ST&T

GUARDIAN OF THE MATRIX

ГАЙД FREE

SecOps:
ПОКРОКОВА ІНСТРУКЦІЯ
ПРОСТИМИ СЛОВАМИ

ЩО ДАЄ СПЕЦІАЛІСТУ

- **Розширення знань:** як працює SecOps від огляду до повноцінного контролю.
- **Прокачування навичок:** MFA, PAM, ZTNA, UEBA, DLP, мікросегментація.
- **Закриття банальних дірок:** швидкі перемоги і стабілізація роботи.
- **Підготовка до складних сценаріїв:** реагування на інсайдерів і зовнішні атаки.

ЯК КОРИСТУВАТИСЯ

Зробіть **15-хвилинний огляд**

↓

Виконайте **швидкі дії за 24 години**

↓

Проведіть **стабілізацію за 7 днів**

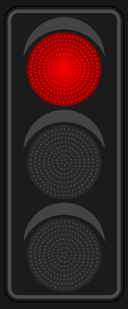
↓

Далі — **план на 30/60/90 днів**

↓

Тримайте **показники ефективності** та **регулярні тренування.**

15-ХВИЛИННИЙ ОГЛЯД «СВІТЛОФОР»



Багатофакторна автентифікація (MFA) не ввімкнена всюди: пошта, віддалений доступ, адмін-панелі, провайдер ідентичності (IdP/єдиний вхід).

Захист кінцевих пристроїв (EDR) покриває < 95% активних комп'ютерів/серверів.

Журнали подій (IdP, пошта, DNS, міжмережевий екран, EDR, хмара) не надходять у систему збору/аналізу (SIEM/XDR).

«Ось це треба виправити негайно»

Адміністративні облікові записи без керування привілеями (PAM), без «доступів за потреби» (JIT).

Мережа без сегментації: немає обмежень для внутрішнього трафіку.

Відсутній централізований моніторинг подій

«Небезпечно відкладати, треба в роботу»

Діє білий список застосунків, інше блокується.

Комплексна парольна політика та складна автентифікація.

Шифрування робочих станцій і мережевого трафіку.

Повна видимість дій користувачів та трафіку.

«Все добре, але це лише база — йдемо далі»

«Якщо бачите хоча б один червоний або жовтий сигнал — це критичний маркер. Не відкладайте, дійте одразу.

Якщо все у зеленій зоні — вітаю, ви можете рухатись далі й переходити до покращення процесів за чеклістом».

24 ГОДИНИ: ШВИДКІ ПЕРЕМОГИ

- **Увімкнути MFA «за замовчуванням»** для IdP/SSO, пошти, віддаленого доступу, адмін-панелей, критичних хмарних сервісів.
- **Обмеження внутрішнього трафіку:** тимчасово заборонити зайві протоколи між сегментами (SNMP v1/ SMB тощо).
- **Під'єднати ключові журнали** до SIEM/XDR: IdP, EDR, пошта, DNS, проксі/брандмауер, аудити хмари.
- **Автоматизація реагування** (SOAR «із коробки»): ізоляція зараженого комп'ютера, карантин підозрілих листів, примусовий вихід із сесій.
- **Гігієна паролів:** вимкнути застарілу автентифікацію (POP/IMAP/Basic), заборонити слабкі паролі; для адмінів — по можливості вхід без пароля (апаратні ключі/FIDO2 чи додаток-підтверджувач).

«Ці дії — ваші швидкі перемоги. Якщо їх зробити протягом доби, ви одразу знизите ризик більшості типових атак: фішинг, інфостілери, компрометація паролів. Це фундамент, без якого рухатися далі немає сенсу».

7 ДНІВ: БАЗОВА СТАБІЛІЗАЦІЯ

- **EDR покриття ⩾ 98%:** інвентаризація, довстановлення, контроль «сірих» пристроїв.
- **Контроль запуску програм** на критичних серверах/робочих місцях (лише дозволені).
- **Мікросегментація v1:** виділіть 2–3 критичні ресурси (CRM/ERP/прод-БД) у окремі зони.
- **Поведінкова аналітика** (UEBA): нетипові логіни (країна/час), незвичні доступи до даних, різкий ріст трафіку.
- **Менше «зайвих сповіщень»:** вимкнути шумні правила, додати винятки з поясненням.
- **Внутрішні загрози:** тригери — масові копії/архівів, підвищення прав, незвичні експортні операції.

«Тиждень — це ваш час на те, щоб прибрати хаос і закрити основні «дірки». Ви переходите від пожежного гасіння до контрольованої безпеки. Це дає стабільність, на якій можна будувати складніші процеси».

ДОРОЖНЯ КАРТА 30/60/90 ДНІВ

30 ДНІВ

- **Доступ з нульовою довірою** до мережі (ZTNA) замість «суцільного» VPN.
- **Керування привілеями** (PAM): підвищені права — лише «за запитом», із записом сесій.
- **Захист пошти та вебу:** SPF/DKIM/DMARC у режимі «відхилити», перепис посилань, блок шкідливих вкладень.
- **Автоматичні сценарії реагування v1** (див. нижче).
- **Перші показники:** час виявлення/реакції (MTTA/MTTR), частка MFA та EDR, кількість заблокованих горизонтальних переміщень.

60 ДНІВ

- **Мікросегментація v2:** суворі правила «заборона за замовчуванням» між зонами, дозволяти лише потрібні порти/сервіси.
- **Безпарольний доступ для привілейованих користувачів** (адміни/фінанси/доступ до даних).
- **Захист даних:** класифікація, політики запобігання витокам (DLP) для пошти/веб/хмар.
- **Хмарна безпека:** контроль базових налаштувань, шифрування, перевірка інфраструктури як коду (IaC), пошук секретів у CI/CD.

90 ДНІВ

- **Полювання на загрози:** щотижневі гіпотези, журнал знахідок і виправлень.
- **Навчальні сценарії «настільного» формату** (purple-team/tabletop): 1–2 на місяць — від фішингу до спроби витоку.
- **Оновлені показники:** час перебування зловмисника в мережі (dwell time), час локалізації, частка адмін-дій під PAM, частка сегментованих сервісів, зниження «шуму».

«Цей план дозволяє розтягнути зміни без перевантаження команди. Через 90 днів ви отримаєте систему, яка вже працює як єдиний організм: сегментація, контроль привілеїв, безпарольний доступ і навчена команда».

ПРІОРИТЕТИ ДЛЯ ЖУРНАЛІВ ПОДІЙ
(що під'єднати спочатку)

- **Увімкнути MFA «за замовчуванням»** для IdP/SSO, пошти, віддаленого доступу, адмін-панелей, критичних хмарних сервісів.
- **Обмеження внутрішнього трафіку:** тимчасово заборонити зайві протоколи між сегментами (RDP/SMB тощо).
- **Під'єднати ключові журнали** до SIEM/XDR: IdP, EDR, пошта, DNS, проксі/брандмауер, аудити хмари.
- **Автоматизація реагування** (SOAR «із коробки»): ізоляція зараженого комп'ютера, карантин підозрілих листів, примусовий вихід із сесій.
- **Гігієна паролів:** вимкнути застарілу автентифікацію (POP/IMAP/Basic), заборонити слабкі паролі; для адмінів — по можливості вхід без пароля (апаратні ключі/FIDO2 чи додаток-підтверджувач).

«Без журналів ви «сліпі». Правильний порядок підключення гарантує, що ви одразу бачите критичні події, а не тонете у сміттєвих логах».

АВТОСЦЕНАРІЇ РЕАГУВАННЯ
(стартовий набір)

- **EDR покриття ⩾ 98%:** інвентаризація, довстановлення, контроль «сірих» пристроїв.
- **Контроль запуску програм** на критичних серверах/робочих місцях (лише дозволені).
- **Мікросегментація v1:** виділіть 2–3 критичні ресурси (CRM/ERP/прод-БД) у окремі зони.
- **Поведінкова аналітика** (UEBA): нетипові логіни (країна/час), незвичні доступи до даних, різкий ріст трафіку.
- **Менше «зайвих сповіщень»:** вимкнути шумні правила, додати винятки з поясненням.
- **Внутрішні загрози:** тригери — масові копії/архівів, підвищення прав, незвичні експортні операції.

«Швидкість реакції рятує бізнес. Автосценарії знімають залежність від ручних дій — реагування відбувається навіть тоді, коли ваша команда спить».

ПОВЕДІНКОВА АНАЛІТИКА (UEBA)
(короткий чек)

- **Які дані:** IdP/SSO, ZTNA/VPN, EDR, файлові події, журнали хмар/ корпоративних сервісів.
- **Базова поведінка:** 2–4 тижні на побудову «нормальних» профілів.
- **Ключові політики:** неможливі переміщення, нетиповий час, незвичні ресурси, підозрілі обсяги даних.
- **Автоматизація реагування** (SOAR «із коробки»): ізоляція зараженого комп'ютера, карантин підозрілих листів, примусовий вихід із сесій.
- **Менше хибних спрацювань:** «фальшиві» обліковки, білі списки сервісних обліковок, під час планових робіт.
- **Конфіденційність:** збираємо мінімум персональних даних, фіксуємо доступи до самих журналів.

«Аналітика поведінки ловить те, що пропускають класичні інструменти: інсайдерів, крадіжку сесій, «неможливі подорожі». Це ваш радар на нетипові дії».

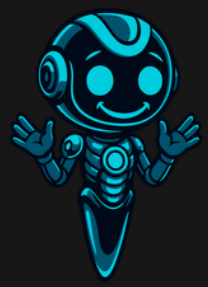
МІКРОСЕГМЕНТАЦІЯ
(практичний підхід)

- **Облік активів → класифікація даних → зони довіри.**
- **Міжзонні правила:** «заборонити все, дозволити необхідне» (L4/L7), журналювати винятки.
- **Доступ до застосунків:** віддавати перевагу ZTNA (доступ до конкретного сервісу), а не «труба в мережу».
- **Ідентичність сервісів/машин:** керування секретами, ротація ключів, уніфіковані ролі.
- **Перевірка:** імітація прориву — атака не має виходити за межі сегмента.

«Мікросегментація — це протипожежні перегородки. Навіть якщо хакер проник усередину, він не зможе «гуляти» по всій мережі. Ви виграєте час для виявлення і блокування атаки».

ВХІД БЕЗ ПАРОЛЯ ТА MFA
(без болю)

- **Карта систем:** де ще живе застаріла автентифікація.
- **Стратегія:** апаратні ключі/додаток-підтверджувач для адмінів; MFA для всіх.
- **Резерв:** аварійні облікові записи з чіткою процедурою доступу.
- **Досвід користувачів:** короткі інструкції, тестування → поступове розгортання.



«Паролі — головний біль. Ключі й MFA знижують ризики крадіжки доступів, а також роблять життя користувачів простішим».

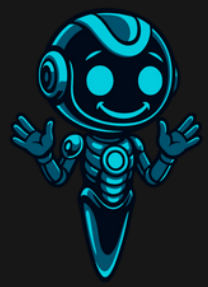
ВНУТРІШНІ ЗАГРОЗИ ТА ПРИВІЛЕЇ

- **Ознаки ризику:** масове копіювання/архівація, нетипові адмін-дії, експорт пошти, нові канали передавання даних.
- **Керування привілеями (PAM):** доступ за потреби (JIT), запис сесій, погодження змін, окремі підвищені облікові записи.
- **Процедура реагування:** канал повідомлень, ролі HR/Legal, збереження доказів, швидке відкликання доступів.

«Найбільше шкоди можуть завдати ті, хто вже всередині. Контроль привілеїв і швидка реакція — єдиний спосіб зупинити інсайдера».

ХМАРИ ТА КОРПОРАТИВНІ СЕРВІСИ
(SaaS)

- **Базові запобіжники:** перевірка налаштувань за еталонами, шифрування за замовчуванням, заборона публічних сховищ без потреби.
- **Керування доступами:** найменші необхідні права, умовні політики, універсальні дозволи, заборона надання глобальних дозволів на всі ресурси.
- **Ланцюжок постачання ПЗ:** пошук секретів, підпис артефактів, ізольовані виконавці у CI/CD.
- **Контроль над SaaS:** перевірки налаштувань, обмеження зовнішнього спільного доступу.



«Хмара — не «чужий комп'ютер», а ваша відповідальність. Правильні налаштування та контроль доступів рятують від витоків через невидимі діри».

ОПЕРАТИВНІ ІНСТРУКЦІЇ
(приклади сценаріїв)

- **Фішинг:** карантин → пошук дублікатів → перевірка посилань → скидання сесій → сповіщення й міні-навчання.
- **Інфостілер:** ізоляція пристрою → збір артефактів → відкликання токенів/сесій → блок індикаторів → посилення політик.
- **Підвищення прав:** заморозка облікового запису → аналіз останніх змін → відкат → звіт власнику системи.

«У критичний момент немає часу на роздуми. Чіткі сценарії — це ваш «пожежний план» у світі кіберзагроз».

ПОКАЗНИКИ, ЯКІ МАЮТЬ ЗНАЧЕННЯ

- **MTTA/MTTR** (виявлення/реакція): знизити на 30–50% за 90 днів.
- **Час локалізації інциденту:** < 30 хвилин для високого ризику.
- **Покриття MFA:** 100% для адмінів, ⩾ 95% загалом.
- **Покриття EDR:** ⩾ 98%.
- **Блокування горизонтальних переміщень:** зростання на старті, далі стабілізація.
- **Хибні сповіщення:** < 15% за 60 днів.
- **Адмін-дії під PAM:** 100% через 60 днів.

«Без цифр безпека — це ілюзія. Метрики дозволяють довести результат і команді, і керівництву».

ТРЕНУВАННЯ

Щомісячні практичні навчання:

- фішинг CFO → спроба входу в фінсистему
- інфостілер → крадіжка сесій
- витік секретів DevOps → підміна артефактів
- шифрувальник у відділі → горизонтальний рух
- інсайдер-адмін → експорт CRM, видалення журналів

«Навички іржавіють без практики. Тренування перетворюють теорію на автоматичні дії».

КОМУНІКАЦІЯ ЗМІН

- Прозорий **журнал змін** політик: що/коли/кого стосується.
- **Пілот → навчання → реліз,** чіткі дедлайни й нагадування.
- **Підтримка користувачів:** короткі інструкції, шаблони листів, FAQ.

«Люди бояться нового. Прозора комунікація та підтримка користувачів зменшують опір і роблять зміни частиною культури».

📌 ПРИМІТКА:

Якщо потрібно, **ST&T допоможе** накласти ці практики на ваш поточний стек (журнали, моніторинг, керування доступами, сегментація) і відпрацювати сценарії під ваші процеси.

📲 **Підписуйся, якщо хочеш знати все про цифрову безпеку простою мовою і з реальними прикладами**

https://stt.llc