

Център за управление на сигурността



Модерните киберзаплахи еволюират постоянно. Постоянно се откриват уязвимости и постоянно се извършват атаки през глобалната мрежа. Инструментите за атакуване използват все по-сложни технологии, но стават все по-лесни и по-бързи за използване.

Справянето с тези изисква решения за постоянно наблюдение, корелация и анализ на поведението на информационните технологии. Подобни решения, изградени в организацията изискват значителни ресурси и време, за да бъдат имплементирани и изискват подготвени киберексперти, които да ги поддържат и да боравят с тях денонощно, защото Интернет никога не спи.

Центърът за управление на сигурността на Телелинк дава възможност на организацията да получат 24/7 видимост и контрол върху информационната сигурност, както и препоръки за подобрения от сертифицирани киберексперти, с които да повишат своята киберзащита.



Защо да използвате Центъра за управление на сигурността?

- Предоставя се като услуга, гарантирайки бързо внедряване без първоначална инвестиция, ясни отговорности и възможност за отказ по всяко време.
- Изграден е базиран на най-съвременна технология от водещи производители.
- Не инвестирате в оборудване, екип, обучения, сертифициране и технологии.
- Получавате гъвкави пакети, които позволяват да се заплаща това, което реално се използва.
- Подходящ за малки, средни и големи организации.
- Наличност 24x7x365.
- На частица от цената от това да изградите свой собствен Център.

ASOC LITE План

- Получете видимост върху състоянието на киберсигурността на цялата си ИТ инфраструктура
- Анализ на до 2 GB журнални записи (логове) дневно
- Опционални Екип за бързо реагиране при инциденти (ERT) и Анализ на поведението на потребителите и крайните устройства (UEBA)

Получете видимост върху киберзаплахите за Вашата организация!

ASOC PROFESSIONAL План

- Получете видимост върху състоянието на киберсигурността, включително вътрешни уязвимости и препоръки за справяне с киберзаплахите, рисковете и атаките
- Анализ на до 5 GB журнални записи (логове) и до 100 GB мрежови данни дневно
- Опционални ERT и UEBA

Започнете да адресирате киберзаплахите и да минимизирате риска!

ASOC ADVANCED План

- Получете пълна видимост върху състоянието на киберсигурността, експертни препоръки за справяне с киберзаплахите и обучения за осведоменост за Вашите служители
- Анализ на до 10 GB журнални записи (логове) и до 200 GB мрежови данни дневно
- Включен ERT и опционален UEBA

Пълна видимост, детайлни анализи и обучения!

Посетете telelink.com, за да откриете повече информация как нашия цялостен подход може да ви помогне да адресирате модерните предизвикателства пред киберсигурността.

Наблюдение на ИТ сигурността

Анализ на журналните данни и корелация

Мрежова работоспособност

Описание на ИТ активите и тяхната приоритизация

Оценка на сигурността на ИТ инфраструктурата

Одит на сигурността на ИТ инфраструктурата

Автоматично откриване на активи и обвързване с процеси

Резервни копия на конфигурациите на мрежовите устройства

Управление на уязвимости

Месечно външно сканиране за уязвимости

Анализ на откритите външни уязвимости

Месечно вътрешно сканиране за уязвимости

Анализ на откритите вътрешни уязвимости

Разширен анализ на уязвимостите върху системите

Детекция на атаки

Автоматично засичане на опити за достъп и атаки

Експертен анализ от екип от кибераналитици

Разширен анализ на потенциалните заплахи

Анализ на атаки

Идентифициране на вектора на атаката

Анализ на експозицията към атаки

Разширен анализ на атаката

Анализи, бюлетини и обучение

Месечен бюлетин за IT Security

Бюлетин относно критични нови заплахи

Специализиран бюлетин, насочен към критични точки клиента

Обучение на служители на добрите практики за киберсигурност

Експертизи на компроментирани системи

Lite Plan

Professional Plan (incl. all from Lite)

Advanced Plan (incl. all from Professional)

Месечни планове

- Наблюдение на сигурността на ИТ инфраструктурата в режим 24x7x365
- Управление на уязвимости – ежемесечно сканиране на ИТ инфраструктурата и предоставяне на структуриран доклад за откритите уязвимости, както и стъпки за адресирането им
- Детекция на атаки – мониториране и засичане на атаки и пробиви в реално време, както и въвлечане на екип от кибераналитици, които да дефинират целта и риска на атаката.
- Анализ на атаките – получаване на информация за вектора на атаката, експозиция към атаки и оценка на въздействието и консолидирането на структурирани доклади и препоръки във връзка с превантивно предотвратяване на злонамерени действия върху ИТ инфраструктурата
- Анализи, Бюлетини и обучения – навременно уведомяване при откриване на критични уязвимости или заплахи в инфраструктурата, както и провеждане на регулярни обучения за сигурност на служителите на организацията, както и в случай на тежки киберпрестъпления, екипът от кибераналитици изготвя експертизи и/или помага на властите с изготвянето им

Защо Телелинк?

- ✓ Екип от високо квалифицирани и сертифицирани инженери по киберсигурност с опит в откриването и адресирането на атаки
- ✓ Висок брой завършени проекти свързани с киберсигурност, отговарящи на различни изисквания и правила за сигурност
- ✓ 10-годишен опит в предоставянето на услуги при строги времена за реакция и отговорности за отчитане
- ✓ Цялостен подход към киберсигурността – юридически анализ, процеси, несъответствия, препоръки, внедряване на организационни мерки, поддържане на съответствие