Anti-Botnet (Анти-ботнет)

Анти-ботнет инструментите автоматично генерират проверки за ботнет, когато потребителят разглежда дадена интернет страница. В случай, че бъде установен риск, инструментът изпраща предупредително съобщение към устройството. Най-честото анти-ботнет решение е CAPTCHA (Напълно автоматизиран публичен тест на Тюринг за разграничаване на компютри от хора).

Anti-Virus (Антивирусни решения)

Антивирусните решения използват най-ново поколение технологии за идентифициране на вируси, така че да защитят потребителите от вируси, шпионски софтуер, троянски коне и червеи, които биха могли да заразят оборудването им чрез имейл или при сърфиране в Интернет.

Anti – malware (Анти-малуер)

Анти-малуер или програма, защитаваща от зловреден софтуер, представлява програма, предназначена да защитава компютрите и мрежите от заплахи или вирусни атаки, като например рекламен софтуер (адуер), шпионски софтуер (спайуер) и други злонамерени програми.

Anti-Phishing (Антифишинг)

Антифишинг защитава потребителите от фалшиви интернет страници, които често представляват съвършена реплика на легитимна страница, като разликите са неуловими за човешкото око. Защитата се постига чрез улавяне на фалшиви имейли и блокиране на фишинг сайтове.

man-in-the-middle attack (Атака от типа „човек по средата“)

Атака от типа „човек по средата“ (man-in-the-middle attack (MITM)) представлява атака, при която хакерът тайно препредава или променя комуникацията между две страни, които са с убеждението, че общуват директно една с друга. Например, жертвата смята, че се е свързала със сайта на банката си, и действително потокът на трафика към и от реалния сайт на банката остава непроменен, така че жертвата не вижда нищо обезпокоително. Трафикът обаче бива пренасочен към страницата на атакуващия, което му позволява да види личните данни, въведени от жертвата (логин, парола, ПИН и др.).

Denial of Service (Атака тип „отказ от обслужване“)

Атака тип „отказ от обслужване“ (Denial of Service (DoS)) или „разпределен отказ от обслужване (Distributed Denial of Service (DDoS)) е налице, когато една или повече компрометирани системи лансират масирана атака върху отдалечена цел или цели, опитвайки се да претоварят мрежовите ресурси и да попречат на предоставянето на услугата. Някои DDoS атаки предизвикват продължителен, пълен срив на дейността на големи онлайн оператори.

Bank Trojan (Банков троянски кон)

Банковият троянски кон представлява злонамерена компютърна програма, която улавя лична информация и данни за самоличност, използвани за достъп до онлайн банкиране или разплащателни сметки.

Clientless (Безклиентска програма)

„Безклиентска програма“ означава програма, която се управлява изцяло от мрежата, без да се изисква инсталирането на софтуер върху крайното устройство, използващо програмата.

Fileless Malware (Безфайлов зловреден софтуер)

Безфайлов зловреден софтуер или „безфайлово заразяване“ представлява форма на злонамерена компютърна атака, която съществува изключително в рамките на енергозависими компоненти за съхранение на данни като например RAM, процеси, осъществяващи се в паметта и обслужващи зони. Това отличава този вид злонамерен софтуер от класическия вирус, загнезден в паметта, който изисква някакъв тип контакт с енергонезависими носители на електронно съхранена информация, като например хард диск или флашка. Заразяването обикновено става при посещение на злонамерен уебсайт. Безфайловият злонамерен софтуер не съдържа файл, който да бъде открит от стандартните антивирусни програми. Той се крие в работната памет на компютъра и по тази причина откриването му е изключително трудно. От друга страна, този тип злонамерен софтуер рядко оцелява след рестартиране на компютъра, след което компютърът би следвало да работи както преди заразяването.

Bot (Бот)

„Бот“ представлява компютърна програма, която автоматизира действия от името на посредник за нуждите на друга програма или индивид. Използва се за изпълнението на рутинни задачи. Използването на ботове за злонамерени цели включва разпространение на нежелани съобщения, събиране на данни за достъп и иницииране на DDoS атаки (атаки за отказ на услуги).

Botnet (Ботнет)

Ботнетът представлява съвкупност от компрометирани компютри със задействани злонамерени програми, които се управляват от разстояние посредством сървър за управление и контрол (C&C – command & control), управляван от киберпрестъпник. Киберпрестъпниците упражняват отдалечен контрол посредством автоматизирани процеси (ботове) в публични комуникационни канали в интернет (IRC) или интернет сайтове (Тези сайтове могат да бъдат управлявани пряко от инициатора на ботнет (т.нар. „бот пастир“) или да бъдат напълно легитимни интернет сайтове, използвани за тази цел.)

Whitelist (Бял списък, позволен списък)

Бял списък, позволен списък, допустим списък представлява списък на позволени елементи, които автоматично се пропускат независимо от използвания гейт.

White Hat – Black Hat Бяла шапка/черна шапка

„Бяла шапка“ и „черна шапка“ са термини, с които се описват „добрите“ и „лошите“ момчета в света на киберпрестъпленията. „Черните шапки“ са хакерите с престъпни намерения. „Белите шапки“ са онези, които използват таланта и уменията си, за да защитят данните от други хакери, като откриват подлежащи на отстраняване уязвимости в системата.

Attack Vector (Вектор на атака)

Векторът на атака представлява съвкупност от всички уязвими точки, през които атакуващият може да осъществи достъп до целевата система. Векторите на атаки включват уязвими точки в технологията, както и човешко поведение, умело използвано от атакуващите, за да получат достъп до мрежите. Увеличаването на видовете устройства, свързани с Интернет на нещата, както и на възможностите за работа от вкъщи силно увеличават вектора на атака, поради което мрежите все по-трудно могат да бъдат защитени.

Virtual Private Network (Виртуална частна мрежа)

Виртуална частна мрежа (VPN) разширява границите на частната мрежа в публичната и позволява на потребителите да изпращат и получават данни в споделени или публични мрежи така, както ако компютърните им устройства са директно свързани към частната мрежа. По същество това е един виртуален, безопасен коридор.

Virus (Вирус)

Вирусът представлява злонамерена компютърна програма, която често се изпраща като имейл приложение или присъства в свалено съдържание и има за цел да зарази устройството. Веднъж заразил устройството, вирусът може да смени уеб браузъра, да показва нежелани реклами, да изпраща спам, да предоставя на престъпниците достъп до устройството и списък с контакти, да промени настройките за сигурност, да сканира и открива лична информация като например пароли.

Вътрешна заплаха

Вътрешна заплаха е налице, когато упълномощен потребител на системата, обикновено служител или изпълнител, представлява заплаха за организацията, тъй като в състояние да заобиколи повечето решения за сигурност, базиращи се на защитен периметър.

Commercial off-the-shelf product (Готов пазарен продукт)

Готовият пазарен продукт (Commercial off-the-shelf product (COTS)) представлява пакетно решение, което впоследствие се адаптира спрямо потребностите на закупуващата организация, вместо да се използват направени по поръчка решения.

Brute Force Attack (Груба силова атака)

Това е метод за разпознаване на парола (или на ключ за криптиране на съобщение), който включва систематизирани опити за пробив, използващи голям обем възможни комбинации от символи докато не бъде открита правилната такава. Един от начините да се намали уязвимостта на груба силова атака е да се ограничи позволеният брой опити за въвеждане на парола – напр. да се разрешат само три неуспешни опити, след което повторен опит да се допуска едва след 15 минути.

Honeypot (Гърне с мед)

„Гърнетата с мед“ представляват програми за компютърна сигурност, които симулират мрежови ресурси, представляващи интерес за хакерите, за да ги подмамят и вкарат в капан. Атакуващият решава, че използвате незащитени услуги, които могат да се използват за пробив в машината. Honeypot програмата ви предупреждава в случай на съгласувана атака. Две или повече „гърнета“ в мрежа образуват „медена мрежа“ (honeynet).

Bring your own computer („Донесете собствен компютър“)	Донесете собствен компютър (Bring your own computer или BYOC) е сравнително нова тенденция в корпоративния свят, при която служителите се насърчават или им се позволява да донесат и използват лично компютърно устройство за осъществяване на част от служебните си задължения, и най-вече личен лаптоп.
Bring Your Own Device („Донесете собствено устройство“)	Донесете собствено устройство (Bring Your Own Device или BYOD) представлява корпоративна политика, която допуска, насърчава или изисква от служителите на организацията да използват свои лични устройства, например смартфон, таблет и лаптоп, за служебни цели и за осъществяване на достъп до корпоративните системи и данни.
2FA Two-factor Authentication (Двуфакторно удостоверяване)	Двуфакторното удостоверяване съчетава статична парола с външно устройство за удостоверяване като например хардуерен токън, генериращ случайна еднократна парола, смарткарта, кратко съобщение (при което мобилният телефон поема функциите на токън), или уникална физическа черта, като например пръстов отпечатък.
Decryption (Декриптиране)	Декриптирането е процес на декодиране на шифров текст в обикновен текст, четим за хората. Това е обратният процес на криптирането, т.е. процеса по превръщане на обикновен в шифров текст. Киберпрестъпниците използват софтуер и техники за декриптиране, за да „прекъснат“ криптирането за нуждите на сигурността и да получат достъп до защитена информация.
Exploit (Експлоатация)	Експлоатация или „ескплойт“ представлява възползване от уязвимост или грешка в мрежова система с цел провикване в същата или атака.
Zero-day Exploit (Експлоатация „Нулев ден“)	Този термин се използва, за да се опише експлойт кода, написан с цел възползване от дадена уязвимост преди софтуерният търговец да е научил за същата и да е публикувал „кръпка“. В резултат на това изпреварване, атакуващите имат възможност да експлоатират уязвимостта, освен в случаите, когато са въведени проактивни технологии за предотвратяване на такава експлоатация, които да защитят избрания за атака компютър.
Domain Name System (Ексфилтрация на данни на база DNS)	Ексфилтрацията на данни на база DNS представлява атака от ниско ниво срещу DNS сървъри с цел придобиване на неупълномощен достъп. Подобни атаки трудно се установяват и могат да доведат до загуби на данни.

Backdoor (Задна врата)

„Задната врата“ са функции или програми, използвани от атакуващите, за да получат достъп до компютър или мрежа. Програмистът може да заобиколи стъпките, свързани със сигурността и да получи достъп до компютъра посредством „трапдор“ програми, в случай на атака срещу компютърната система или мрежата. Атакуващите могат да използват такива механизми и за достъп до компютри и мрежи без надлежно разрешение.

Защита на крайни точки

Под „защита на крайни точки“ се разбира система за управление на мрежовата сигурност, която следи крайните точки в мрежата – хардуерни устройства като работни станции и мобилни устройства, от които се осъществява достъп до дадена мрежа.

Secure Sockets Layer (Защитен гнездови слой)

Защитеният гнездови слой (SSL) представлява стандартна технология за сигурност, която установява криптирана връзка между уеб сървър и браузър. SSL е разработен от Netscape, за да позволи частния пренос на документи през интернет.

Firewall (Защитна стена)

Защитната стена (firewall) представлява система за сигурност, която образува виртуален периметър (ограда) около дадена мрежа или работна станция, за да я защити от вируси, червеи и хакерски атаки.

Web Application Firewall (Защитна стена за уеб приложение)

Защитна стена за уеб приложение (Web Application Firewall (WAF)) е специален вид защитна стена за приложения, която филтрира, следи и блокира HTTP трафик към и от уеб услугата. Чрез проверка на HTTP трафика, защитната стена може да предотврати атаки, които експлоатират известните уязвимости на приложението, като например SQL инжектиране, кръстосано скриптиране (XSS), вмъкване на файлове и неправилна конфигурация на системата.

Maware (Злонамерен софтуер)

Злонамерен софтуер е общ термин за всякакъв вид софтуер със зловредни намерения спрямо потребителя.

Aware (Злонамерена реклама)

Злонамерена реклама представлява използването на онлайн реклами за разпространение на злонамерени програми. Киберпрестъпниците могат да вградят специален скрипт в рекламен банер или да пренасочат потребител, кликнал върху реклама, към специална страница, съдържаща код за сваляне на злонамерен софтуер. Престъпниците използват специални методи, за да заобиколят филтри на големите рекламни мрежи и да вмъкнат злонамерено съдържание в доверени сайтове. В някои случаи дори не се налага посетителят да кликне върху фалшивата реклама – кодът се изпълнява при показване на рекламата.

Indicators of Compromise (Индикатори за компрометираност)	Индикаторите за компрометираност (Indicators of compromise (IoC)) представляват криминалистични данни от влизания в системата или файлове, с помощта на които се идентифицира злонамерена дейност в система или мрежа. Индикаторите за компрометираност подпомагат специалистите по информационна сигурност и информационни технологии в установяването на пробиви в данните, зараза със злонамерен софтуер и други заплахи.
Process hollowing (Инжектиране на зловреден код в неактивен процес)	Този подход представлява експлоатиране на сигурността, при който атакуващият премахва кода на изпълним файл и го замества със злонамерен код. Този тип атака се използва от хакерите, за да принудят легитимен процес да изпълни злонамерен код. Подобни атаки могат да се извършват чрез заобикаляне на потенциалните защити, като например софтуер за анализ на установените пробиви.
Code injection (Инжектиране на код)	„Инжектиране на код“ е процес, който често се използва от злонамерен софтуер с цел избягване на идентифицирането му от страна на антивирусни и антималуер програми. По същество представлява „инжектиране“ на зловреден код в легитимен процес. Така легитимният процес служи като прикритие и антималуер инструментите остават под заблудата, че работи легитимен процес, като по този начин се прикрива изпълнението на злонамерения код.
Internet of things (Интернет на нещата)	Терминът „Интернет на нещата“ (Internet of Things (IoT)) се използва за ежедневни предмети, свързани към Интернет, които са в състояние автоматично да събират и прехвърлят данни без да е необходима човешка намеса. Интернетът на нещата включва всякакви физически предмети (а не само традиционните компютри), които имат IP адрес и могат да прехвърлят данни: тук се включват домакински уреди, измервателни уреди, автомобили, охранителни камери и дори хора (напр. сърдечни импланти).

Cybersecurity (Киберсигурност)

Киберсигурност представлява съвкупността от процесите за защита и опазване на активите, пренасящи информацията на дадена организация, от кражба или атака. Необходими са задълбочени познания за възможните заплахи, като например вируси и други злонамерени обекти. Управлението на самоличността, управлението на риска и управлението на инцидентите съставляват същината на стратегията за киберсигурност на дадена организация.

Cyber bullying (Кибертормоз)

Кибертормозът представлява използване на електронни средства, най-вече съобщения и платформи на социални медии, за оказване на тормоз и тероризиране на жертвата. Кибертормозът е сериозен проблем, засягащ най-вече младите хора, тъй като позволява на тормозещия да засили агресивното си поведение, публично да осмива жертвата си и да извършват увреждащи действия по начин, който трудно може да се установи от родители и учители.

Keylogger (Кийлогър)

Кийлогър е вид шпионски софтуер, който записва всичко, въведено чрез клавиатурата на компютъра. Софтуерът може да запише всичко, написано от потребителя, включително съобщения, имейли, потребителски имена и пароли.

Data theft (Кражба на данни)

Кражбата на данни представлява умишлена кражба на чувствителни данни от страна на злонамерени лица.

Identity theft (Кражба на самоличност)

Кражба на самоличност е налице, когато злонамерено лице събере достатъчно информация относно жертвата (име, адрес, дата на раждане), за да може да извършва измами с фалшива самоличност – напр. да използва откраднатa информация за потвърждаване на самоличността, за да получи стоки или услуги посредством измама. Откраднатите данни могат да бъдат използвани за създаване на нова сметка/акаунт на името на жертвата (напр. банкова сметка), за превземане на съществуващ акаунт на жертвата (напр. акаунт в социална мрежа) или за използване на самоличността на жертвата като прикритие за извършването на престъпни дейности.

Encryption (Криптиране)

Криптирането е процес по поддръжка на поверителността на данните чрез конвертиране на обикновени данни в таен код с помощта на криптиращ алгоритъм. Единствено потребители с подходящ декриптиращ ключ могат да разчетат и получат достъп до криптирани данни или шифрован текст.

Cryptojacking (Криптоджакинг)

Под „криптоджакинг“ се разбират опитите на хакери да използват изчислителните сили на компрометирано устройство, за да генерират или „копаят“ криптовалута без знанието на собственика. „Копаенето“ може да се извършва чрез инсталиране на зловредна програма върху целевия компютър или чрез различни видове безфайлов злонамерен софтуер. Понякога превземането на изчислителната сила на компютъра се извършва при отваряне на страница, съдържаща специален скрипт за „копаене“, при гледане на онлайн реклама или решаване на captcha тест.

Critical infrastructure (Критична инфраструктура)

Под „критична инфраструктура“ се разбират основните системи на организацията, които са важни за нейното оцеляване, като заплахите спрямо тези основни системи поставят под опасност цялата организация.

Patch (Кръпка)

Кръпката осигурява допълнителен, ревизиран или актуализиран код за дадена оперативна система или приложение. С изключение на софтуера с отворен код, повечето търговци на софтуер не публикуват изходния си код. В повечето случаи, кръпките представляват части от бинарен код, които се „закърпват“ към съществуваща програма (използвайки програма за инсталиране).

PII Personal identifiable information (Лични данни, позволяващи идентифициране на индивида)

Лични данни, позволяващи идентифициране на индивида (Personal identifiable information) представляват данни, които идентифицират уникалната самоличност на дадено лице.

Threat hunting (Лов на киберзаплахи)

Лов на киберзаплахи представлява активна дейност по кибер защита, при която професионалистите по киберсигурност активно претърсват мрежите, за да открият и отстранят усъвършенствани заплахи, които заобикалят съществуващите решения за сигурност.

Cybersecurity (Мрежова (кибер) сигурност)

Услуги по киберсигурност за масовия пазар (напр. антималуер, антифишинг), които оперират от мрежата за защита на киберсигурността, а не в крайна точка, като например настолен компютър или мобилно устройство. Базираните в мрежа услуги могат да защитят всяко свързано устройство, независимо от модела му и използваната оперативна система. Този тип услуга обаче не може да бъде заобиколена подобно на други решения за киберсигурност и могат да бъдат внедрени без да се налага крайният потребител да инсталира, актуализира или конфигурира софтуер, което води до по-голяма ползваемост.

In-line Network device (Мрежово устройство)

Мрежово устройство е устройство, което получава пакети и ги изпраща към нужната дестинация. Кабелните мрежови устройства включват рутери, суичове, защитни стени, системи за установяване и предотвратяване на вмешателства, защитни стени на уеб приложения, антималуер и мрежови кранове.

CAPTCHA (Напълно автоматизиран публичен тест на Тюринг за разграничаване на компютри от хора)	CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) или „Напълно автоматизиран публичен тест на Тюринг за разграничаване на компютри от хора“ представлява тест за реакция на предизвикателства, често използван от интернет сайтовете, за да проверят дали потребителят е човек, а не робот. Тестът може да включва прости аритметични задачи и въпроси относно представени изображения, с отговорите на които роботите обикновено се затрудняват.
Clickjacking (Отвличане на кликове (кликджакинг))	Отвличането на кликове представлява подвеждането на потребител да кликне върху даден обект в интернет страница посредством заблудата, че всъщност кликва върху нещо друго. Атакуващият зарежда прозрачна страница върху легитимното съдържание на интернет страницата, така че жертвата си мисли, че кликва върху легитимен обект, а всъщност кликва върху нещо в невидимата страница на атакуващия. По този начин атакуващият „отвлича“ кликването на жертвата за свои собствени цели. Отвличането на кликове може да се използва за инсталиране на злонамерен софтуер, за получаване на достъп до онлайн сметка на жертвата или за задействане на уебкамерата на жертвата.
Threat Assessment (Оценка на заплахите)	Оценката на заплахите представлява структуриран процес, използван за идентифициране и оценка на различни рискове или заплахи, пред които може да бъде изправена дадена организация. Оценката на киберзаплахи е важна част от стратегията за управление на риска и усилията за защита на данните на всяка една организация.

Security Perimeter (Периметър за сигурност)

Периметър за сигурност представлява дигитална граница, определена за дадена система или домейн, в рамките на която се прилага конкретна политика или архитектура за сигурност.

Business continuity plan (План за непрекъснатост на работата)

Планът за непрекъснатост на работата представлява набор от правила, приложими от дадена организация, за работа в извънредна ситуация, като например масирана кибератака. Планът за непрекъснатост на работата осигурява защита срещу бедствия и очертава стратегиите и плана за действие с цел продължаване на дейността както обичайно, в случай на значително по мащаб кибер събитие.

Zero-Touch Provisioning or deployment (Поддръжка или внедряване с нулево докосване)

Поддръжка с нулево докосване представлява автоматичен процес по конфигуриране на устройствата, което освобождава ИТ администраторите за по-важни задачи. Автоматичният процес намалява възможността за грешки при ръчното конфигуриране на устройствата и намалява нужното време за настройка на използваните от служителите устройства, често без да се налага намесата от страна на ИТ специалист. Потребителите могат да настроят устройствата си с няколко кликвания, с което отпада необходимостта администраторите да създават и следят изображения или да управляват инфраструктурата, необходима, за да внедрява тези изображения в нови или повторно използвани устройства.

Packet sniffing (Подслушване на пакети)

Подслушването на пакети позволява улавянето на данни, докато същите се пренасят в мрежата. Програмите за подслушване на пакети се използват от мрежовите професионалисти за диагностициране на мрежови проблеми. Злонамерени лица също могат да използват такива програми, за да улавят некриптирани данни като пароли и потребителски имена в мрежовия трафик. Веднъж след като улови тази информация, злонамереното лице може да се сдобие с достъп до системата или мрежата.

Data Loss Prevention (Предотвратяване на загубата на данни)

Предотвратяване на загуба на данни (DLP) е общ термин за широк набор от инструменти, процеси и процедури за сигурност, насочени към предотвратяване на попадането на чувствителни данни в ръцете на неупълномощени или злонамерени индивиди. DLP има за цел да предотврати такива инциденти посредством различни техники, като например строг контрол върху достъпа до ресурси, блокиране или проследяване на приложения към имейли, възпрепятстване на размяната на файлове към външни системи, блокиране на функцията „изрязване и поставяне“, забрана на използването на социални мрежи и криптирането на съхранявани данни.

Data breach (Пробив в данните)

Пробив в данните е събитие, при което хакер успешно експлоатира уязвимост на мрежа или устройство и си спечелва достъп до съответните файлове и данни.

Endpont protection and response (Проверка на крайните точки и реакция)

Проверка на крайните точки и реакция (EDR) представлява набор от инструменти, които защитават крайните точки от евентуални заплахи. EDR платформите включват софтуерни и мрежови инструменти за установяване на подозрителни дейности в крайните точки, обикновено чрез постоянно следене.

NDR (Проверка на мрежата и реакция)

Проверката на мрежата и реакцията (NDR) представлява вид решения за сигурност, използвани от организациите за установяване на злонамерена мрежова активност, извършване на разследване с цел определяне на първопричината и реакция с цел намаляване на заплахата.

RDP (Протокол за отдалечен достъп до десктоп)

RDP е протокол за отдалечена връзка с компютри, използващи операционна система Windows. Протоколът позволява взаимодействие с елементите на десктопа, както и достъп до други ресурси на устройството. Замислен е като инструмент за отдалечена администрация, но често се използва от нарушители за пробив в компютрите. Киберпрестъпниците експлоатират неправилно конфигурираните RDP настройки или уязвимости на системния софтуер и могат да прекъснат RDP сесия и да влязат в системата с „разрешението“ на жертвата.

sandbox (Пясъчник)

В областта на киберсигурността, под „пясъчник“ (sandbox) се разбира изолирана среда в дадена мрежа, която имитира оперативната среда на крайния потребител. „Пясъчниците“ се използват за безопасно изпълнение на подозрителен код, така че да не се излага на опасност устройството или мрежата-приемник.

SIM swapping (Размяна на СИМ карти)	Размяната на СИМ карти представлява измама, използвана за улавяне на изпращаните с кратко текстово съобщение кодове за потвърждение при онлайн банкиране. За да уловят еднократните пароли за финансови транзакции, киберпрестъпниците създават или се сдобиват по нечестен начин с копие от СИМ картата на жертвата – например, като приеме самоличността на жертвата, атакуващият може да претендира за изгубена СИМ карта и да поиска нова от мобилния оператор. За да защитят клиентите си от подобни схеми, повечето банки изискват новата СИМ карта да бъде повторно свързана към акаунта.
Threat Intelligence (Разузнаване на заплаха)	Разузнаване на заплаха или киберразузнаване на заплахи представлява проактивно набавяне и използване на информация с цел разбиране на заплахите, насочени срещу организацията.
ATP (Разширена защита от заплахи)	Разширената защита от заплахи (Advanced Threat Protection (ATP)) представлява набор от решения за сигурността, които защитават срещу усъвършенстван зловреден софтуер или хакерски атаки, насочени срещу чувствителни данни. Разширената защита от заплахи включва както софтуер, така и услуги по управление на сигурността.
MITRE ATT&CK™ Framework (Рамка MITRE ATT&CK™)	Рамката MITRE ATT&CK™ представлява всеобхватна матрица от тактики и техники, използвани от ловци на заплахи, изпитатели на уязвимости и защитници за по-точно класифициране на атаките и оценка на риска, пред който е изложена организацията. Целта на рамката е да подобри откриването на неприятели след компрометиращо сигурността събитие в организацията, като илюстрира действията, вероятно предприети от хакера. https://attack.mitre.org/
Ransomeware (Рансъмуер)	Под „рансъмуер“ се разбират злонамерени програми, които имат за цел да изнудят жертвите си за пари чрез блокиране на достъпа им до компютъра или чрез криптиране на съхранени данни. Злонамереният софтуер изписва съобщение, с което атакуващият предлага да възстанови системата/данните в замяна на заплащане на определена сума. Понякога киберпрестъпниците се опитват да придадат достоверност на действията си като се преструват на органи на реда. В такъв случай съобщението им гласи, че системата е блокирана или данните са криптирани, тъй като жертвата използва нелицензиран софтуер или е осъществила достъп до незаконно съдържание и по тази причина ще трябва да заплати съответна глоба.
Security Incidence response (Реакция на инциденти със сигурността)	Реакцията на инциденти представлява планиран подход за адресиране и управление на реакцията след кибератака или пробив в мрежовата сигурност. Целта е да се въведат ясни процедури, които да бъдат определени преди настъпването на атака с цел минимизиране на щетите, намаляване на времето за възстановяване след бедствието и на разходите, свързани с пробива.

Adware (Рекламен софтуер, създаден с користна цел (адуер))	Рекламният софтуер, създаден с користна цел (адуер) бомбардира потребителите с безброй реклами и изскачащи рекламни прозорци, предизвиквайки сериозни неудобства. Адуерът може да носи и реална опасност за устройствата, тъй като не е изключено нежеланите реклами да съдържат злонамерен софтуер или да пренасочват търсенията на потребителя към злонамерени интернет страници, които събират личните му данни. Адуер програмите често са вградени в софтуер за свободно (фриуер) или ограничено във времето (шеъруер) ползване, като операторът на рекламният софтуер непряко получава приходи от използването на програмата. Адуер програмите обикновено не се отличават в системата по никакъв начин. Рядко включват процедура за деинсталиране, а опитите за ръчното им премахване могат да причинят неизправност на оригиналната програма-носител.
Security Orchestration, Automation and Response (Решение за оркестрация, автоматизация и реакция за сигурност)	Решението за оркестрация, автоматизация и реакция за сигурност (Security Orchestration, Automation and Response – (SOAR)) представлява многопластово решение от съвместими софтуерни програми, използвани от организацията за набиране на данни относно заплахите за сигурността в мрежата и да реагира на по-маловажните събития, засягащи сигурността, без човешка намеса.
Рисктул (RiskTool)	Risktool програмите притежават редица функции, като например прикриване на файлове в системата, скриване на прозорците на текущи приложения или прекратяване на активни процеси. Сами по себе си не са зловредни, но включват „миньори“ на криптовалута, които генерират биткойни, използвайки ресурсите на набелязаното устройство. Киберпрестъпниците обикновено ги използват в скрит режим. За разлика от NetTool, тези програми са предвидени да работят на местно ниво.
Parental control (Родителски контрол)	Под родителски контрол се разбират различни опции, които могат да бъдат включени в услуги за цифрова телевизия, компютърни и видео игри, мобилни устройства и софтуер и които позволяват на родителите да ограничат достъпа до съдържание за децата си. Тези опции са създадени, за да помогнат на родителите да контролират какъв тип съдържание може да бъде достъпно за децата им.
Rootkit (Руткит)	Руткит представлява набор от софтуерни инструменти или програма, които предоставят на хакера отдалечен достъп до и контрол върху даден компютър или мрежа. Самите те не носят преки щети, а и този тип софтуер има легитимни ползи, като например отдалечена подкрепа за крайните потребители. Повечето обаче отварят задна врата в компютъра за въвеждането на зловреден софтуер, вируси и рансъмуер или използват системата за последващи атаки срещу мрежовата сигурност. Обикновено се инсталират посредством откраднатата парола или чрез експлоатиране на уязвимостите на системата без знанието на жертвата. В повечето случаи се използват успоредно с друг зловреден софтуер, за да се избегне откриването им от антивирусен софтуер в крайната точка.

Greylist (Сив списък)	Сивият списък съдържа елементи, които са временно блокирани (или временно разрешени) до изпълнението на допълнителна стъпка.
Security as Service (Сигурност като услуга)	„Сигурност като услуга“ (SECaaS) е вид облачна изчислителна услуга, при която доставчикът предлага на клиента възможността да използва дадено приложение. Примери за SaaS включват онлайн имейл услуги или онлайн системи за редактиране на документи. Потребител на SaaS решение може единствено да използва предложеното приложение и да извършва минимални промени в конфигурацията. Доставчикът на SaaS носи отговорност за поддръжка на приложението.
Intrusion Prevention System (IPS) (Система за предотвратяване на проникване)	Система за предотвратяване на проникване (Intrusion Prevention System (IPS)) представлява система за мрежова сигурност, предвидена да предотвратява пробиви в мрежата от страна на злонамерени лица.
Drive-by Download (Скрито зареждане)	Този тип атаки са често срещан метод за разпространяване на злонамерен софтуер. Киберпрестъпниците намират незащитени интернет страници и имплантират злонамерен скрипт в HTTP или PHP кода на някоя от страниците. Този скрипт може да инсталира злонамерен софтуер директно в компютъра на посетител на сайта или да приеме формата на вградена рамка (IFRAME), която пренасочва жертвата към контролиран от киберпрестъпниците сайт. Такива атаки са известни като „скрито зареждане“, тъй като не изискват каквото и да било действие от страна на жертвите, освен посещението на компрометирания сайт: инфектирането става автоматично (и незабелязано), ако компютърът е уязвим по някакъв начин (например, ако са пропуснали да актуализират защитата на някое от приложенията си).
Social engineering(Социален инженеринг)	Социалният инженеринг е метод с нарастваща популярност за добиване на достъп до неупълномощени източници посредством експлоатиране на човешката психология и манипулиране на потребителите, вместо осъществяване на пробив или използване на технически хакерски техники. Вместо да се опитва да намери софтуерна уязвимост в дадена корпоративна система, социалният инженер може да изпрати имейл до даден служител, като се преструва на член на ИТ отдела, опитвайки се да го подмами да му разкрие чувствителна информация. Социалният инженеринг е основата на метода „фишинг с харпун“.
Spam (Спам)	Спам е наименованието, което най-често се дава на нежелани имейли. По същество, това представляват нежелани реклами – електронният вариант на рекламните брошури, пускани в пощенската кутия.
Scareware (Сплашващ софтуер)	Скеъруер представлява злонамерен софтуер, който използва тактики на сплашване, често под формата на изскачащи прозорци, които предупреждават потребителите, че са заразени с вирус, за да ги принудят да посетят интернет страници, съдържащи зловреден софтуер.
Spoofing (Спуфинг)	Спуфинг представлява опит от страна на неупълномощен субект или атакуващо лице да се сдобие с незаконен достъп до дадена система като се преструва като упълномощен потребител. Спуфингът включва всякакво действие, при което комуникация от неизвестен източник се маскира като комуникация от известен, доверен източник. Спуфинг може да се прилага по отношение на имейли, телефонни обаждания и интернет страници или може да бъде по-техническо по характер, като например компютър, който извършва спуфинг на IP адрес.
Срив на дейността	Терминът „срив на дейността“ обозначава всякакво прекъсване на обичайния начин на работа на дадена система, процес или събитие. Кибератаките водят до срив в бизнес операциите и свързания с него риск от загуби за организацията.

Pen test (Тестове за пробив)	Тестове за пробив (Penetration) Testing) е начин за умишлено поставяне на сигурността на дадена компютърна система, мрежа или уеб приложение на изпитание, за да се установят уязвимостите, които биха могли да бъдат използвани от хакери.
Trojan (Троянски кон)	Троянският кон представлява злонамерена програма, която изпълнява неоторизирани от потребителя действия: изтрива, блокира, модифицира или копира данни и нарушава работата на компютрите или компютърните мрежи. За разлика от вирусите и червеите, троянските коне не са в състояние да се копират или репликират.
Dark net (Тъмна мрежа)	Под „Тъмна мрежа“ разбираме криптирани части от Интернет, които не се индексират от търсачките и се използват от всевъзможни престъпници, включително педофили, трафиканти на хора и контрабандисти, както и киберпрестъпници, с цел комуникация и споделяне на информация без да бъдат засечени или идентифицирани от силите на реда. В тъмната мрежа може да се закупи всякакъв вид зловреден софтуер. Като подгрупа на дълбоката мрежа, до която има достъп всеки с правилното url, тъмната мрежа изисква специален софтуер (напр. Tor) с правилен ключ за декриптиране, право на достъп и знания за откриване на съдържание. Потребителите на тъмната мрежа остават почти напълно анонимни, благодарение на мрежови връзки от типа „точка до точка“ (P2P), което прави активността им в мрежата изключително трудна за проследяване.
Удостоверяване на самоличността	Удостоверяването на самоличността представлява процес по установяване на самоличността на потребител или произхода на данни, както и на истинността на подадена информация. В света на компютрите, това е процес на идентифициране на лице или система посредством потребителско име, парола и т.н. Удостоверяването на самоличността помага на индивидите и системите да получат оторизация въз основа на своята самоличност и да предотвратят неоторизиран достъп.
Управление на информацията и събитията по сигурността	Управление на информацията и събитията по сигурността (SIEM) представлява формален процес, чрез който сигурността на дадена организация се следи и оценява на постоянна база. SIEM помага за автоматично идентифициране на системи, които не съответстват на политиката за сигурност и информира екипа за реакция на инциденти (IRT) за всякакви събития в нарушение на сигурността.
Identity and Access Management IAM (Управление на самоличността и достъпа)	Управление на самоличността и достъпа (Identity and Access Management (IAM)) е процес, използван от дадена организация за предоставяне на достъп или отказ на такъв до обезопасена система. Процесът интегрира системите от работни потоци и включва организационен мозъчен тръст, който анализира и се грижи за ефективната работа на системите за сигурност.
Advanced Persistent Threat (Усъвършенствани постоянни атаки)	Усъвършенстваната постоянна атака използва най-усъвършенстваните тактики и технологии за пробив в мрежи на високо равнище. Тези атаки се стремят да останат „извън полезрението“ докато изследват мрежата, като остават незабелязани в продължение на седмици, месеци и дори години. Усъвършенстваните постоянни атаки се използват най-често от злонамерени представители на национални държави, които се стремят да причинят сериозен срив и поражения за икономическата и политическа стабилност на дадена държава. Тези атаки могат да се разглеждат като кибер аналог на шпионските „спящи клетки“.
Уязвимости	Уязвимостите представляват слабости в софтуерните програми, които могат да бъдат експлоатирани от хакерите с цел компрометиране на компютъра

Phishing (Фишинг)

„Фишинг“ е вид интернет измама, чрез която киберпрестъпниците се стремят да получат данните на потребителя посредством заблуда. Тук се включва кражбата на пароли, на номера на кредитни карти, на банкови данни и друга поверителна информация. Фишинг съобщенията обикновено приемат формата на фалшиви уведомления от банки, доставчици, системи за електронни плащания и други организации. С тях се насърчава получателя, по една или друга причина, да въведе/актуализира свои лични данни. Най-често цитираните причини включват „подозрително влизане в акаунта“ или „изтекъл срок на валидност на паролата“.

Spear phishing (Фишинг с харпун)

Фишинг с харпун представлява фишинг схема, която се прицелва в конкретен индивид или организация, обикновено чрез персонализиран имейл, кратко текстово съобщение или друг вид електронна комуникация, за да измами жертвата под прикритието на легитимна транзакция.

Hacker (Хакер)

Хакер е термин, с който обикновено се описва лице, опитващо се да получи неупълномощен достъп до дадена мрежа или компютърна система

Security Operations Center (Центърът за управление на сигурността на информацията)

Центърът за управление на сигурността на информацията (ISOC или SOC) представлява функция, с която корпоративните информационни системи (интернет сайтове, приложения, бази данни, центрове за данни и сървъри, мрежи, десктоп и други крайни точки) се проследяват, оценяват и защитават от SOC аналисти.

Цифрова криминалистика

Цифровата криминалистика представлява процес по събиране и интерпретиране на електрони данни с цел представянето им като законни доказателства в съда.

Цифрова трансформация

Цифровата трансформация представлява процес по използване на цифрови технологии за създаване или модифициране на бизнес процесите и обслужването на клиенти с цел поддържане на актуалност спрямо текущите бизнес и пазарни изисквания.

Цялост на данните

„Цялост на данните“ е широк термин, който се отнася до поддръжката и гарантирането на качеството на данните. Тук се включват точността и постоянството на данните в хода на целия им жизнен цикъл. Целостта на данните е важен елемент от дизайна, прилагането и използването на всяка система за данни, която съхранява, обработва или възстановява информация. Терминът има широк обхват и силно различаващи се значения, според конкретния контекст.

Worm (Червей)

Червеят представлява компютърна програма, която се инсталира в устройството на жертвата, след което търси начин да се разпространи към други компютри като нанася щети посредством изключване на части от мрежата

Blacklist (Черен списък)

Черен списък, списък с блокирани елементи или списък със забранени елементи представлява базов механизъм за управление на достъпа, който пропуска елементи като имейл адреси, потребители, пароли, адреси (URL), IP адреси, имена на домейни, файл хешове и т.н. през системата, с изключение на изрично посочените, за които достъпът е отказан.

Spyware (Шпионският софтуер (спайуер))

Шпионският софтуер (спайуер) представлява софтуер, инсталиран тайно в устройството на даден потребител с цел събиране на чувствителни данни. Шпионският софтуер тихомълком събира информация, като например данни за оторизация, и я изпраща извън мрежата към злонамерени лица. Шпионският софтуер често приема формата на безплатно за сваляне съдържание и се инсталира автоматично, с или без съгласието на потребителя.