік функцій:

- Packet filtering;
- Network address translation (NAT);
- URL blocking and virtual private networks (VPNs);
- Quality of Service (QoS);
- Intrusion prevention;
- SSL and SSH inspection;
- Deep-packet inspection;
- Reputation-based malware detection;
- Application awareness;
- Full stack visibility and granular control.

Перевагою впровадження такого рішення є можливість відмови від історичної спадщини у вигляді групи старих рішень, а також можливість оптимізації витрат на персонал і підтримку та інфраструктури.

ПОРТФЕЛЬ РІШЕНЬ ЩОДО ЗАХИСТУ КІНЦЕВИХ ТОЧОК

Захист додатків, робочих місць, серверів і реагування

КОНТРОЛЬ ДОДАТКІВ (APPLICATION CONTROL)

Для захисту та запобігання вторгнення на кінцеві точки, як-от настільні комп'ютери і сервери, окрім використання динамічних білих і чорних списків, необхідно контролювати, чи дозволені виконання різних фрагментів коду. Також перевагою буде можливість конфігурації різних ступенів контролю над тим, що додаток може робити, коли він працює, і коли він взаємодіє з системними ресурсами.

За наявності подібного рішення сумнозвісний Petia не мав би такого ефекту. До всіх застосунків (додатків), що запускаються, застосовуються попередньо налаштовані політики, і, відповідно до них, застосунок отримує встановлену ступінь свободи.

КОНТРОЛЬ ПРИСТРОЇВ (DEVICE CONTROL)

Можливість копіювати дані на носії, і подальша робота за межами компанії, дуже зручна і прискорює багато робочих процесів. Однак така зручність неухильно призводить до серйозних ризиків втрати або крадіжки даних. Оскільки зовнішні носії інформації як і раніше займають провідні позиції серед уразливих сфер в інформаційній безпеці, існує гостра необхідність захисту від витоку даних, що знаходяться на зовнішніх носіях. Для цього використовуються рішення, які застосовують політики безпеки і шифрування. Контроль за дотриманням таких політик виконується офіцерами безпеки з єдиної панелі. Система звітів дозволяє в кілька кліків визначати, наскільки ефективними є політики безпеки.

АНТИВІРУСИ (ANTIVIRUS)

Є одним з перших рішень інформаційної безпеки. Важко уявити людину, яка не стикалася з різними вендорами, що надають свої антивіруси. Спочатку працювали в режимі реактивного захисту. Характерною рисою такого захисту є виявлення відомих загроз з використанням знань про ділянки коду і інших унікальних особливостей шкідливих програм. Для коректного та ефективного захисту антивірусна програма повинна мати найсвіжіші бази вірусних сигнатур. Тоді з'явився проактивний захист - захист від невідомих вірусів, заснований на розумінні особливостей коду і поведінки, характерних для шкідливого ПЗ.

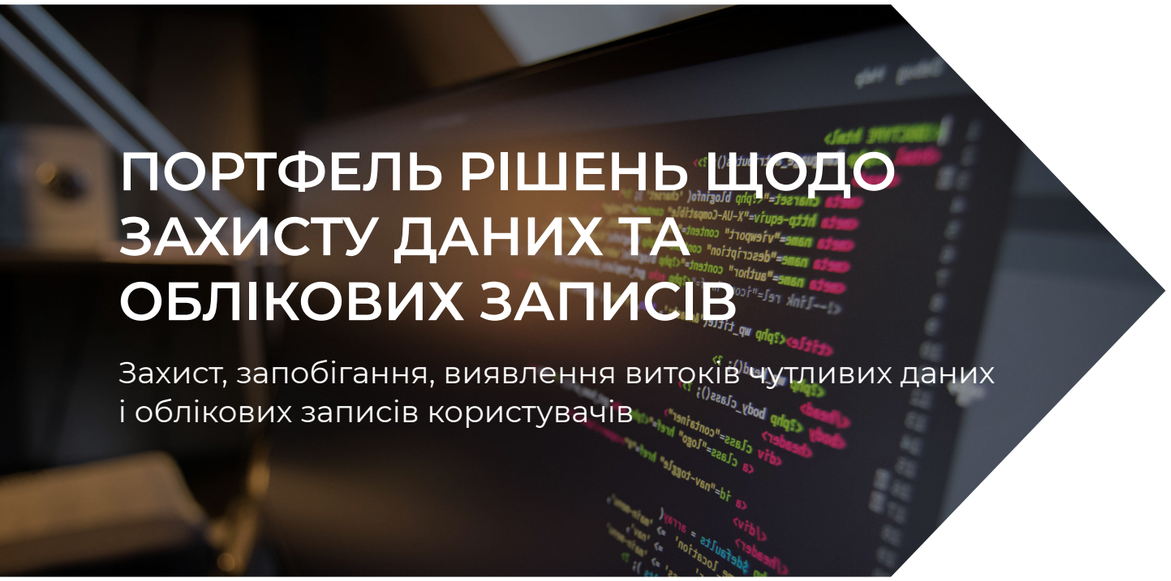
Багато антивірусів натепер є частиною або основою більш складних рішень.

ШИФРУВАННЯ (ENCRYPTION)

Ще одним програмним інструментом для запобігання витоків конфіденційних даних є шифрування носіїв інформації. Його можна виконати на планшетах, ноутбуках і настільних ПК під управлінням Windows. Це дозволить запобігти витоку конфіденційних даних, зокрема у разі втрати або крадіжки обладнання. При шифруванні диска всі дані на ньому стають незрозумілими для сторонніх осіб, що, в свою чергу, допомагає дотримуватися нормативно-правових вимог. Цей інструмент сумісний з традиційними, твердотільними і самошифрувальними накопичувачами.

ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ НА КІНЦЕВИХ ТОЧКАХ (ENDPOINT DETECTION AND RESPONSE)

Виявлення складних націлених атак є непростим завданням. Ще складніше швидко і ефективно відреагувати. Для цих цілей використовують прогресивні рішення, які, як правило, об'єднуються з центром моніторингу та реагування на інциденти інформаційної безпеки (SOC), а також являють собою клієнт-серверну архітектуру. Дані подій, що відбуваються на кінцевих точках мережі, безперервно записуються, оброблюються і аналізуються для виявлення загроз інформаційній безпеці в режимі реального часу. Можуть використовуватися хмарні платформи об'ємних даних, які включають агреговану інформацію про погрози. Такі платформи дозволяють: виявляти раніше невідомі загрози, порівнюючи інформацію про поточні та вже наявні дані робочих станцій; об'єднувати служби запобігання, виявлення, реагування, пошуку загроз інформаційній безпеці з керованими сервісами в єдину платформу, для спрощення забезпечення інформаційної безпеки організації.



ПОРТФЕЛЬ РІШЕНЬ ЩОДО ЗАХИСТУ ДАНИХ ТА ОБЛІКОВИХ ЗАПИСІВ

Захист, запобігання, виявлення витоків чутливих даних і облікових записів користувачів

КОНТРОЛЬ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ (PRIVILEGE ACCESS MANAGEMENT)

Ключі від королівства - так називають привілейовані облікові записи. Це зумовлено високими адміністративними повноваженнями. Тому здійснення моніторингу і контролю цих записів, управління їх автентифікацією і авторизацією, проведення аудиту виконуваних ними дій, контроль доступу і записи їх сесій є критично важливими завданнями перед підрозділом безпеки. Функціонал охоплює: 1) централізоване управління обліковими записами з привілеями; 2) аудит дій привілейованих співробітників; 3) управління паролями; 3) контроль доступу співробітників до адміністративних ресурсів; 4) управління процесом автентифікації і авторизації; 5) запис і контроль сесій.

Результатом впровадження PAM буде захищеність від більшої частини націлених атак і дотримання регуляторних вимог. Офіцери ІБ матимуть впевненість у дотриманні парольних політик і запобіганні небажаних дій. Співробітники ІТ отримають ефективний інструмент доступу до критичної інфраструктури.

ЗАПОБІГАННЯ ВИТОКУ ДАНИХ (DATA LEAK PREVENTION)

Мінімізувати можливість витоку даних можна завдяки наступним діям та операціям, що виконуються на регулярній основі:

- Виявлення та автоматизоване взяття під контроль конфіденційної інформації на всіх корпоративних ресурсах.
- Реалізація політик, прав і блокування операцій незалежно від місцезнаходження даних. Важливо реєструвати інциденти, переміщати в карантин підозрілі події і оперативно повідомляти про зафіксовані інциденти.
- Подальше корегування і створення нових політик безпеки. Подальше керування рішенням на основі нових і змінених документів. Загальний аналіз ситуації і автоматизована підготовка звітності щодо зниження ризиків.

Завдяки впровадженню та правильному налаштуванню таких рішень самі користувачі будуть захищені від передачі чутливої інформації зловмисникам.

ЗАХИСТ І МОНІТОРИНГ БАЗ ДАНИХ (DATABASE ACTIVITY MONITORING)

Для оптимізації та захисту баз даних необхідно проводити моніторинг активності баз даних незалежно від типу і виробника рішення, що використовується в інфраструктурі. Моніторинг привілейованих користувачів дозволяє відстежувати всі дії, що виконуються в базі даних, і виявляти нетипові і аномальні дії. Доповнюється це моніторингом активності програмного забезпечення, в той час як додатки працюють з базами даних. В результаті виявляються співробітники, які виконують нелегітимні дії безпосередньо або використовуючи додатки. Завдяки виконанню аналізу, такі рішення захищають від атак, націлених на бази даних.

БЕКАПУВАННЯ І ВІДНОВЛЕННЯ ДАТА ЦЕНТРІВ (DATA CENTER BACKUP AND RECOVERY SOLUTIONS)

У джентельменський набір будь-якої організації обов'язково входить рішення для бекапування. Корпоративні рішення для бекапування об'єднують в собі захист віртуального і фізичного середовища, спрощують резервне копіювання, а також мають можливість створювати моментальні копії віртуальних машин завдяки інтеграції з такими технологіями, як Volume Shadow Copy Service і VMware vStorage API for Data Protection. Все це дозволяє скоротити використання ресурсів процесора, пам'яті і введення-виведення на віртуальних хостах. Завдяки своїй спеціалізації дані рішення можуть виконувати резервне копіювання на диски, магнітні стрічки і в хмару.

УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ І ДОСТУПОМ (IDENTITY AND ACCESS MANAGEMENT)

Для забезпечення належного рівня захищеності організації потрібно отримати повноцінну і актуальну картину щодо облікових записів, присутніх в інфраструктурі. Досягти цього можливо завдяки проведенню регулярного аудиту облікових записів, збору даних про облікові дані, що використовуються та не використовуються, їх привілеї, доступ і управління ними. Важливим аспектом оптимізації роботи і виключення людського фактора є автоматизація процесів залучення нового співробітника в організацію, залишення ним посади або переміщення на іншу посаду. IAM здатний полегшити життя як фахівцям з безпеки, так і співробітникам інших підрозділів.

МОНІТОРИНГ ТА УПРАВЛІННЯ ПОДІЯМИ БЕЗПЕКИ (SECURITY INFORMATION AND EVENT MANAGEMENT)

SIEM потрібна для отримання і аналізу інформації. Отримувати цю інформацію можна з різних джерел, як-от з DLP-системи, IDS, маршрутизаторів, міжмережевих екранів, серверів тощо. Мотивацією для покупки такого рішення може стати колосальна кількість об'єктів, за подіями яких необхідно стежити. Не є поодинокими ситуації, коли зовні нешкідливі події, при проведенні кореляції, несуть в собі загрозу. Припустімо, відбувається відправка листа з чутливими для компанії даними людиною, що має на це право, але на адресу, що знаходиться поза стандартного кола його адресатів. DLP система цього може не відловити, але SIEM, використовуючи статистику, вже згенерує інцидент.

УПРАВЛІННЯ ОНОВЛЕННЯМИ (PATCH MANAGEMENT)

За наявності великої кількості нормативних вимог і сторонніх додатків, схильних до вразливостей, необхідне комплексне управління патчами і оновленнями. Будь-які зміни в конфігурації можуть порушити логіку налаштованих процесів. Для запобігання таких ситуацій необхідно протестувати оновлення і патчі. Не варто випускати з уваги можливості з автоматизації, які знизять час простою і навантаження на інфраструктуру. Деякі рішення дозволяють швидко виявляти уразливості в Windows, Mac OS, Linux і сотнях сторонніх додатків (Acrobat Flash / Reader, Java, веб-браузери тощо), а також централізовано розгортати попередньо перевірені патчі.

МОНІТОРИНГ ПІДПІЛЬНИХ ДЖЕРЕЛ (DARK WEB MONITORING)

Рішення цього класу індексують веб-сторінки самого дарквеба, Telegram-канали, кримінальні форуми, маркетплейси і інші джерела. Таким чином, попереджаються ризики, пов'язані з небажаними витоками даних, і організація отримує можливість захиститися від зовнішніх загроз. Головними перевагами таких рішень є автоматизація і можливість виявляти саме ту необхідну інформацію з усього розмаїття і шуму, яка зберігається на сторінках даркнета. Використання таких рішень відкриває можливості для відстеження витоків облікових даних користувачів, конфіденційної інформації у вигляді документів, технічних даних, інтелектуальної власності або ж даних Ваших клієнтів.

ПОРТФЕЛЬ РІШЕНЬ З ОПТИМІЗАЦІЇ

Результатом синергії, що полягає в обміні досвіду з передовими виробниками, є можливість надання якісного сервісу та забезпечення найвищих вимог клієнта.

ПОРТФЕЛЬ РІШЕНЬ З ОПТИМІЗАЦІЇ ЗАСТОСУНКІВ (APPLICATION PERFORMACE MANAGEMENT)

Рішеннями з оптимізації роботи застосунків є інтелектуальні платформи, що швидко окупаються. Завдяки своїй універсальності застосовуються також для застосунків із сучасними архітектурами. Принцип роботи полягає в перехопленні контекстуальних даних рівня програмного коду з прив'язкою за часом для всіх транзакцій – end-to-end. Паралельно виконується моніторинг, з моменту кліка користувача, формування запиту в базі даних, його доставки і у зворотному напрямку через всі компоненти архітектури. Завдяки повній та глибокій деталізації 100% транзакцій та інфраструктури забезпечується високошвидкісне виявлення першопричин проблем. Спеціалізацією є забезпечення необхідного рівня видимості, потрібний контекст та здатність до адаптації – все те, що потрібно для проактивного усунення проблем з продуктивністю роботи застосунків і проблем, які впливають на досвід користувача.

НАША КОМАНДА

Завдяки знанням і багатому досвіду, що були набуті в процесі співпраці з локальними та іноземними компаніями, наша команда гарантує експертний підхід до вирішення завдань клієнта.

ЯКОВЛЕВ ОЛЕКСІЙ, КЕРІВНИК ВІДДІЛУ ІННОВАЦІЙНИХ ПРОЄКТІВ

Олексій Яковлев є Керівником відділу інноваційних проєктів. Олексій має багатий досвід надання IT послуг як приватним клієнтам, так і державному сектору. Відповідає за впровадження комп'ютерних методів аудиту (CAAT) та IT-програм, що оптимізують процеси ведення бізнесу та аудиту. Впродовж останніх років Олексій працює в сфері блокчейну та займається дослідженням правових та фінансових питань, пов'язаних з прийняттям цієї технології на урядовому та корпоративному рівнях.

НАСОНОВ ВІТАЛІЙ, КЕРІВНИК ДЕПАРТАМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Віталій Насонов – досвідчений фахівець, що працює в сфері інформаційної безпеки. Пройшов шлях від аналітика та інженера рішень інформаційної безпеки до керівника департаменту. Має досвід реалізації комплексних проєктів з впровадження рішень інформаційної безпеки у великих комерційних і державних організаціях.

НАШІ ПАРТНЕРИ

Symantec
ixia
TREND MICRO
Chainalysis
OneSpan Be bold. Be secure.
JoeSecurity
TRAPX SECURITY
RISKIQ
FORCEPOINT
algosec
f5
VERITAS
IBM
portnox
hp
SailPoint
CITRIX
FARSIGHT SECURITY
paloalto NETWORKS
tufin
Carbon Black.
DELL
VARONIS
Flowmon Driving Network Visibility
RSA
gemalto a Thales company
ARBOR NETWORKS
SKYBOX SECURITY
ivanti
SOPHOS
dynatrace
imperva
digital shadows_
Check Point SOFTWARE TECHNOLOGIES LTD.
splunk>
GTB Technologies Data Security that Works
CYBERARK
CISCO
HYAS
DOMAINTOOLS
CLOUDFLARE

ІЗ ВДЯЧНІСТЮ ЗА СПІВПРАЦЮ!

Наші контакти:
T: +380 63 170 8884
T: +380 44 206 1030
E: info@moore.ua
вул. Вадима Гетьмана, 8/26, ТРЦ «Космополіт», 10-ий поверх, м. Київ, 03057

MOORE

www.moore.ua