Что такое SIEM и приоритет подачи журналов в SIEM

Что такое SIEM

Security information and event management (SIEM) – решение для консолидации и анализа данных о событиях, создаваемые системами безопасности, сетевой инфраструктурой конечными точками, приложениями и облачными сервисами.

Типы данных:

- Логи/журналы
- EDR - телеметрия
- Сетевая телеметрия

Возможности:

- Обогащение контекстной информацией о пользователях, активах, угрозах, уязвимостях
- Анализ корреляции, формирования отчетов, графиков
- Ретроспективный поиск, расследование инцидентов
- Проверка соответствия законодательству

?????? SIEM ??? ??????? ?????? Gartner ? 2005.
? 2015, ??? ??????????? ??????? "next-gen SIEM" ??? SIEM 2.0. ???????? ??????? – ???????? user behavioral analytics (UBA). Next-gen SIEM ????????????? ? ?????? ??????? ?? ?????????? ? ????? ??????? ??????? (??????? SOC 10+ ???????????).

? 2020 SIEM ???????? ???????? ???????????? ??? ?????? ?????? SOC ??? ??. SIEM ?????????????:

- ????????? ?????? ? ????????? ??????? ????
- ???????????????? ???????? ? ???????? ????????? ?????? ? ?????????????? ????
- ?????-?????????? ??????

Возможности SIEM:

- Logs management (collection, normalization, storage)
- Detection (correlation)
- Reporting (dashboards, reports)
- Assets inventory (vulnerability management)

Новые запросы к SIEM:

- TI management - as a context about threats
- Threat Hunting support (quick advanced search, anomaly detection)
- Machine learning detection (UEBA/UBA)
- Response orchestration and automation

Сценарий применений SIEM

1. ????????????? ???????????? (???? ?????????? ?? ??????????, ?????????????), ?????????? ?????? ?????, ?????????? ????????? ?????????
2. ????????????? ? ????????????? ????????? ?????????? ?????????? ???????, ?????????? ? ?????????? ??? ???????????? ? ??????????
3. ????????? ? ????????? ?????? ??????????, ?????????, ???????
4. ????????????? ? ????????????? ???????, ????? ?????????????
5. ??????? ?????? ? ???????? (?????????? ???????????, ???????????? ?? ?????????, Threat Hunting)
6. [?? ???? ?????????????] ?????????? ????? ??????????, ?????????? ??????????, ?????? ??????????
7. [?? ?????????? ??????] ?????? ????????????? ? ???????????? ????????? ????????? ? ?????? ??????????
8. ????????? ??????? ????? ?? ???? ???????? (? ??????????)

Эффективное логирование направлено на:

Отправку оповещений о событиях критических изменений в конфигурации программного обеспечения или развертывание новых программных решений;

Выявление событий, указывающих на инцидент кибербезопасности, например, методы Living off the Land (LOTL) или боковое перемещение после компрометации;

Поддержку реагирования на инциденты путем выявления масштаба и степени компрометации;

Мониторинг соответствия учетных записей организационным политикам, сокращение шума по оповещениям;

Предоставление возможности принимать гибкие и обоснованные решения на основе приоритизации оповещений и аналитики;

Гарантирование того, что журналы будут пригодными для аналитиков.

Хранение журнала событий

????? ???????? ???????? ?????? ???? ???????? ?? ?????? ?????? ??? ?????? ???????. ??? ?????? ?????? ??? ??????? ???????, ??? ? ????????? ??????? ????? ????????????? ?? 18 ???????, ????? ?????????? ???????? ??????????????????, ? ????????? ?????????? ????????? ????? ?????????? ? ???? ?? 70 ?? 200 ????, ?????? ??? ??????? ????? ????.

????? ???????? ???????? ????? ?????? ?????????????? ????? ?????????? ?????????? ? ?????????? ??????????????????, ??????? ????? ?????????? ? ?????????? ??????????. ??????? , ??????? ????? ???????? ???????? ??? ????????????? ????????? ? ??? ??????????, ?????? ???? ????????????? ??? ????? ?????????? ????????.

Приоритет журналов систем к подаче в SIEM

????????? ?????? ??????? ?? ???????????? ??????, ?????? ????? ??????? ?? ?????? ?????????? ? ??? ???????????? ?? ?????? ??????. ???? ?????? ????????? ???, ?? ????? ????????????? ???????? ?? ??????? ????????? ?????????? (??? ???????) ?????? ? ??????? ??????????:

1. ????????????/??????????? ??????? (External facing Systems): *VPN ???????, WEB ???????, ?????????, ????? ???????, ??????? ? ??.*
2. ??????? ????????????? ???????????? (Security Devices): *??, IPS/IDS, Email ??????, NGFW, ???????????? ??????, EDR, WAF ? ??.*
3. ??????? ????????????? (Authentication Systems): *PAM, MFA, LDAP/FreeIPA, RADIUS, CA Systems, SAML, AD ? ??.*

4. SaaS ??????????/?? ??? ?????? (SaaS Apps): *Slack, Cloudflare, Microsoft Azure Active Directory, Zscaler ? ??.*
5. ??????? ??? ??????????? ?? Windows (Windows Systems): *??????? (AD, MS SQL,Exchange, DNS, DHCP, SCCM, WSUS, ? ??.), ??????? ??????? ? ??.*
6. ??????? ??? ??????????? ?? Linux (Linux Systems): *apache, nginx, mysql, fail2ban, bind, samba, exim, squid, postgres ? ??.*
7. ??????? ?????????? (Network Devices): *????????????? (Netflow ???????), ???????????, ?????, Wi-Fi, ??????, ????????????? ? ??.*
8. ??????? ????????????? (Virtualization Systems): *VMware, Citrix, Hyper-V, KVM, ProxMox ? ??.*
9. ?????????? ??????? (Internal Systems): *??????????, ??????-?????????? ? ??.*
10. ?????????? ? ?????? ? ?????????? ???????????? (Mobile Devices): *MDM, EMM, UEM ? ??.*
11. ??????? ???????? ?????? ? ??? (Storage/Backup Systems): *DELL EMC, HP 3PAR, NetApp, Veeam, CommVault ? ??.*
12. ??????????????????????? ?? (COT: commercial off-the-shelf): *??????????? ??????????, The Microsoft Office, Adobe Photoshop, SAP ? ??.*

Подход для корпоративных сетей на основе рисков

1. ??????????? ??????? ? ????????? ??????, ???????, ????????, ????? ?????????;
2. ????????-???????, ??????? ????????? ?????? ? ???, ??????? ?????????? ? ?? ??; ??????? ?????????? ????????????? ? ????????;
3. ????? ?????? ??????????? ???????;
4. ??????????? ??????????, ????? ??? ????????? ????????????? ? ????????;
5. ???????????????? ??????? ???????;
6. ????????????????????????? ???????, ????? ??? ?????????? ????????????, ?????????? ?????????????????? ? ??????????? (? ???????, ????? ???????????? ?????????????????? ??????), CI/CD, ?????? ???????????? ???????????, ?????????? ????????? ? ????????????;
7. ????????? ??????;
8. ??????? ????????? ? ?? ? ?????????? ?????? ??;
9. ???????????????? ??????????;
10. ??????? ???????????????? ??????????;
11. ???-??????, ???????????? ????????????? ??????????? ? ????????? ??????? ??????;
12. DNS-??????? (???????????? ????????????? ???????????), ??????? ??????????? ?????, ??????? DHCP;
13. ?????????? ??-?????? (??????? ????? ?? ???? ????????????? ? ??????????? ??? ????????-????????).
14. ??????? ? ????? ?????? ???????????:
    1. ??????? ??????????????, ????????, ????? ???????????;
    2. ??-???????????, ????????, ????????

3. ??????? ??????, ????????, ????? ??????????.

Revision #7
Created 2023-10-24 11:42:58 UTC by Boris Rzr
Updated 2026-07-13 15:05:35 UTC by Dmitry Borisov