dimension data

accelerate your ambition

Cybersecurity Intern Team

Dimension Data Dash

02 March 2020

Disclaimer: This is PI 1 and is still awaiting content review, so content may not be 100% accurate as of yet.

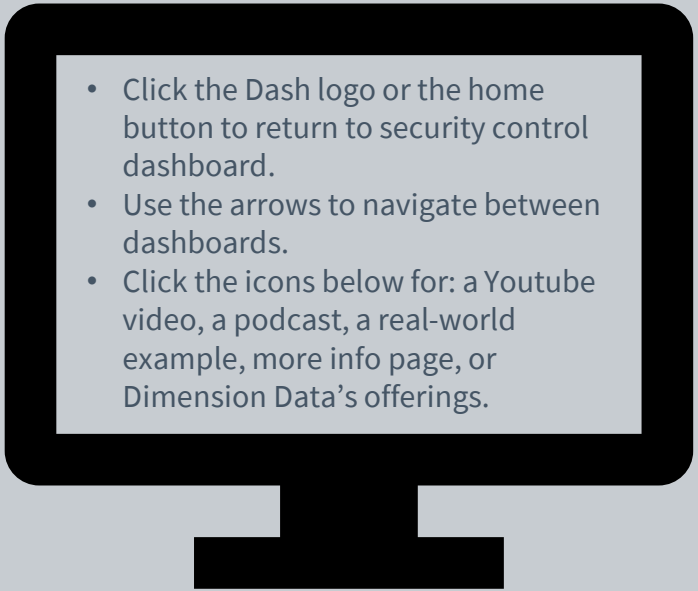
Name of Security Control

What is it?

This text here explains in simple terms what the security control is in such a way that a non-technical person will be able to understand it.

Why is it Important?

This text here explains why the security control is important to implement.



What is the risk?

This text here gives a brief and simple explanation of the risks associated with an absence of this particular security control.

Need more information?

Security Control Dashboard

4. Operations

- Access Management
- Asset / Config Management
- Change Management
- Event Monitoring and Management
- Incident Management
- Vulnerability / Patch Management
- GRC

3. Applications

1. Application Security

- CASB
- Vulnerability Management
- Application Security Testing
- API Security
- App Container Security
- App Control Whitelisting
- Application Sandboxing
- BAS
- RASP
- Source Code Analysis
- WAF

2. Data Security

- 1. DAM - DB Activity Monitoring
- DRM - Document Rights Management
- Data Encryption
- Data Masking
- PKI / Certificate Management
- Secure Collaboration and File Transfer
- Fraud Prevention & Transaction Security
- Host DLP
- FIM
- Data Discovery& Classification

2. Devices

Endpoint and Mobile Protection

- Antivirus / NGAV
- Asset / Secure Configuration Management
- EDR
- HIPS
- Remote Browser Isolation
- VDI Security
- MDM
- Patch Management
- Mobile Data Protection
- NAC

Identity & Access management

- SSO
- IAM
- Password Management
- AAA
- MFA
- PAM

1. Infrastructure

Infrastructure Protection

- CWP - Cloud Workload Protection
- Web Security
- DNS Security
- Messaging & Email Sec.
- Wireless Security

Network Security

- Firewall /NGFW / UTM / Segmentation
- Network IDPS
- VPN GW / (IPSEC & SSL)
- ETA – Encrypted Traffic Analysis
- Network DLP
- DDOS Protection

Threat Management

- Deception / Honeypots
- ATP
- SIEM
- TIP-Platform
- Threat Intelligence
- NBAD -Network Behaviour Anomaly Protection
- DRP -Digital Risk Protection
- Network Malware Sandboxing
- UEBA
- Network Packet Forensics
- SOAR – Security Automation, Orchestration & Response

5. Human

Access Management

What is it?

Access Management is a framework of policies and technologies designed to easily manage and control the access to assets by identities within a business.

Why is it Important?

It is important to control access to information, assets and processes by ensuring identities have the right privilege required for access in order to do the work of their role.

What is the risk?

Without access management processes, business critical assets and information can be compromised through loss, theft or damage when accessed by the wrong entities.

Need more information?

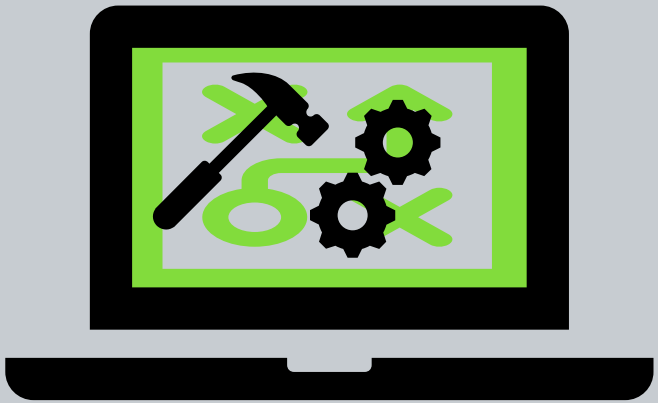
Asset / Config Management

What is it?

Asset and Configuration Management is the process of identifying, controlling and supporting IT assets throughout their lifecycle.

Why is it Important?

This process allows for accountability of IT assets and their configurations necessary for auditing and risk mitigation purposes.



What is the risk?

Without an Asset/config management process, assets can be incorrectly configured and present a compliance issue, regulation violation or a vulnerability in the asset that can be exploited.

Need more information?

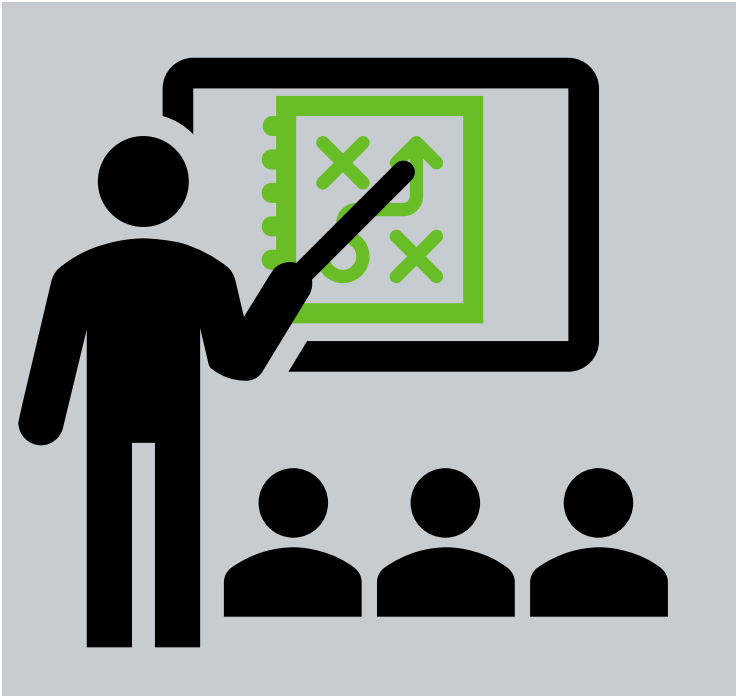
Change Management

What is it?

Change management is an organized approach to facilitate and control the transition or transformation processes within an organization.

Why is it Important?

It is important for undergoing effective and efficient change while reducing the negative impact that change has on people, processes and technologies.



What is the risk?

Without a change management strategy, transitional processes will cause disruptions to business operations, slow down the change process and assets being replaced could be lost.

Need more information?

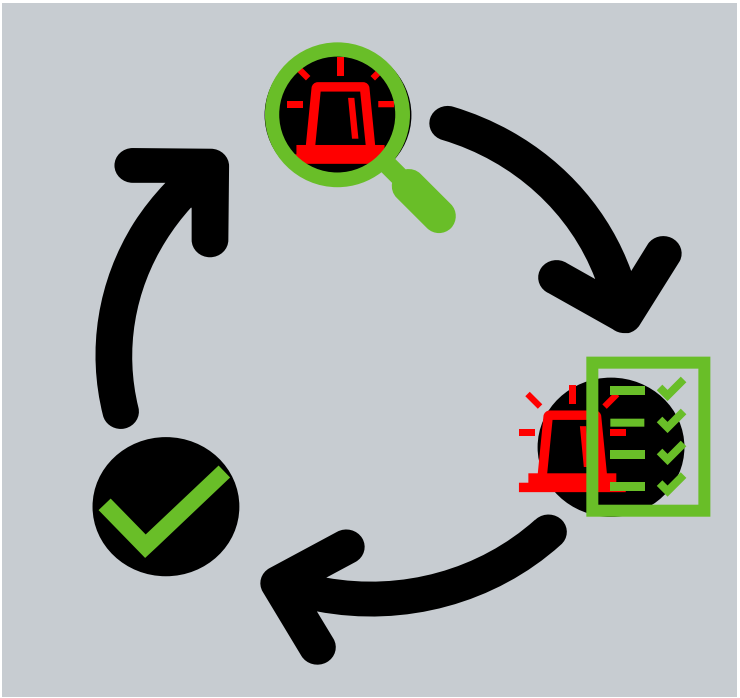
Event Management and Monitoring

What is it?

Event management and monitoring is the process of detecting, investigating and handling security events that impact IT systems.

Why is it Important?

This process aims to continually monitor events in order to categorize them so that they receive the appropriate action required.



What is the risk?

Without an Event Management and Monitoring process, critical events can go unnoticed or be incorrectly categorized, which can mean longer response times to repair systems impacted by events.

Need more information?

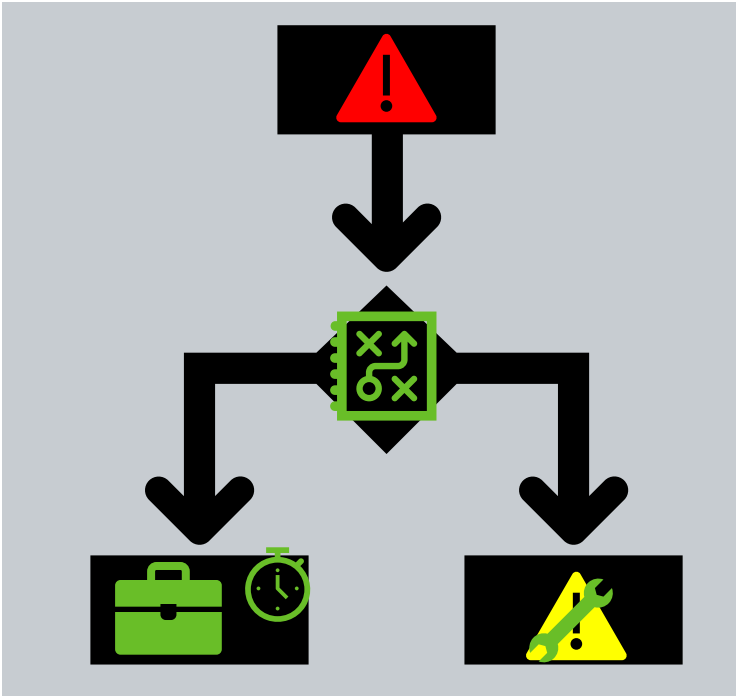
Incident Management

What is it?

Incident management is a process to mitigate and resolve incidents to help the organization successfully return to business operations.

Why is it Important?

This plan outlines a procedure to resolve and remediate incidents by reducing their impact and the time to recover from them.



What is the risk?

Without an incident management strategy, incidents could continue to damage the business's operations, its finances and its reputation if the incident is not resolved.

Need more information?

Vulnerability/Patch Management

What is it?

Vulnerability and Patch Management is the process of identifying, prioritizing and remediation of vulnerabilities.

Why is it Important?

This process allows companies to mitigate and reduce risks associated with their systems by patching vulnerabilities.

What is the risk?

Without a vulnerability and patch management process, systems with known vulnerabilities may not receive appropriate patching, potentially allowing these systems to be exploited.

Need more information?

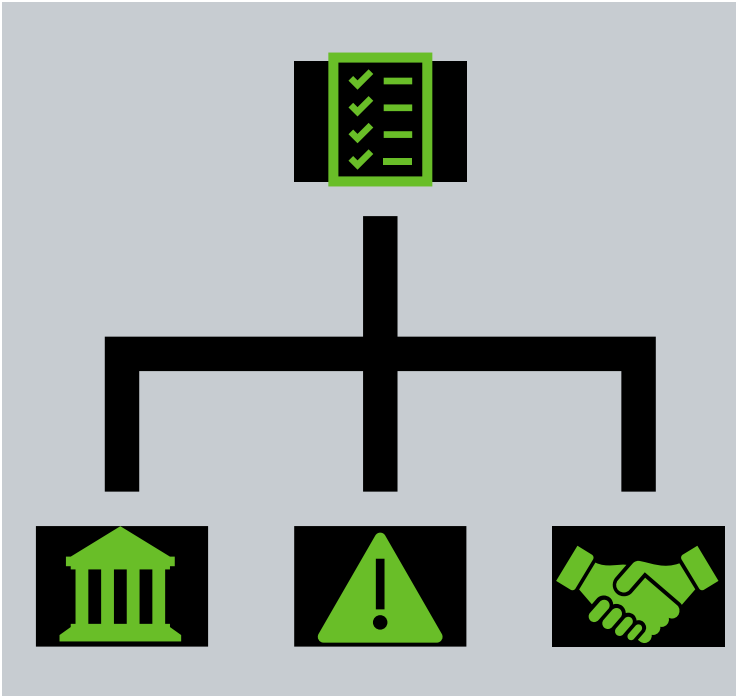
GRC – Governance, Risk, and Compliance

What is it?

Governance, Risk and Compliance refers to strategies that manage business operations overlapping between governance, risk and compliance.

Why is it Important?

It offers visibility into corporate governance responsibilities, risk management and being compliant with regulation requirements of business operations.



What is the risk?

Without a GRC plan, the regulations not met could incur fines for the business, while the reduced visibility into risks results in unnecessary remediation costs and without corporate governance there is an increase in inefficient business practices.

Need more information?

DAM - Database Activity Monitoring

What is it?

Database Activity Monitoring is the process of observing, logging, and analyzing activities occurring in a database in real-time.

Why is it Important?

DAM helps ensure that users with higher privileges are using database resources within the limits of their role and provides greater user accountability for auditing purposes.

What is the risk?

Without DAM, a database could be vulnerable to insider and outsider threats such as abuse of privilege, malware infections, and data exfiltration.

Need more information?

DRM - Document Rights Management

What is it?

Document Rights Management, also known as Information Rights Management, is a form of controlling read-write capabilities for a specific document.

Why is it Important?

This aids in protection of a file from unauthorized or illegal viewing, copying or editing.

What is the risk?

Without DRM, sensitive information could be stolen, changed, or viewed by unauthorized parties.

Need more information?

Data Encryption

What is it?

Data Encryption is a way of protecting information by converting it into an unreadable, unusable form which can only be unlocked by using a special key.

Why is it Important?

Data encryption allows the encryption of sensitive confidential information and protects it while in transit or at rest.

What is the risk?

Without Data Encryption, sensitive data could be read or used by unauthorized entities which could lead to a compromise in confidentiality of the information.

Need more information?

Data Masking

What is it?

Data Masking, also known as data obfuscation, is a way of hiding information by replacing it with similar but fake information.

Why is it Important?

It prevents unauthorized parties from viewing confidential information.

What is the risk?

Unmasked data increases risk of data leaks which could compromise personal information, intellectual property, and other confidential information. This could pose potential regulation and compliance issues.

Need more information?

PKI/Certificate Management

What is it?

Public Key Infrastructure/Certificate Management is the administering of certificate and public key pairs. This includes the issuing, maintaining, and revoking of the certificates.

Why is it Important?

This enables finer access control to information on the network and enables policy compliance through the use of certificates.

What is the risk?

Without PKI/Certificate Management, it could be difficult to revoke access in the event of a compromised device.

Need more information?

Secure Collaboration and File Transfer

What is it?

Secure Collaboration and File Transfer is the safeguarding of information while it's transit which is often done through encryption.

Why is it Important?

The workforce has become quite mobile and often works remotely which requires secure methods of sharing and collaborating on sensitive projects.

What is the risk?

If information is not transferred or shared securely then it is susceptible to interception by threat actors through Man-in-the-Middle attacks.

Need more information?

Fraud Prevention & Transaction Security

What is it?

Fraud Detection and Transaction Security is a set of activities that ensure the protection of sensitive information, such as banking and personal details, during transactions.

Why is it Important?

This helps to prevent the information from being intercepted and used fraudulently.

What is the risk?

Without Fraud Prevention & Transaction Security, user's banking account details could be stolen by threat actors which could lead to identity theft.

Need more information?

Host DLP – Host Data Loss Prevention

What is it?

Host Data Loss Prevention ensures that data is not removed or copied from a host without the correct authorization.

Why is it Important?

Host DLP helps maintain the confidentiality, integrity and availability of information within the business.

What is the risk?

Without Host DLP, insider threats could exfiltrate sensitive data such as personal information or intellectual property.

Need more information?

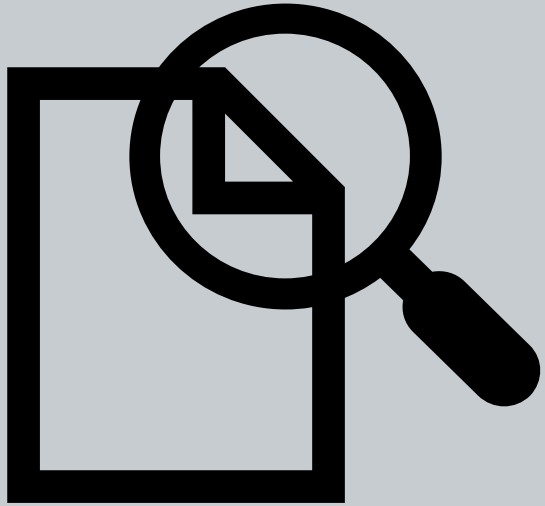
FIM – File Integrity Monitoring

What is it?

File Integrity Monitoring enables file changes to be tracked and logged in order to ensure that the file has not been tampered with.

Why is it Important?

It is important to preserve integrity of a file in order to ensure the creditability and usability of the information contained within.



What is the risk?

Without FIM, threat actors could access and change business files and it would be difficult to account for these changes as there would be no records of who changed what information and where it was changed.

Need more information?

Data Discovery & Classification

What is it?

Data discovery is the collection of data from multiple sources, such as databases, into a single place. Data Classification is the assignment of sensitivity levels to information to control access to it.

Why is it Important?

This is important in order to identify and analyse data from all sources into a single place so that it can be properly classified in order to ensure least-privilege access based on roles.

What is the risk?

If data isn't properly identified and classified then the confidentiality could be compromised by unauthorized users that have access to it. This could jeopardize personal information and trade secrets.

Need more information?

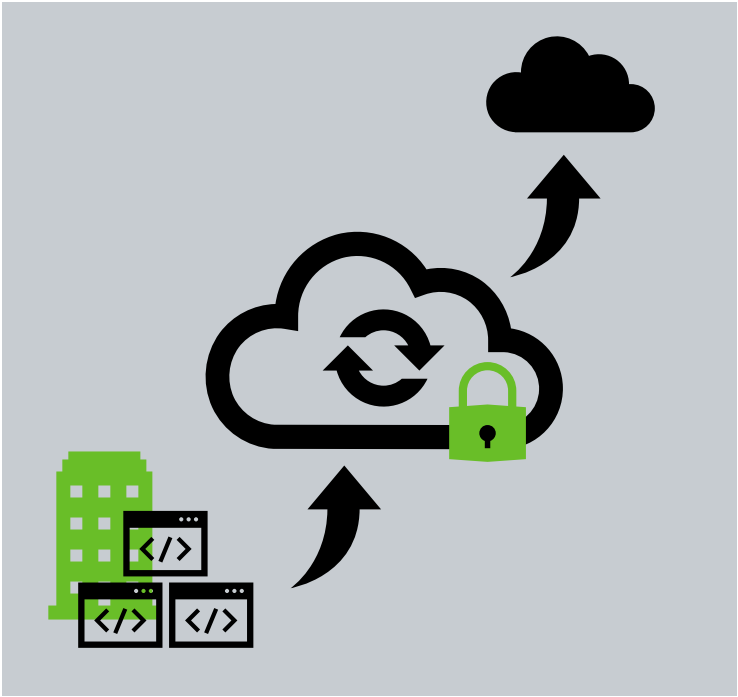
CASB – Cloud Access Security Broker

What is it?

A Cloud Access Security Broker is a tool that is used to regulate and monitor traffic between on-premise infrastructure and cloud services infrastructure.

Why is it Important?

It helps businesses ensure compliance with company policy with regards to cloud application usage and aids in identifying shadow IT operations.



What is the risk?

Without CASB, there is no visibility into how cloud applications are being used, meaning that shadow IT within the company's on-premise and cloud infrastructure can become an issue.

Need more information?

Vulnerability Management

What is it?

Vulnerability management is a proactive practice/process used within the IT field to identify and reduce potential vulnerabilities.

Why is it Important?

It's important to be aware of potential risk within your business's environment so that it can either be mitigated, or so that the identified risk can then be accepted.

What is the risk?

Without vulnerability management, IT vulnerabilities could be left unchecked in the business's environment which exposes the business to cyber attacks that could exploit them.

Need more information?

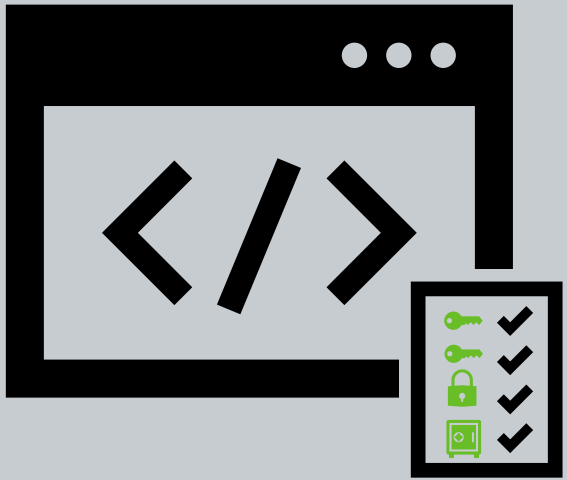
Application Security Testing

What is it?

Application Security Testing is the process whereby applications are checked and tested in order to identify potential flaws in their source code or execution.

Why is it Important?

This process helps identify vulnerabilities in an application which could be exploited by threat actors.



What is the risk?

Without regular Application Security Testing an application could be vulnerable to attack which opens up the company to risks including data exfiltration and unauthorized access.

Need more information?

API Security – Application Programming Interface Security

What is it?

API Security is a set of best practices that utilize authentication and authorisation methods in order to secure API's and prevent them from being misused or attacked.

Why is it Important?

API's are becoming more and more prevalent in web-based software development and thus are a big target for threat actors and need to be secured properly.

What is the risk?

If an API is not properly secured then it could be used by threat actors to bypass traditional authentication and authorisation methods in order to gain access to a web application or an environment.

Need more information?

App Container Security

What is it?

App Container Security is the protection of a container which includes the applications that it holds as well as the infrastructure that it relies on.

Why is it Important?

Containers have become quite popular methods of packaging and running applications and so it is important to ensure they are protected from attacks.

What is the risk?

Without securing your application containers there is a risk of the container being compromised potentially leading to unfettered access to business critical applications and data.

Need more information?

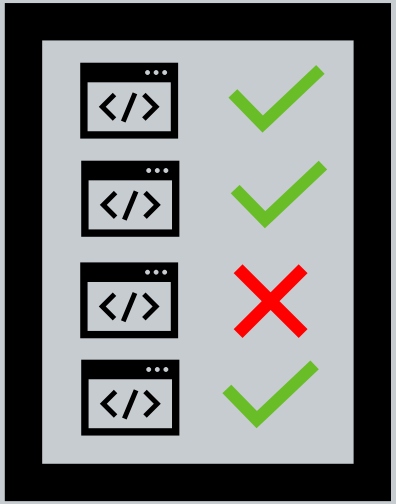
App Control Whitelisting

What is it?

An App Control Whitelist is a list of applications that a business allows to be used within their environment.

Why is it Important?

Whitelisting helps control which apps are being used by end users making it easier for a business to prevent the use of malicious apps or apps that violate policy.



What is the risk?

If app Control Whitelisting is not implemented then there is the risk for increased shadow IT within the business as well as the potential for unknown malicious applications to be run within the business environment.

Need more information?

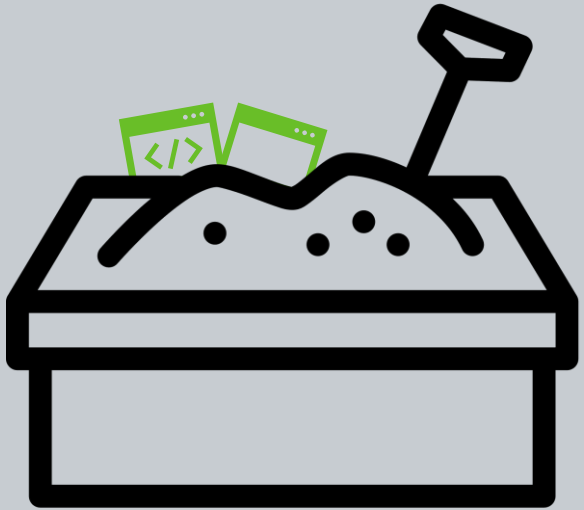
Application Sandboxing

What is it?

Application Sandboxing is the process of running an application in a contained environment in order to limit it's interaction with the outside environment.

Why is it Important?

This can be done to protect the app from outside malware influences or to test an application for suspected malicious behavior without compromising your entire system.



What is the risk?

Without application sandboxing an application could be vulnerable to attack or your network could be compromised by a malicious application which can lead to the spread of an infection and loss of sensitive business data.

Need more information?

BAS – Business Application Security

What is it?

Business Application Security, also referred to as Enterprise Application Security, is security that focuses primarily on securing business critical applications to protect them from attacks.

Why is it Important?

Businesses depend on certain applications for everyday operation so it is important to ensure that these applications are secure.

What is the risk?

Without BAS, business applications could be left vulnerable to attack by threat actors as most applications today have security flaws. BAS can help reduce the risk of a successful attack.

Need more information?

RASP - Runtime Application Self-Protection

What is it?

Runtime Application Self-Protection is a tool that enables an application to be monitored and protected when it executes.

Why is it Important?

RASP helps to protect vulnerable applications that do not have security built into their source code.

What is the risk?

Due to some applications not being secure they can be vulnerable to attacks when they are released or updated and without RASP it becomes difficult to detect and prevent these attacks.

Need more information?

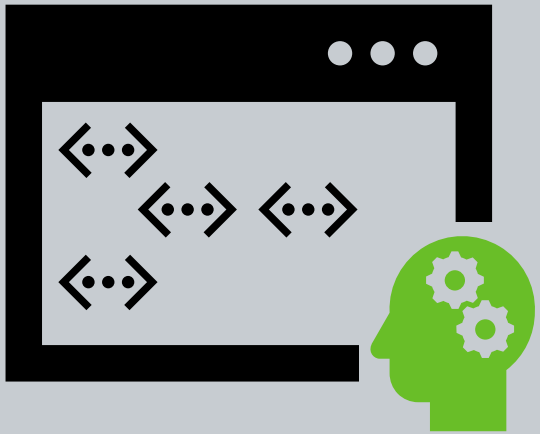
Source Code Analysis

What is it?

Source Code Analysis is the automated process of testing the code of a program or application in order to check it for errors before it is put into operation.

Why is it Important?

This analysis allows for issues to be identified and resolved before the application gets used and decreases the need for patching later on in the software's development lifecycle.



What is the risk?

If source code analysis is not done vulnerabilities and errors in the code might not be identified before the code is put into production and thus opens the application up to potential attacks by threat actors.

Need more information?

WAF – Web Application Firewall

What is it?

A Web Application Firewall is a firewall that monitors data sent to and from a web application or website. It can be used to filter or block the data and comes in both physical appliance and cloud application forms.

Why is it Important?

With the move to cloud computing and more web-based applications, data being transferred in these environments needs to be protected and continually monitored for threats.

What is the risk?

Business cloud applications are not well protected and thus are vulnerable to attack. A WAF can help decrease the risk of malicious traffic coming from or going to a business critical web application.

Need more information?

Antivirus/NGAV

What is it?

An antivirus is software used to prevent, detect and remove malware from endpoint devices.

Why is it Important?

Antiviruses check devices for known malware and can quarantine them, preventing malware spreading to other devices or the network.

What is the risk?

Without an antivirus, malware can damage business operations by compromising the endpoint, spread across the network infecting more devices and tamper with all the affected device's data.

Need more information?

Asset/Secure Configuration Management

What is it?

Asset Configuration Management is a system designed to ensure consistency amongst IT assets while monitoring and documenting their functions and interactions with other IT assets.

Why is it Important?

Documentation and tracking of assets reduces operational impact when changes occur, it supports audit and compliance efforts and facilitates the detection of shadow IT.

What is the risk?

Without Asset Configuration Management, inconsistent work environments, and out of date assets could make it difficult to manage incidents and overall reduce business operational efficiency.

Need more information?

EDR – Endpoint Detection and Response

What is it?

Endpoint Detection and Response is a system for protecting endpoints from threats by monitoring the network and endpoint.

Why is it Important?

EDR is able to respond in real-time to events to stop attacks from happening.

What is the risk?

Without EDR, malicious actors and malware could disrupt business operations, cause loss of data on the endpoint, or infect the network.

Need more information?

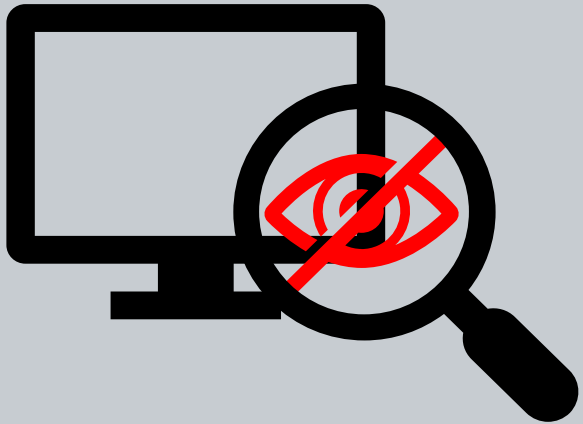
HIPS – Host Intrusion Prevention System

What is it?

Host Intrusion Prevention System is a system used to protect endpoints against known attack patterns of malicious activities by monitoring the endpoint for suspicious activity.

Why is it Important?

It builds on defence-in-depth by working with other security systems to ensure; endpoint protection by alerting, blocking and logging of malicious traffic activity.



What is the risk?

Without a HIPS, malicious attack signatures like malware can compromise and result in the loss of data on endpoints and a disruption of business activities.

Need more information?

Remote Browser Isolation

What is it?

Remote Browser Isolation is connecting to and using a virtual browser environment hosted in the cloud to browse the internet.

Why is it Important?

The remote browser is physically separate to the local network and is recreated every session, destroying any malware collected during its use.

What is the risk?

Without Remote Browser Isolation, malware and zero-day exploits can compromise the local browser and potentially lead to an infection spreading across the business network.

Need more information?

VDI Security – Virtual Desktop Infrastructure Security

What is it?

Virtual Desktop Infrastructure security is the securing of the technology that hosts virtual desktop operating systems.

Why is it Important?

VDI Security ensures the availability and integrity of virtual desktop environments and the data they store.

What is the risk?

Without VDI Security the desktop images, and data stored can be lost, compromised or damaged rendering them inaccessible.

Need more information?

MDM – Mobile Device Management

What is it?

Mobile Device management is software installed on mobile devices, such as smartphones and tablets, that enables the administration and control of these devices.

Why is it Important?

Personal mobile devices today contain work data. With MDM, IT services can enforce polices that ensure compliance, secure the device and prevent data exfiltration.

What is the risk?

Without MDM, compromised mobile devices can access the corporate network and can potentially cause the exfiltration of data.

Need more information?

Patch Management

What is it?

Patch Management is the process of controlling the roll out of patches for software and operating systems on endpoints.

Why is it Important?

Patch management creates a structured approach to remove known vulnerabilities and ensure system upkeep and hardening.

What is the risk?

Without Patch Management, patches being applied can create unscheduled downtime in systems or in the case of patches not being applied, create opportunities for vulnerabilities to be exploited.

Need more information?

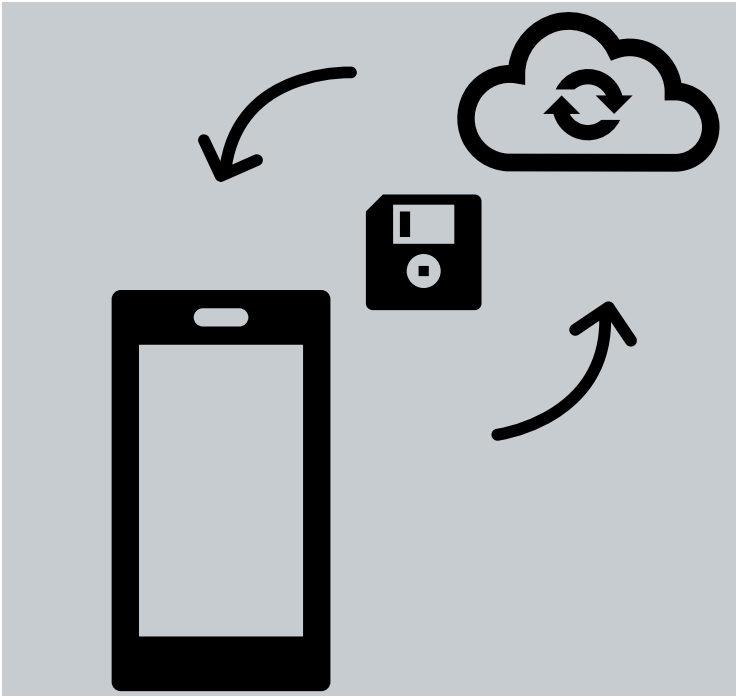
Mobile Data Protection

What is it?

Mobile Data Protection is a strategy to safeguard and ensure availability of important data stored on mobile devices, such as smartphones and tablets.

Why is it Important?

User's mobile devices can contain work-related information therefore they must be secure in order to maintain the confidentiality, integrity and availability of business information.



What is the risk?

Without Mobile Data Protection, the data on mobile devices can be corrupted, lost or compromised without a data back-up strategy.

Need more information?

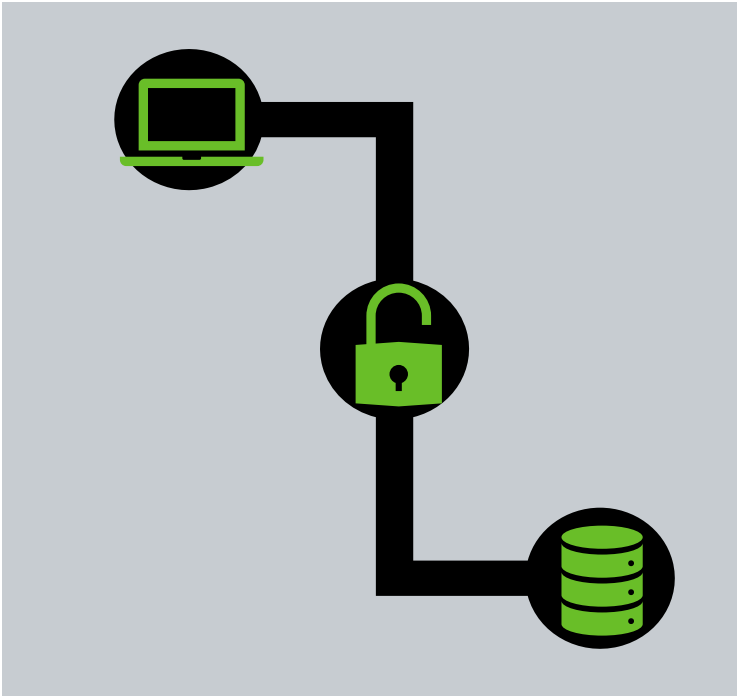
NAC – Network Access Control

What is it?

Network Access Control is a network system that authenticates and authorises an endpoint device allowing it to connect to the network.

Why is it Important?

NAC enforces compliance with security policies and ensures only authorised users have access to business resources.



What is the risk?

Without NAC, any unauthorized endpoint device could connect to the network, access its resources, and potentially compromise information.

Need more information?

SSO – Single Sign-on

What is it?

Single Sign-on is a form of access control whereby a single login credential is used to access multiple related accounts. This is also known as federated access.

Why is it Important?

It removes the need for multiple usernames and passwords for different sites which means they aren't stored on 3rd party servers.

What is the risk?

Without SSO, users will need to remember many different credentials and this may lead to them storing them unsafely. These credentials will also be stored on 3rd party servers which increases the potential attack surface for malicious actors.

Need more information?

IAM – Identity and Access Management

What is it?

Identity and Access Management is a tool that enables an IT department to better track and manage user identities within a digital environment from a centralized location.

Why is it Important?

IAM makes it easier to control account privileges across the business based on the roles of each identity. It is more consistent in enforcing authentication policies.

What is the risk?

If user identities are not properly managed then some users can gain higher access privileges than their roles allow which means they could access data they're not authorized to access.

Need more information?

Password Management

What is it?

Password management is a set of best practices including: changing passwords regularly, using unique passwords for different accounts, and keeping shared passwords confidential within the business.

Why is it Important?

Password management is important because passwords are the first line of defense when guarding your data and so they should be kept strong and up-to-date.

What is the risk?

Over time passwords that are not subject to password management practices become more at risk for being compromised by malicious actors who could then steal your company's data.

Need more information?

AAA – Authentication, Authorization, and Accounting

What is it?

Authentication, Authorization and Accounting refers to a set of processes that help monitor the usage of IT resources. Users must first be authenticated to gain access, then they must be authorized to perform specific actions and lastly the resources and time used by the user is accounted for and logged.

Why is it Important?

AAA ensures accurate usage monitoring, regular checks of user privilege levels, and it helps ensure compliance with company policy.

What is the risk?

Without AAA it cannot be ensured that users are performing efficiently and with the correct level of access and compliance which means less visibility into the usage of the business resources.

Need more information?

MFA – Multi-Factor Authentication

What is it?

Multi-factor Authentication is a method of confirming a user's identity via one or more additional identity checks. This includes something they know, they have, or they are.

Why is it Important?

MFA adds an extra layer of protection in case your password is obtained by somebody other than yourself and prevents them from accessing your account.

What is the risk?

People tend to use the same passwords for multiple accounts meaning that if one of them is breached then all accounts using the same passwords are vulnerable. Without MFA, a user's account is more vulnerable to attack as passwords can be easily gained by malicious actors who can then access a company's sensitive data.

Need more information?

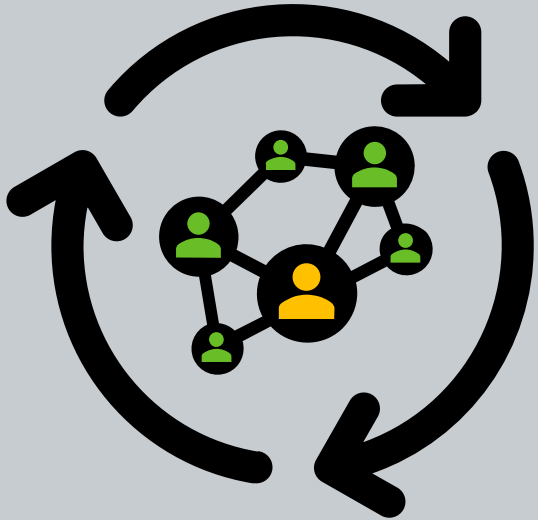
PAM – Privileged Access Management

What is it?

Privileged Access Management makes use of different technologies to secure and monitor the access of privileged business information. PAM is similar to Identity and Access Management but focuses primarily on privileged accounts (see IAM for more information).

Why is it Important?

Privileged accounts often have access to business critical information so it is important to secure them and know who is accessing them.



What is the risk?

Without PAM, there is less visibility into what privileged users are doing within the business making it harder to identify potential malicious activity.

Need more information?

CWP - Cloud Workload Protection

What is it?

Cloud Workload Protection adapts traditional on premise security to cloud Infrastructure as a Service in order to secure cloud based workloads.

Why is it Important?

CWP gives better visibility into cloud workloads allowing you to control and monitor issues related to them.

What is the risk?

It is a business's responsibility to secure their data stored in the public cloud and without CWP, data stored in the cloud is vulnerable to attack.

Need more information?

Web Security

What is it?

Web security is the process of securing the way a user accesses the internet.

Why is it Important?

Web security is important to prevent users from accessing unsafe, inappropriate or malicious sites.

What is the risk?

Without Web Security, users are at risk and may be subjected to web-based attacks that exploit the way they use the internet and mislead them or take them to malicious sites.

Need more information?

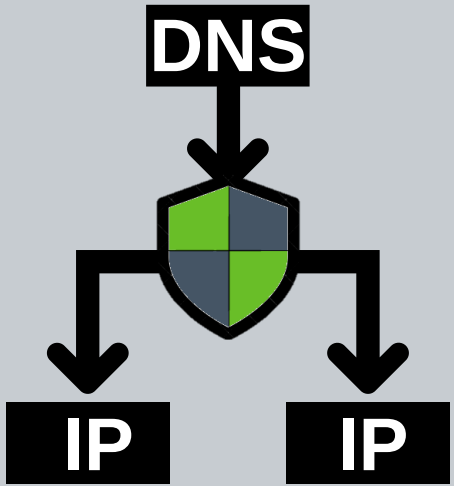
DNS Security - Domain Name System Security

What is it?

DNS security is the set of technologies used to protect the DNS service from being manipulated.

Why is it Important?

DNS is used whenever you use the internet therefore it is important to protect it from being exploited by threat actors.



What is the risk?

Without DNS security, the DNS service could be exploited to redirect users to malicious sites or launch attacks.

Need more information?

Messaging & Email Security

What is it?

Messaging & Email Security focuses on protecting the contents of an e-mail or message from being read by entities other than the intended recipients.

Why is it Important?

With the large amount of sensitive data that we send, receive, and store, it is important to secure the means of communication.

What is the risk?

Without Messaging & Email Security, messages sent can be read or altered in transit by third parties with malicious intent compromising the confidentiality and integrity of the data.

Need more information?

Wireless Security

What is it?

It is the prevention of unauthorized access or damage to computers or data using wireless networks.

Why is it Important?

Wireless connections are a preferred method of connecting to network access point thus they need to be secured.

What is the risk?

Without Wireless security, wireless networks could be exploited by threat actors to breach sensitive information.

Need more information?

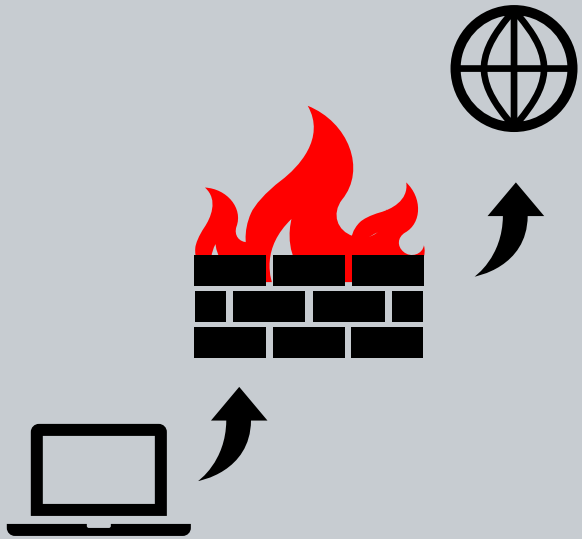
Firewall / NGFW –Next Generation Firewall

What is it?

A Firewall protects a network from unauthorized access and malicious activity based on security rules that it applies to network traffic and can be deployed as both a hardware unit or a software solution. A Next Generation Firewall provides multiple capabilities beyond that of a regular Firewall.

Why is it Important?

Every business has an internal network which connects to external networks and the internet and thus need protecting at a network traffic level from threats.



What is the risk?

Without a Firewall solution, the business network is directly exposed to external network threats and the most common of malicious attacks such as, trojans, worms, and viruses.

Need more information?

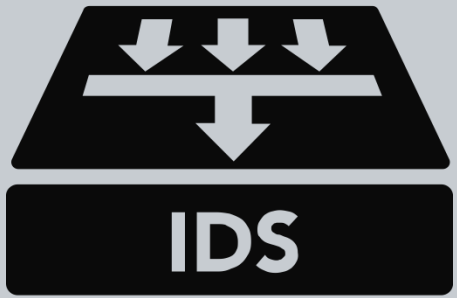
Network IDPS – Intrusion Detection and Prevention System

What is it?

Network IDPS – Intrusion Detection and Prevention Systems monitor inbound and outbound network communications and report or possibly block suspicious activity.

Why is it Important?

It aids in securing and detecting malicious activity on the network. It also helps ensure that internal users adhere to policies.



What is the risk?

Without Network IDPS, it could be difficult to monitor and react to network level activity in real-time in order to determine whether or not it is malicious.

Need more information?

VPN GW – Virtual Private Network Gateway

What is it?

A Virtual Network secures the communications transmitted from an external network to the internal network over an internet connection.

Why is it Important?

A VPN helps preserve confidentiality of actions and secures any sensitive information being accessed over a public internet connection.

What is the risk?

Without a VPN, the connection is susceptible to eavesdropping and other man-in-the-middle attacks by threat actors who may be monitoring vulnerable public internet connections.

Need more information?

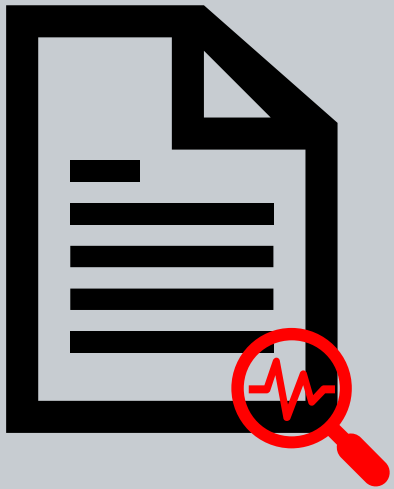
ETA – Encrypted Traffic Analysis

What is it?

Encrypted Traffic Analysis allows the inspection of network traffic without the need for decryption in order to check it for malicious activity or signatures.

Why is it Important?

Most of the traffic on the internet has become encrypted increasing the need for ETA which provides a higher level of privacy in order to comply with privacy regulations while still protecting a business from malicious activity.



What is the risk?

Without ETA, a malicious payload could be delivered via an encrypted channel to a business network infecting it the moment that traffic is decrypted.

Need more information?

Network DLP – Network Data Loss Prevention

What is it?

Network Data Loss Prevention is a set of technologies that ensure data is transferred over the network securely and is not lost or leaked via any of the different methods of communication that a business may use.

Why is it Important?

Businesses communicate primarily through network communication so it is important to protect information transferred using these channels.

What is the risk?

Network DLP can help prevent accidental disclosure, theft by employees having access to sensitive data, and preserves the confidentiality of the information.

Need more information?

DDoS Protection - Distributed Denial-of-Service Protection

What is it?

A Distributed Denial of Service attack reduces the availability of system or service and prevents users from accessing them. DDoS protections helps prevent these attacks from happening ensuring system/service availability.

Why is it Important?

DDoS Protection makes a system/service more robust thus ensuring availability to users and also delivers benefits such as monitoring and detection.

What is the risk?

Without DDoS Protection, a business's critical systems or services that it provides could be taken down which could decrease productivity of users and affect customer's satisfaction levels.

Need more information?

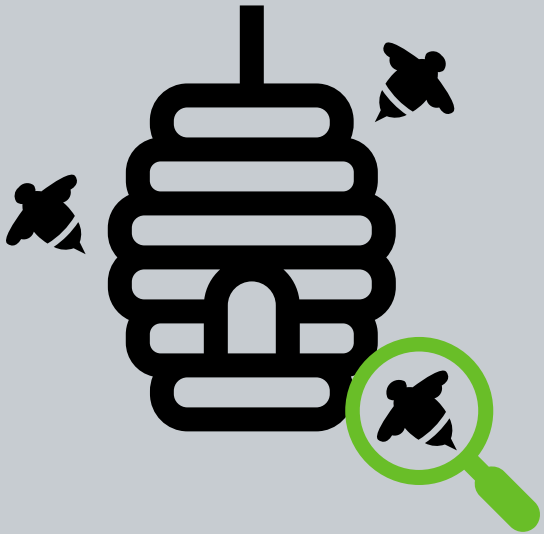
Deception / Honeypots

What is it?

It is an isolated replication of the environment that threat actors are targeting.

Why is it Important?

Threat actors believe that they have achieved access allowing us to observe how threats would act inside the environment .



What is the risk?

Without Honeypots, there is no visibility into how threat actors could access a business's network or what they were targeting.

Need more information?

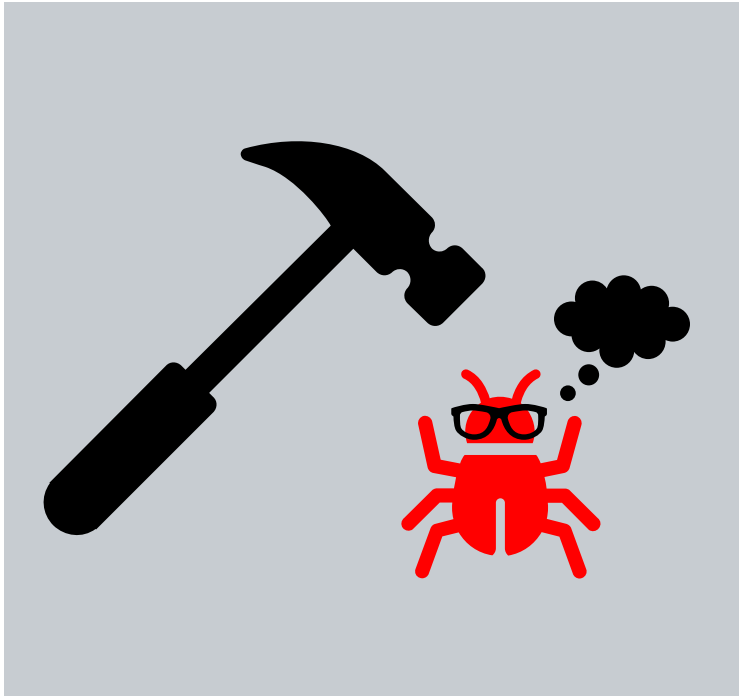
ATP – Advanced Threat Protection

What is it?

A collection of security solutions that defend against sophisticated malware or hacking-based attacks.

Why is it Important?

It is able to proactively handle more complex threats with little to no human assistance.



What is the risk?

Without ATP, a business is more vulnerable to the ever-changing threat landscape and which is why it requires a more flexible and advance treat protection solution.

Need more information?

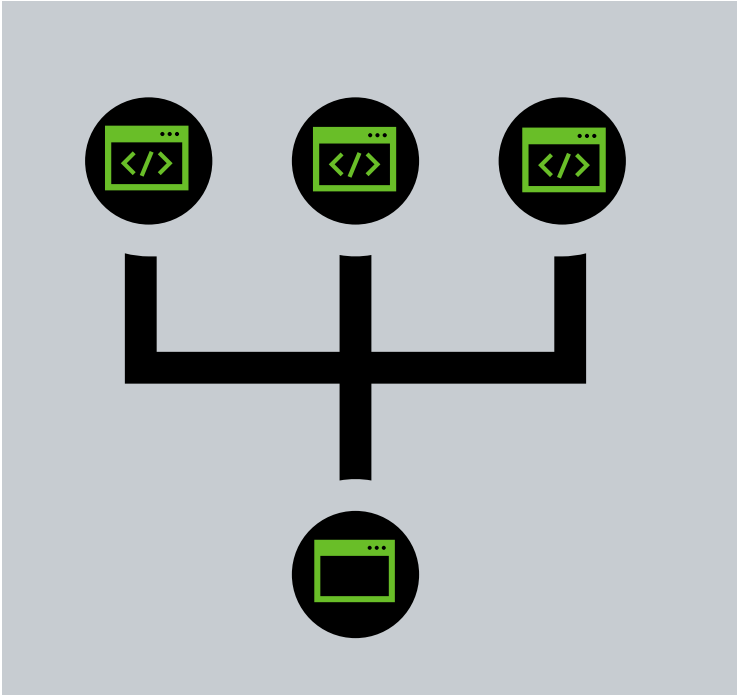
SIEM – Security Information & Event Management

What is it?

A SIEM collects data from multiple sources in a centralized location to make them easier to analyse.

Why is it Important?

Businesses are able to analyse the collected data and better identify events and potential threats.



What is the risk?

Without a SIEM, it is difficult to correctly identify how security incidents occur due to the large number of security solutions producing log files.

Need more information?

TIP – Threat Intelligence Platform

What is it?

Threat Intelligence Platforms can be utilized as a SaaS, Software as a Service, or on-premise solution to give businesses insight into what threats are in their environment.

Why is it Important?

It gives the ability to allocate resources effectively in order to address the most crucial threats within the environment.

What is the risk?

Without TIP, businesses are unable to effectively use threat intelligence to defend their environment from new, old, and evolving threats.

Need more information?

Threat Intelligence

What is it?

Threat intelligence is organized, analyzed and refined information about potential/current attacks that threaten an business.

Why is it Important?

Threat intelligence provides businesses with the information necessary to mitigate and prevent potential threats.

What is the risk?

Without threat intelligence, the current threat landscape is unknown, which makes it difficult to secure the business IT environment.

Need more information?

NBAD - Network Behaviour Anomaly Detection

What is it?

Network Behaviour Anomaly Detection continuously monitors network traffic for abnormal or threatening behaviour.

Why is it Important?

It is able to detect threats using more than just their predefined signatures even when traffic is encrypted.

What is the risk?

Without NBAD, businesses will not be able to detect threats if network traffic is encrypted and won't be able to identify threats that don't have existing signatures.

Need more information?

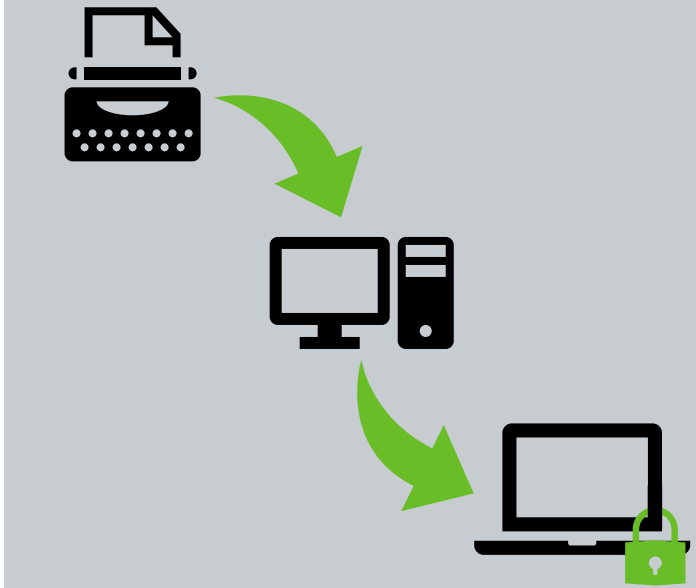
DRP - Digital Risk Protection

What is it?

Digital Risk Protection reduces risks that emerge from digital transformation such as upgrading or utilizing new technology and software within the business.

Why is it Important?

Companies are adopting more digital processes to conduct business, this increases the attack surface and creates opportunities for risk that needs to be mitigated.



What is the risk?

Without DRP, Businesses undergoing digital transformations are vulnerable to potential exploits in new digital processes these process increase the attack surface.

Need more information?

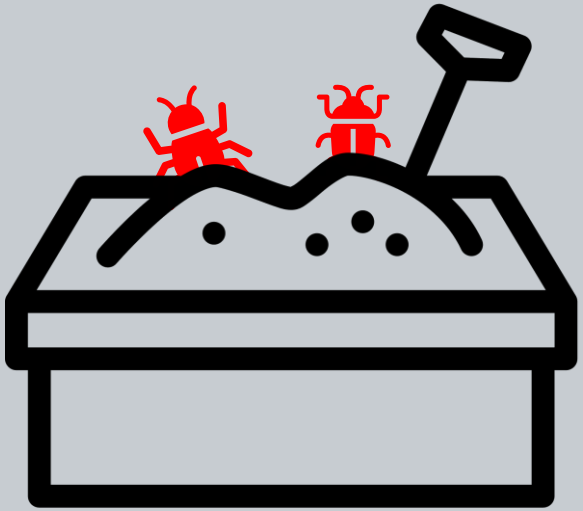
Network Malware Sandboxing

What is it?

Network Malware Sandboxes monitor network traffic for suspicious objects and automatically submit them to the sandbox environment for inspection and analysis.

Why is it Important?

Sandboxing prevents zero day threats, provides context for future attacks and integrates well with existing security programs



What is the risk?

Without network malware sandboxing, new malware that's not yet recognized by existing security programs is able to enter the network undetected and execute.

Need more information?

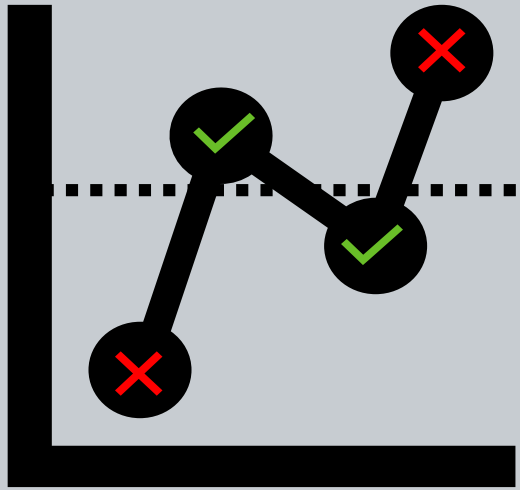
UEBA - User and Entity Behavior Analytics

What is it?

User and Entity Behavior Analytics is a process that establishes a baseline for normal conduct of users and then detects any abnormal behavior or deviations from the baseline.

Why is it Important?

It tracks all user and entity behavior when using company resources to identify possible threats.



What is the risk?

Without UEBA, threats such as rogue employees or compromised users are more difficult to identify due to a lack of visibility into business resource usage.

Need more information?

Network Packet Forensics

What is it?

Network packet forensics is the capture and analysis of network packets in order to determine the source of network security attacks.

Why is it Important?

This is important for monitoring a network for abnormal traffic, identifying intrusions and detecting malware while it is still in transit.

What is the risk?

Without Network Packet Foresnics, a network intrusion could go undetected as threat actors may be able to obfuscate their activity on the network.

Need more information?

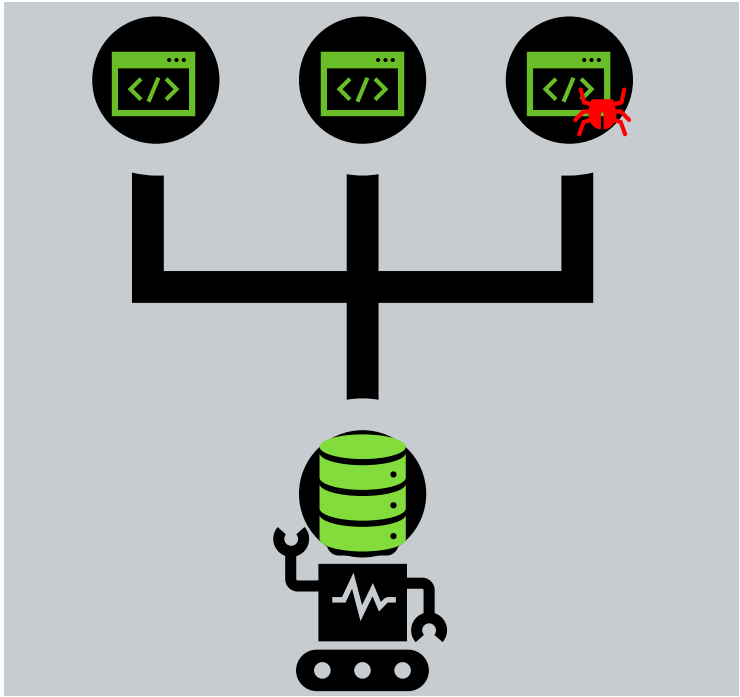
SOAR – Security Automation, Orchestration & Response

What is it?

Security Automation, Orchestration & Response is a collection of software programs that enable a business to collect data about threats from multiple sources and respond to low-level security events without human assistance.

Why is it Important?

Security teams do not have enough people to deal with every possible threat given the constant increase in the number of threats.



What is the risk?

Without SOAR, yber security teams would not be able to keep up with the vast number of threat alerts making it easier for security incidents to be overlooked.

Need more information?