Ваша IT-інфраструктура під наглядом ШІ

Неможливо керувати тим, чого не бачиш.

Для того, щоб щось контролювати, треба бачити предмет контролю. Тільки коли знаєш усе, що відбувається в системі, можна ефективно впливати на її внутрішні процеси, тоді як неповна картина навпаки обмежує контроль та управління. Це стосується будь-яких систем, а особливо — комплексних, таких як сучасна корпоративна IT-інфраструктура. І це є першоджерелом основної проблеми сучасних IT-керівників: контролювати IT-інфраструктури з кожним роком стає дедалі складніше через їх постійний всебічний розвиток.

Чудовим прикладом є поточні тенденції SDx (програмно визначене «все»), які перетворюють доти статичні інфраструктури на динамічні — залежні від поточної ситуації, мінливих потреб застосунків і процесів. Окрім корпоративних мереж усіх рівнів (SD-WAN для глобальної мережі, SD-Access — для кампусної/локальної мережі, SDN — для ЦОД), ці тенденції також стосуються архітектури датацентрів. Є різні типи класичної трирівневої моделі з мережею зберігання даних: архітектура з Fibre Channel (FC), пакетними SAN-мережами (iSCSI) та мережами NVMe-oF; з класичною СЗД та з програмно-визначеною СЗД, а також на основі гіперконвергентної інфраструктури (HCI). Вони змінюють одна одну в IT-інфраструктурі або існують одночасно, додаючи гнучкості та ефективності. Але все це вимагає високого ступеня керованості, а отже, і тотальної видимості процесів.

Складна інфраструктура, необхідність динамічного управління нею та безліч рівнів вже не дозволяють говорити про наскрізну видимість та управління IT за допомогою лише базових інструментів: ping, telnet/SSH, SNMP trap тощо. Потрібні потужні засоби збору, кореляції та аналізу подій, адже з урахуванням сучасних рівнів складності IT ми ніколи не можемо стверджувати, що першопричина аварії знаходиться в тій системі та в сегменті, де її помічено. Тому нам необхідна вся фактична, історична та аналітична інформація, яка створить достатню прозорість для своєчасного виявлення проблеми, а також для оперативного та якісного аналізу інциденту, визначення кореневої причини проблеми та успішного відновлення системи.

«Джерело» обізнаності

На основі 33-річного досвіду роботи із складними корпоративними та операторськими IT-інфраструктурами компанія «ЕС ЕН ТІ УКРАЇНА» створила концепцію ефективної системи моніторингу IT на основі комплексу засобів, що надають розвинуту телеметрію, статистику та глибоку аналітику щодо інциденту або аварії. Комплекс отримав назву «Джерело».

Повне бачення ситуації вимагає збору журналів подій (логи) та параметрів стану з максимальної кількості пристроїв і систем. Це уможливлюють системи моніторингу з доступом до всіх суттєвих систем за різними протоколами: вони отримують логи та метрики, обробляють та нормалізують їх для аналізу. Повний аналіз включає дані, отримані по SNMP-каналу (поточний статус на основі метрик) та дані у форматі syslog (події). Інформація про один і той самий факт або подію може надходити по кількох каналах (SNMP, syslog, API...) (**рис. 1**), а тому потребує попередньої обробки та очищення перед потраплянням до бази та аналізу.

Крім інформації про подію або стан цільових систем, необхідно розуміти процеси у мережі: як та який трафік передається, з якою швидкістю, куди і звідки тощо. Зазвичай таку інформацію отримують через відомі потокові протоколи сімейства NetFlow. Вони надають інформацію про конкретну сесію мережевого пристрою з інформацією третього та четвертого рівня моделі OSI, що уможливлює базовий аналіз трафіку та поведінки мережі. Повне розуміння інформації про те, що передається, вимагає глибокої інспекції пакетів (DPI) — аж до рівня застосунків. Але в сучасних мережах досить велика кількість застосунків шифрують трафік між хостами, і найчастіше відкритий доступ є лише до заголовку — інформації, доступній по NetFlow. Тому DPI не

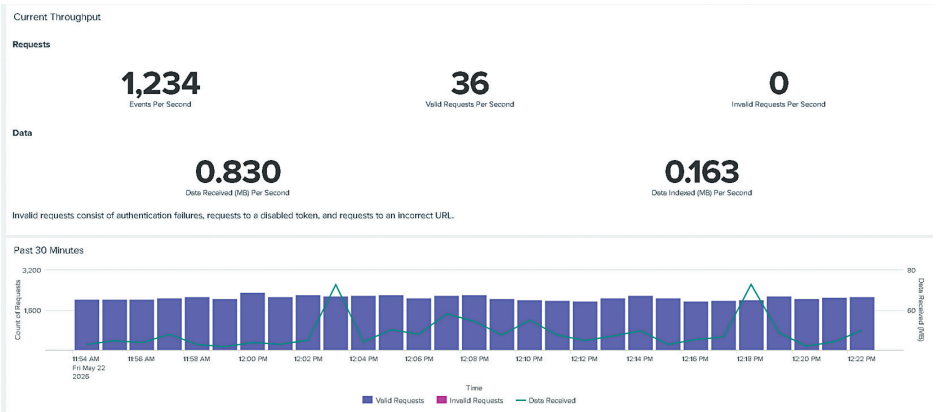

Рис. 1. Приклад дашборда системи моніторингу WEB-порталу

завжди застосовується в корпоративних системах моніторингу.

Використання даних NetFlow від ключових та важливих вузлів корпоративної мережі вимагає організації в системі моніторингу не лише syslog-сервера та аналізатора, а й інфраструктури NetFlow-колекторів та аналізатора, які також є елементами системи моніторингу.

Задля вирішення цих проблем ми реалізували комплексну інтеграцію рішень для моніторингу IT-інфраструктури. Вона ґрунтується на аналітичній системі Splunk Enterprise, що збирає та аналізує syslog-повідомлення від найрізноманітніших систем, запитує метрики по SNMP, отримує сповіщення за допомогою SNMP trap. Splunk також може отримувати інформацію по протоколу NetFlow через стандартний модуль. Всі ці дані потрапляють на стандартний сервіс Edge Processor для попередньої обробки та фільтрації даних. Система аналітики займається кореляцією подій та логів, визначенням аномалій, аварій та інцидентів. Результати обробки, кореляції й аналізу, а також тренди можуть бути представлені через дашборди стандартного модуля Splunk Enterprise або в модулі Splunk ITSI, на базі якого ми будуємо аналітичні системи для бізнесу та IT-керівників. Це надбудова над аналітичною платформою для аналізу і представлення впливу параметрів, подій та трендів в IT-системах на відповідні бізнес-процеси та бізнес-застосунки, а також розуміння зворотних зв'язків та впливів (**рис. 2**).

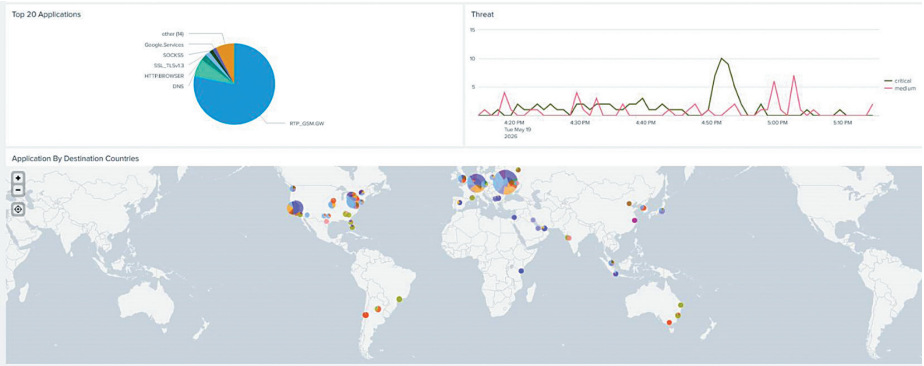

Рис. 2. Наскрізна видимість потрібна як глобальним корпораціям, так і локальним підприємствам

Моніторинг процесів і виявлення першопричин

Згадаймо також про особливий клас взаємодоповнюючих аналітичних систем — Application Performance Monitoring (APM) та Network Performance Monitoring (NPM), які детально вивчають процеси в застосунках та параметри проходження пакетів у мережевій інфраструктурі.

APM аналізує затримки в застосунках та базах даних, проблеми або неефективності в роботі апаратного забезпечення серверів та СЗД, користувацький досвід у конкретній системі, помилки в ПЗ та БД тощо. NPM аналізує затримки в мережі посегментно та по кожному потоку, втрати пакетів та помилки передачі по ділянці, проводить глибокий аналіз пакетів та аналізує утилізацію каналу по кожній сесії.

Це потужні системи аналізу для підвищення ефективності та оптимізації процесів в IT. У нашому комплексі «Джерело» вони виступають і як незалежні інструменти для аналітиків, і як джерела інформації для Splunk, що збагачують події, забезпечуючи більш ефективний пошук причин проблеми та її усунення. З урахуванням різних ландшафтів IT та вподобань IT-команди замовника є кілька варіантів систем APM (AppDynamics, Dynatrace) та NPM (Riverbed, Solarwinds, ...) для інтеграції зі Splunk. Можлива інтеграція лише APM або NPM, або навіть робота без них. Зазначимо, що обмеження або відмова від використання аналітичних систем — це компроміс, який позначиться на повноті інформації для аналізу та ефективності визначення причин проблеми. Будь-яке нове джерело додає дані зі своєю ефективністю та вагою, тобто створює нову площину вивчення IT-системи. Це як ще один вимір n-вимірного простору ознак, який дозволяє аналітичним алгоритмам різко збільшити ефективність пошуку аномалії в досліджуваній системі.

Всі отримані дані будуть використані під час дослідження причин виникнення проблеми (Root Cause Analysis або RCA) на основі діаграми Ісікави для аналізу всіх подій та виділення або синтезування вихідної події — причини проблем. Аналітичне завдання вирішується як запрограмований алгоритм або як завдання для систем ШІ. Це залежить від реалізації відповідної функції системи моніторингу або окремої аналітичної системи, яка працює в парі з нею. Для пошуку першопричини аварії в даній системі моніторингу використовується або модуль ШІ Splunk Enterprise, або кореляційне ядро, розроблене «ЕС ЕН ТІ УКРАЇНА» — модуль CRL.

Основні завдання системи моніторингу IT-інфраструктури:

- виявити проблему;
- з'ясувати її кореневу причину;
- розробити спосіб усунення та реалізувати його (за дозволом та під контролем інженера).

Кіберзахист

Згадані вище дані можуть бути використані й іншими аналітичними системами: зі схожими вихідними даними та алгоритмами аналізу, але в іншому контексті та зі своєю специфікою (**рис. 3**).

Гарним прикладом є кібербезпека. Кіберзагрози — зворотний бік тотальної цифровізації. Згідно з Cybercrime Magazine, витік або втрата даних в результаті кібератаки в 60% випадків призводять до закриття СМБ протягом півроку. Оскільки ця стаття — про повну видимість процесів та подій для розуміння стану системи, то для повноти картини необхідно зазначити, що навіть без зламу до 30% компаній малого бізнесу закриваються в перший рік свого існування, тому залежність кількості банкрутств від зламу насправді

не виглядає настільки катастрофічною☺. Втім, реальність та суттєві решта 30% все ж свідчать про те, що кібербезпека критично важлива для існування бізнесу. Ця статистика наочно демонструє основну думку статті: лише повна видимість усіх даних дозволяє виконати коректний аналіз.

Кіберзахист — це, здебільшого, системи захисту мережевої інфраструктури, кінцевих точок, IT-систем, а також рішення з аналітики, які працюють з даними як від IT-систем, так і від систем кіберзахисту. Принципи роботи кіберзахисту подібні до розглянутих вище: збір та аналіз даних IT-систем та систем кібербезпеки дозволяють вирішити перелічені вище завдання — просто цього разу у контексті захисту IT-інфраструктури від атак. Аналітичні моделі різні, а алгоритми й вихідні дані практично однакові. Це вихідна концепція Splunk, що надає аналітичне ядро та модулі ШІ для вирішення комплексу завдань. Моніторинг та аналіз причин збоїв у IT-інфраструктурі реалізуються з використанням модуля ITSI, аналіз та виявлення кіберінцидентів — за допомогою Splunk Enterprise Security. Ця синергія дозволяє використовувати схожий набір даних та єдину платформу для вирішення завдань, критично важливих для IT-інфраструктури, розподіляючи, за необхідності, вихідні дані та результати між вищезгаданими та іншими аналітичними завданнями, такими як аналіз IoT або інженерної інфраструктури.

Досвід впровадження

Чудовим прикладом реалізації цієї концепції став проєкт побудови системи комплексного моніторингу для організації, яка розгорнула потужну IT-інфраструктуру на території двох основних фізичних сайтів. Замовник працює з великою кількістю прикладного ПЗ та суттєвими обсягами даних і постійно прагне підвищити прозорість інфраструктури. Спочатку моніторинг всієї його інфраструктури забезпечувало глибоко кастомізоване рішення Zabbix. Крім того, у нього розгорталося APM — рішення від одного з лідерів ринку, але не з рекомендованого нами переліку, і

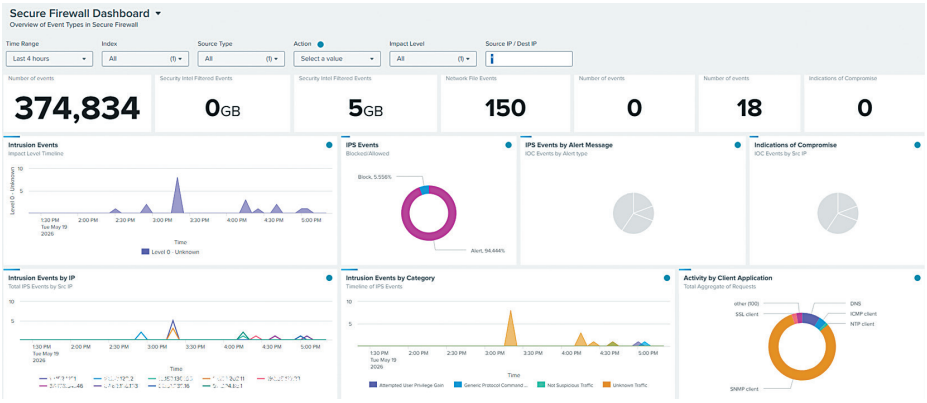

Рис. 3. Аналітика кібербезпеки як невід'ємна частина системи моніторингу IT-інфраструктури

цього виявилось недостатньо. Жорсткі вимоги до безперебійності роботи IT-сервісів та спеціалізованого ПЗ призвели до створення потужної служби моніторингу та аналізу подій в інфраструктурі — фактично створено справжній Network Operations Center (NOC).

На основі аналізу систем та обсягу телеметрії NOC було розроблено проєкт, що визначив: які IT-системи підключаються, за яким протоколом, які дані отримуються, на які системи встановлюються агенти, який обсяг телеметрії зберігається, де і протягом якого часу, які апаратні ресурси потрібні для розгортання систем, з якими аналітичними системами об'єднуємось, як здійснюється взаємодія з Service Desk тощо...

В результаті було впроваджено рішення Splunk Enterprise: розгорнуто ядро, встановлено декілька Edge Processors (по два на сайт) для попередньої обробки вхідних даних телеметрії та більш ефективного використання ліцензій. Викликом стала інтеграція з існуючим APM для отримання та обробки системою моніторингу й аналізу інформації про процеси в численних застосунках. Замовник вирішив не розгортати NPM, тому ми «здобули» всю можливу інформацію із вже розгорнутого рішення класу NTA/NDR (Network Traffic Analyzer / Network Detection & Response). Звичайно, ефективність даних, які збирає NTA, не зрівняється з обсягом даних, які надає NPM, але така інтеграція все одно надає більше інформації для аналізу, ніж за відсутності мережевої аналітики взагалі.

З цим нестандартним набором компонентів нам вдалося досягти головної мети: знизити час реагування на IT-інциденти і зменшити їх кількість. За рахунок впровадження аналітики, використання правил кореляції та компонентів ШІ вдалося прискорити розслідування інцидентів на ~35% (оцінка замовника). За рахунок використання динамічних адаптивних еталонних рівнів, які керуються самонавчальним ШІ, та предиктивного аналізу вдалося запобігти появі великої кількості інцидентів — за оцінкою замовника, кількість аварій зменшилася на ~30%. Побічним результатом проєкту, а точніше інтеграції з системою мережевої аналітики кібербезпеки NTA, стала ідея збагачення подій безпеки на основі роботи системи моніторингу. У подальшому передбачається використання модулів безпеки Splunk для розгортання повноцінної аналітики кібербезпеки на існуючому аналітичному базисі та забезпечення відмовостійкості рішення.

SNT
Systems. Networks. Technologies

Сергій БОБРОВ,
технічний директор,
компанія SNT Ukraine
+380 (44) 238–63–88
info@snt.ua, www.snt.ua