Day1 of Internship

- **Introduction**

This documentation provides an overview of the key learnings undertaken during the day 1 of internship. It focuses on understanding the role of **ApexaiQ, IT asset management,** and **cybersecurity** in modern organizations. The aim is to explore important industry concepts, and gain practical insights into managing IT assets, ensuring compliance, and securing enterprise systems.

- **What does ApexaiQ do? What problems does it solve?**

ApexaiQ is a product-based SaaS platform that helps organizations manage their IT assets with accuracy and ease. It delivers clean, trusted data, uncovers shadow IT, and tracks all company assets while checking their security and compliance status. Each asset is given an Apexa Score that highlights its risk level, making it easier to prioritize fixes and stay audit-ready. By doing so, ApexaiQ enables businesses to find, fix, and report issues before they turn into real risks.

It solves problems such as unknown or unmanaged IT assets, hidden security vulnerabilities, and compliance gaps. It also eliminates the inefficiency of manual tracking and provides real-time visibility into the IT environment. With ApexaiQ, organizations can confidently manage IT operations, strengthen security, and ensure compliance in a simple, structured way.

Source: https://www.apexaiq.com/solutions/

- **What is IT asset management and why companies need asset management software?**

IT Asset Management (ITAM) manages and maintains an organization's hardware, software, and other technology-related assets throughout its lifecycle. ITAM involves tracking IT assets' acquisition, deployment, usage, maintenance, and disposal to ensure that they are used efficiently and cost-effectively. ITAM is an essential process for organizations that rely heavily on technology to operate their business. Effective ITAM can help to reduce costs, increase productivity, minimize risks, and improve compliance with regulatory requirements.

Companies need asset management software due to the following reasons:

Improved performance: ITAM helps organizations improve their overall performance by ensuring their IT assets are optimized and working efficiently. By tracking the lifecycle of IT assets, organizations can identify assets that are no longer useful and replace them with newer, more effective solutions. Additionally, ITAM can help identify and resolve software conflicts, improve system reliability, and reduce downtime.

Increased security: ITAM helps improve an organization's security by ensuring that all IT assets are properly tracked and managed. By maintaining an accurate inventory of IT assets, organizations can identify potential security risks and vulnerabilities. It can help them take proactive measures to address these issues before they become more severe security threats.

Reduced costs: ITAM helps organizations reduce their IT costs by optimizing their IT asset usage and avoiding unnecessary expenditures. By tracking the lifecycle of IT assets, organizations can identify assets that are underutilized or no longer needed and dispose of them properly. It can help reduce maintenance and support costs and eliminate the need for additional software licenses and hardware.

Asset visibility: ITAM provides organizations with better visibility into their IT assets, enabling them to track and manage them more effectively. This visibility is essential because it allows organizations to know what they have, where it is, and how it's being used. By understanding what assets they have and how they're being used, organizations can make better decisions about their IT investments and ensure that their assets are being used to their full potential.

Improved budgeting: By providing better visibility into IT assets, ITAM also allows organizations to budget more accurately. ITAM helps organizations understand the total cost of ownership of their IT assets and how those costs are distributed across different departments and locations. This information is valuable when it comes to budgeting for IT expenses, as it allows organizations to allocate resources more effectively and make better decisions about replacing or upgrading assets.

Automation: ITAM helps automate many of the manual processes involved in asset management. For example, ITAM software can automatically discover and inventory IT assets, track asset ownership and location changes, and generate reports on asset usage and performance. Automation not only saves time and reduces the risk of errors but also enables organizations to make more informed decisions about their IT assets by providing real-time data.

Analytics: Collecting, analysing, and interpreting data is essential to gain insights and make informed decisions. With ITAM software, organizations can collect data on their IT assets, such as hardware and software inventory, license information, and usage data. This data can then be analysed to identify trends, patterns, and potential issues, such as over or underutilized assets, license compliance issues, and security risks.

Reporting: ITAM software can generate a variety of reports, such as hardware and software inventory reports, license compliance reports, usage reports, and cost reports. These reports can be used by IT managers, procurement managers, and other stakeholders to make informed decisions about asset management, budgeting, and resource allocation.

Source: https://infraon.io/blog/importance-of-it-asset-management/

- **3-5 competitors of Apexaiq and how they are different from Apexa. Case studies.**

Vicarius provides vulnerability remediation and management solutions in the cybersecurity field. The offerings include patching, protection, and remediation for applications, operating systems, and third-party software. The company serves sectors including manufacturing, finance, government, healthcare, and education. It was founded in 2016 and is based in Jerusalem, Israel.

Source: https://www.cbinsights.com/compare/apexa-iq-vs-vicarius

Nanitor is a company focused on Continuous Threat Exposure Management (CTEM) in the cybersecurity domain. Its main offerings include a platform that provides visibility, prioritization, and management solutions for IT infrastructure security, such as asset inventory, remediation guidance, compliance reporting, and health scoring. The company serves sectors that require strong cybersecurity measures, including global companies with complex IT environments. It was founded in 2014 and is based in Reykjavik, Iceland.

Source: https://www.cbinsights.com/compare/apexa-iq-vs-nanitor

CloudWize provides cloud security and compliance solutions across various domains. The company offers a platform for threat monitoring, misconfiguration detection, and

compliance risk management for cloud environments. CloudWize serves sectors that require cloud security measures, such as the technology and cybersecurity industries. It was founded in 2019 and is based in Netanya, Israel.
Source:https://www.cbinsights.com/compare/apexa-iq-vs-cloudwize-1

Bionic develops an application security posture management platform. It helps in the reduction and mitigation of security, data privacy, and operational risks by analyzing an application architecture. The platform works across all environments, from on-premises monolithic applications to hosted cloud-native microservices, and is completely automated. It was founded in 2019 and is based in Palo Alto, California. In September 2023, Bionic was acquired by CrowdStrike.

Source:https://www.cbinsights.com/compare/apexa-iq-vs-bionic-2

Axonius is an asset management platform. Serving as a central hub, Axonius aggregates and normalizes security data from over 1.1K diverse business, IT, and security sources via APIs as of February 2025. By leveraging adapter-based data collection and graph-based mapping, Axonius provides a unified view of an organization's entire asset landscape—including endpoints, cloud services, and SaaS applications—while automatically identifying security gaps and enforcing policies. Rather than replacing specialized security tools such as endpoint protection, firewalls, or vulnerability scanners, Axonius complements them by offering an overarching analysis of the overall security posture.

Source: https://research.contrary.com/company/axonius

- **Why is ApexaiQ an agentless platform?**

Agent-based IT Asset Management refers to a method of managing and tracking software and hardware assets by deploying agents that collect real-time data. This approach excels in providing granular insights, enhancing compliance, and optimizing resource utilization. The ultimate goal is to use the data they extract to map the IT infrastructure and create an up-to-date asset inventory. This depth of detail empowers better decision-making and operational efficiency, distinguishing agent-based ITAM from agentless approaches.

Agentless IT Asset Management consists of managing and tracking software and hardware assets through network scanning and remote data collection techniques to gather information about the assets.In ITAM, "agentless" means that there are no dedicated software agents installed on individual devices to collect asset data. Instead, the ITAM system interacts with the devices remotely, leveraging network protocols, APIs (Application Programming Interfaces), or other methods to obtain information.

Agentless ITAM focuses on gathering data from network endpoints and infrastructure devices:

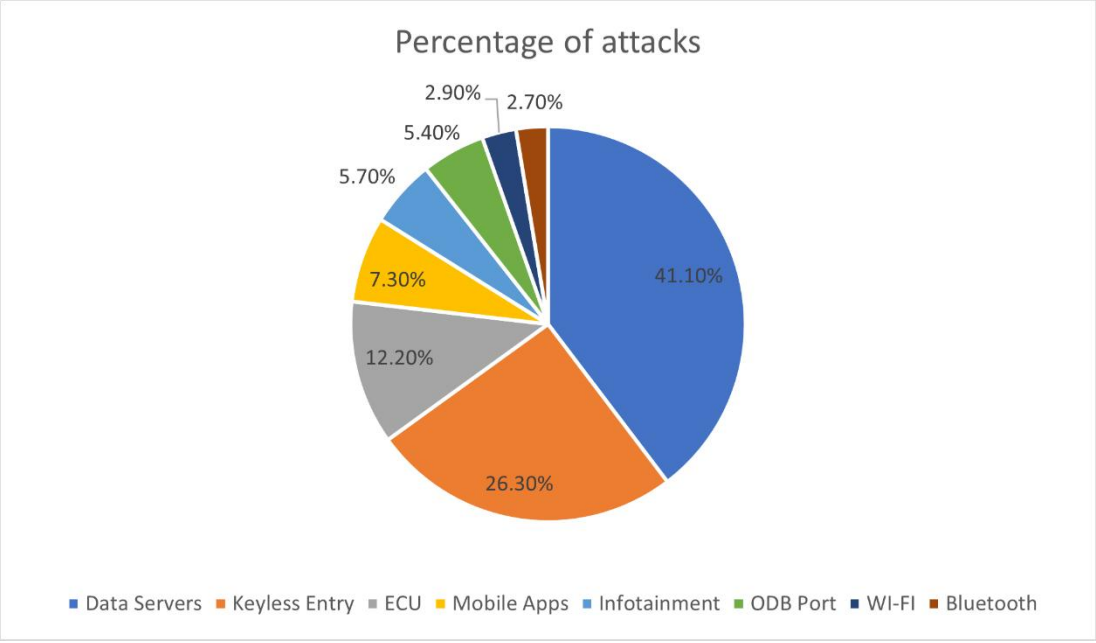
- Servers.
- Network switches.
- Routers.
- Storage systems.
- Printers.
- Scanners.
- IoT devices.

Source: https://blog.invgate.com/agent-vs-agentless

Without the need to install agents on each device, ApexaiQ can be deployed quickly across your entire IT environment. By eliminating the need for additional software on devices, It reduces potential attack vectors, enhancing overall security.and hence, ApexaiQ is said to be agentless.

- **Research on Cybersecurity.**

Research Paper: https://ijrpr.com/uploads/V5ISSUE4/IJRPR24628.pdf



- **Some Concepts**

ApexaiQ Score

ApexaiQ is a SaaS based platform that delivers your IT Risk Score, asset Compliance, Obsolescence, Maintenance and Vulnerability in a single dashboard.
In this dashboard, we give you a quantified and an actionable summary of your internal IT. This score, your Apexa iQ, is inspired by human IQ and ranges between 60 (poor) to 160 (genius)

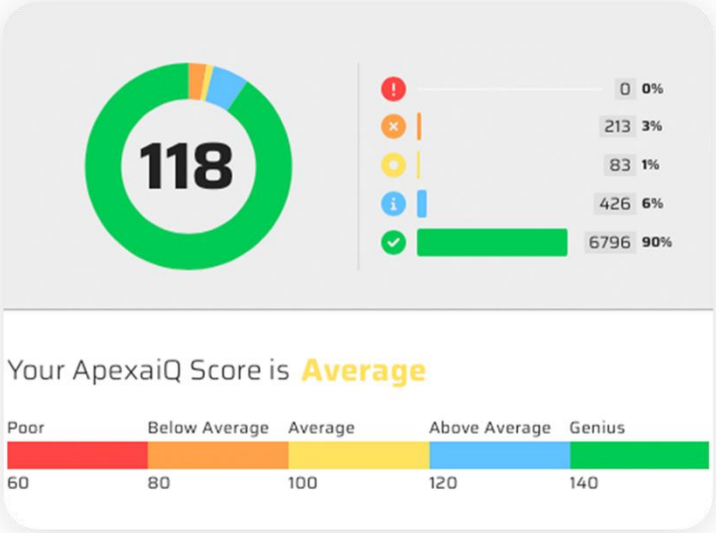
.ApexaiQ score, is inspired by human IQ and ranges between 60 (poor) to 160 (genius). It is like a credit rating for your entire IT estate, including every device on your network.

Your Apexa iQ is like a credit rating for your entire IT estate, including every device on your network. It computes all your risks and security gaps into a single score, based on the most vital obsolescence and compliance factors. The higher the score, the stronger and more secure your IT environment.

The score is calculated based on 3 different things:

1. IT Environment
2. Asset Hygiene - Obsolescence, Maintenance, Vulnerabilities
3. IT Gaps

Source: https://www.apexaiq.com/welcome-to-apexaiq/



IT Asset Management

IT asset management (ITAM) is a process that ensures an organization's IT assets—both tangible and intangible—are tracked, deployed, maintained, and eventually retired. It integrates financial, inventory, and contractual data to optimize asset value throughout the asset lifecycle. Assets have a limited amount of time for use, and an organization can maximize their value with ITAM and proactive management. ITAM is a practice that tracks and manages IT assets throughout their lifecycle, ensuring they are deployed efficiently, maintained properly, and retired responsibly. Phases of the lifecycle generally include planning, procurement, deployment, maintenance, retirement, and disposal.

ITAM encompasses several categories designed to optimize and control different types of assets within an organization. Each type plays a crucial role in ensuring assets are tracked, utilized efficiently, and managed to minimize risk and cost:

Software asset management involves tracking and optimizing the acquisition, licensing, and usage of software applications.

Hardware asset management focuses on physical IT equipment, such as servers, laptops, mobile devices, and network hardware.

Cloud asset management oversees cloud-based services and resources, including software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS). This type of ITAM helps organizations monitor cloud service consumption, manage costs, and ensure compliance with cloud provider agreements.

While ITAM focuses on IT-specific assets, related fields like fixed asset management, (also known as enterprise asset management or EAM), track broader physical assets within an organization. These include items like office furniture, network cabinets, and server room air conditioning units. Although not strictly IT assets, they are often managed by IT teams when they directly support IT infrastructure.

Source: https://www.servicenow.com/products/it-asset-management/what-is-itam.html

Vulnerabilities

A vulnerability in cybersecurity refers to a weakness or flaw in a system, network, application, or even human behaviour that attackers can leverage to compromise the security posture. These weaknesses can exist in hardware, software, configurations, or procedures. When exploited, vulnerabilities can allow attackers to:

- Gain unauthorized access: Hackers can exploit vulnerabilities to bypass security controls and gain access to sensitive systems or data.
- Install malware: Malicious software can be introduced into a system through vulnerabilities, allowing attackers to steal data, spy on activity, or launch further attacks.
- Disrupt operations: Denial-of-service (DoS) attacks can exploit vulnerabilities to overwhelm systems with traffic, rendering them unavailable to legitimate users.
- Escalate privileges: Attackers can exploit vulnerabilities to gain higher levels of access within a system, allowing them to move laterally and compromise more critical assets.

Types of Vulnerabilities:

1. **Software Vulnerabilities:** These vulnerabilities reside within the code of applications or operating systems. They can arise from various factors, including Programming Errors, Insecure Coding Practices and Outdated Software.
2. **Hardware Vulnerabilities:** While less common than software vulnerabilities, weaknesses in hardware components can also be exploited. These vulnerabilities can be Design Flaws, Manufacturing Defects and Firmware Bugs.
3. **Network Vulnerabilities:** Weaknesses in network configuration or protocols can create entry points for attackers. Common examples include Unpatched Network Device Unsecured Wireless Networks and Misconfigured Firewalls.
4. **Procedural Vulnerabilities:** These vulnerabilities stem from weaknesses in organizational policies and procedures related to security. Examples include Weak Password Policies, Lack of Employee Training.

Source: https://thecyberexpress.com/what-are-vulnerabilities/

Obsolescence

Obsolescence is the process of becoming antiquated, out of date, old-fashioned, no longer in general use, or no longer useful, or the condition of being in such a state.

Source: https://en.wikipedia.org/wiki/Obsolescence

Technological obsolescence occurs when your equipment, software, or systems can no longer meet operational or industry requirements because newer technology or standards have taken their place. This challenge is driven by the rapid pace of innovation, updated compliance requirements, and changing integration needs.

Unlike physical wear or scheduled end-of-life, technological changes often trigger component obsolescence, meaning parts become outdated even if they still work. As a result, components may no longer connect, protect, or perform as required in modern industrial settings, creating risks for system reliability and ongoing operations.

Source: https://www.amplio.com/post/technological-obsolescence

Compliance

compliance is the process of verifying whether the organization follows certain rules standards. This involves building certain guidelines in which the data should be collected stored and used. Security compliance is one of the critical components of any business's cyber security strategy since it helps to protect customer data from falling into the wrong hands while ensuring that businesses follow laws and regulations. Cybersecurity compliance is the rules that are implemented to protect the confidentiality, integrity, and availability of data which means safeguarding the data by following the principles.

These rules are enforced by governments, law authorities, and industry leaders. These standards may vary from industry to industry and in terms of organizational size. These standards are difficult to follow but it helps in protecting the organization. compliance standards safeguard sensitive personal information and product details protecting the employee's and customer's data and also improving the organization's fame, and customer trust.

Source: https://www.geeksforgeeks.org/computer-networks/what-is-cyber-security-compliance/

Maintenance

Maintenance, otherwise known as technical maintenance, refers to a set of processes and practices that aim to ensure the continuous and efficient operation of machinery, equipment, and other types of assets typically used in business.

Source: https://safetyculture.com/topics/maintenance

Software maintenance is a crucial phase of the Software Development Lifecycle (SDLC), ensuring that a system continues to perform optimally after deployment. Moreover, in this dynamic environment, user expectations, security standards, and technology ecosystems evolve constantly, making software maintenance more important.

Source: https://www.mindinventory.com/blog/what-is-software-maintenance/

End of Life, End of Support, End of Maintenance

End-of-Life (EOL) is the last phase in the life cycle of a product. This can affect electronic products, components and software that are no longer produced by the manufacturer. They are therefore no longer available, but can still be used without any problems. The support offer remains in place. In electromechanics, EOL describes the phase from the transition from series production to discontinuation, in which only small quantities of spare parts are produced. As series and supplier companies are often no longer able to produce these quantities cost-effectively, an external service provider often takes over production.

End-of-Support (EOS), “End-of-Service”, or “End-of-Sale”. The latter is the discontinuation of a product, similar to EOL. From this point on, the product is no longer offered by authorized dealers or directly by the manufacturer. It is very important to recognize the difference between all these terms in order to avoid misunderstandings.

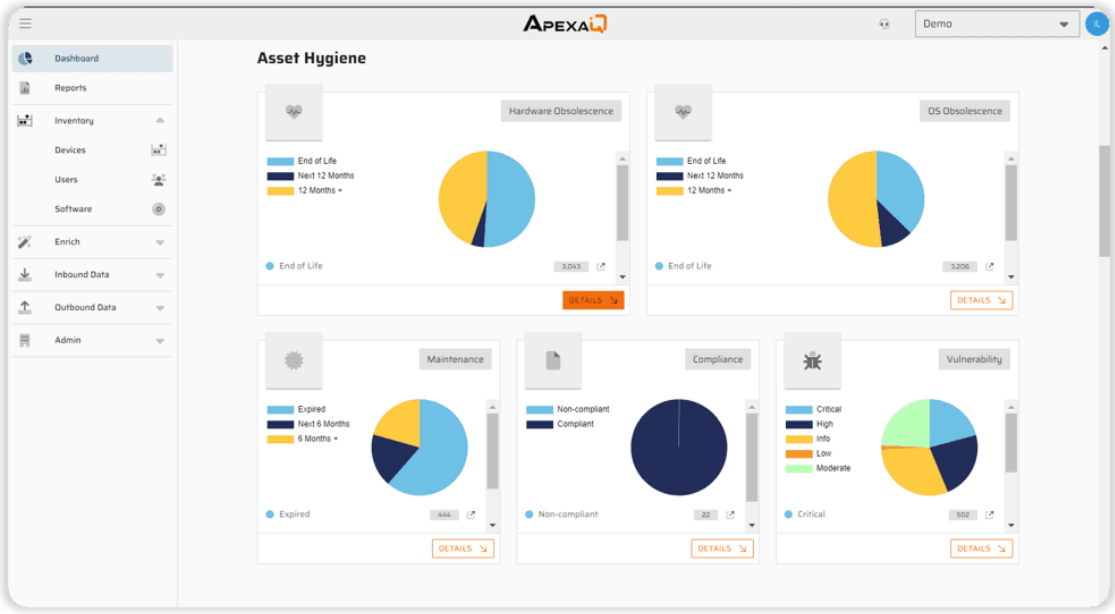
“End-of-service” or ‘end-of-support’ means the discontinuation of support for a product or service by the manufacturer. This no longer includes updates, maintenance or technical support. Although use is still possible, there are security risks. Users are therefore responsible for their own maintenance and security.

Source: https://blog.it-planet.com/en/eol-vs-eos-what-is-the-difference-and-why-is-it-important/

End of Maintenance It is the stage when a vendor discontinues releasing updates, bug fixes, and enhancements for a product. After this point, the product receives no improvements or security patches, making it more vulnerable to risks and compliance issues. Organizations cannot rely on the vendor for problem resolution and must depend on internal resources or third-party support. Hence, companies usually plan for upgrades, migration, or replacement before EOM to ensure security and smooth operations.

Asset Hygiene

Asset Hygiene is the practice of maintaining IT assets—like hardware, software, and data—in a secure, updated, and compliant state. It involves regular patching, accurate inventory tracking, license compliance, and proper disposal of unused assets. Good asset hygiene reduces cybersecurity risks, saves costs, and ensures smooth IT operations.



Crown Jewel

Crown Jewel Analysis teaches you what to protect and how to protect it. This fundamental risk management methodology has been used for decades to help organizations determine what is important to them and where to prioritize their resources to defend against cyberattacks.

This guide delves into this risk management methodology to show how to use it today. It explores Crown Jewel Analysis, its benefits, and how to perform it. There are also recommendations for tools to help you use this methodology in the real world, along with practical examples that show how to secure a fictitious hair salon against cyber threats.

Crown Jewel Analysis (CJA) is a risk management methodology used in cyber security to identify and prioritize the protection of an organization's most valuable assets, which are its crown jewels.

Source: https://kravensecurity.com/crown-jewel-analysis/

Inventory

The term inventory refers to the raw materials used in production as well as the goods produced that are available for sale. A company's inventory represents one of the most important assets it has because the turnover of inventory

Inventory management tracks the stock that comes in and goes out of a company's stores and warehouses. Asset management tracks the equipment and supplies that a company uses to run the business.

In other words, inventory management and asset management both track a company's property. But inventory management focuses on the flow of items a company sells or parts it uses to make goods. One of the goals of inventory management is to find the right balance of stock to satisfy customer demand or, in a manufacturing environment, supply production lines. Asset management, on the other hand, monitors items an organization uses internally, which are not for sale. Asset management also deals with ensuring asset value and availability

Source: https://www.netsuite.com/portal/resource/articles/inventory-management/inventory-management-asset-management.shtml

NVD

The National Vulnerability Database (NVD) is a foundational cybersecurity resource that provides detailed information on vulnerabilities across a wide range of software and hardware. Maintained by the National Institute of Standards and Technology (NIST), the NVD serves as the U.S. government repository of standards-based vulnerability management data. For security professionals, the NVD offers an invaluable source of actionable data to identify and mitigate cyber threats.

The NVD catalogues vulnerabilities based on the Common Vulnerabilities and Exposures (CVE) naming standard. Each CVE entry contains important metadata like descriptions, severity scores, and references to related advisories or solutions. The NVD currently contains over 150,000 CVE vulnerability entries compiled from over 200 data sources.

Source: https://www.fortinet.com/resources/cyberglossary/national-vulnerability-database-nvd

Patch Management

A patch is a piece of software code (usually made up of one or more files) written by a programmer to fix and update an application or file. Patches are created to fix problems and improve the functionality of computer applications and operating systems. They can be applied to both the Linux and Windows platforms, but do not work on Mac computers.

Patches or updates are released by the utility vendors to fix existing bugs and provide new features. Updating your system with patches is an important part of protecting it from cyberattacks and exploits. Patch Management is a tactic in which an ethical hacker focuses on the software compatibility of various versions for a number of devices, computers, and operating systems. It is significant to know the differences between each patch and what the implications are for different types of devices. A patch manager can help determine which patches are appropriate and when they should be deployed. When there is a brand-new OS release, such as iOS 8 or Windows 8, there may be many new patches released even before it has been released to consumers, so it is essential that organizations have a strategy in place to patch these machines in timely releases as well as ensure that these patches reach their target audience.

Source: https://www.geeksforgeeks.org/ethical-hacking/what-is-patch-management/

Data Breaches

A data breach is any security incident in which unauthorized parties access sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) and corporate data (customer records, intellectual property, financial information).

The terms “data breach” and “breach” are often used interchangeably with “cyberattack.” However, not all cyberattacks are data breaches. Data breaches include only those security breaches where someone gains unauthorized access to data.

Source: https://www.ibm.com/think/topics/data-breach

MSP

A managed services provider (MSP) is an outsourced third-party company that takes on the ongoing, day-to-day responsibilities, monitoring, and maintenance of a range of tasks and functions for another company—their customer. The MSP and the customer are typically bound by a contract with a standardised service level agreement that defines the expectations and quality metrics of the delivered services.

Source: https://www.sap.com/india/products/hcm/workforce-management/what-is-a-msp.html

Device Type

Device Type is a label associated to the device which is used to match it to a series or model. For e.g , Windows 7, Windows 2012, Cisco Catalyst 6509IOS

While configuring parameters and intervals for a network device, the type of the device and its function in the network has to be considered. For e.g, an IBM server which stores critical business data, its disk utilization and memory utilization should be monitored. On the other hand, availability has to be monitored for a Juniper switch.

Source: https://www.manageengine.com/network-monitoring/kb/difference-between-device-type-and-category.html

True SaaS

SaaS, which stands for Software-as-a-Service, is a model where vendors make software products available to customers over the internet on a subscription basis. The code, servers and database that make up the product are hosted and maintained by software providers like Amazon Web Services or Google Cloud. The customers then access the software through a web browser or a mobile app.

Source: https://builtin.com/articles/saas

Inbound and Outbound Integration

Inbound integration is when a system receives data from external sources to update or enrich its database. For example, importing customer details from a CRM into an ERP or pulling employee data from an HR system into payroll software.

Outbound integration is when a system sends data to external platforms for use elsewhere. For example, exporting sales reports to a BI tool, sending alerts from monitoring software to Slack, or pushing transaction data from POS to accounting systems.

Compliance Standards – eg. CISA, CISO, HIPPA, ISO 27001

Compliance standards are a set of guidelines, rules, and best practices established by industry associations, government bodies or regulatory bodies to ensure that organizations operate in an ethical, legal, and responsible manner.

Compliance standards typically address information security, privacy, risk management, and governance aspects of an organization.

HIPAA or the Health Insurance Portability and Accountability Act is a federal law that mandates the creation of national standards to protect sensitive patient data from being disclosed without the consent of the patient. Meeting HIPAA compliance requirements is mandated by law and it came into effect by the US Congress in 1996.

ISO 27001 – International Standard on requirements for information security management is a standard for managing and implementing Information Security Management Systems or ISMS. It provides a comprehensive framework for organizations to manage and protect sensitive data and information.

Source:https://sprinto.com/blog/compliance-standards/#:~:text=Compliance%20is%20a%20set%20of%20established%20rules%20and,CIS%2C%20CCPA%2C%20CSA%20STAR%2C%20and%20NIST%2C%20among%20others.

CISA (Cybersecurity and Infrastructure Security Agency) compliance standards are the cybersecurity directives and frameworks issued by the U.S. federal agency under the Department of Homeland Security. They are mainly meant for federal agencies and critical infrastructure providers, focusing on reducing cyber risks, strengthening resilience, improving incident response, and aligning with frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Zero Trust models.

CISO (Chief Information Security Officer) compliance standards refer to the security and regulatory requirements that the senior executive responsible for information security ensures their organization follows. These include global and industry regulations such as International Organization for Standardization (ISO) 27001, National Institute of Standards and Technology (NIST) guidelines, General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and Sarbanes–Oxley Act (SOX). They focus on data protection, risk management, and meeting legal and industry obligations.

Perimeter

Security perimeter is the area that divides and protects some valuable a company asset (a location, a network or a system) from the outside world. From information security point of view a security perimeter is the area in which data or information is stored and processed and where the IT devices are located (data center, server room, etc.).

Source: https://aptien.com/en/kb/articles/what-is-security-perimeter

ROI (Return on Investment) and KPI (Key Performance Indicators)

Return on investment (ROI) is a performance measure used to evaluate the efficiency or profitability of an investment.

Expressed as a percentage, return on investment (ROI) is a financial ratio that measures the profit generated by an investment relative to its cost. Key factors influencing ROI include the initial investment amount, ongoing maintenance costs, and the cash flow generated by the investment. To calculate ROI, the return of an investment is divided by the cost of the investment. The result is expressed as a percentage or a ratio.

Source: https://www.investopedia.com/terms/r/returnoninvestment.asp

Key Performance Indicators (KPIs) are important tools for measuring how well a company, project, or activity is doing. They provide clear and measurable data to track progress, find areas that need improvement, and make informed decisions.

Key performance indicators (KPIs) are a collection of quantifiable measurements. KPI are used to assess the overall long-term performance of a business. KPIs (Key Performance Indicator) in particular assist in identifying the strategic, financial, and operational accomplishments of a business, especially compared to other companies operating in the same sector. Organizations may make data-driven choices, identify areas of strength and weakness, and take action to maximize performance by keeping an eye on key performance indicators (KPIs).

Source: https://www.geeksforgeeks.org/data-science/what-is-a-kpi-key-performance-indicator/

Auto-remediation

Auto-remediation is a proactive approach to problem-solving that involves the use of automated tools and processes to detect and resolve issues in real-time. These tools can be programmed to monitor systems, applications, and networks for any signs of trouble, such as performance issues, security breaches, or configuration errors. When an issue is detected, the auto-remediation system can take predefined actions to resolve the problem, such as restarting a service, applying a patch, or rolling back a configuration change.

Source: https://www.b2oceans.com/glossario/what-is-auto-remediation/

Auto remediation is a cybersecurity capability that automatically executes predefined response actions to address security incidents, vulnerabilities, and compliance violations without manual intervention. Auto remediation combines advanced detection technologies with programmatic response workflows to neutralize threats at machine speed. This dramatically reduces response times from hours to minutes while minimizing human error and operational burden on security teams.

Source: https://expel.com/cyberspeak/what-is-auto-remediation/

Network protocols

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocols are the reason you can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

Similar to the way that speaking the same language simplifies communication between two people, network protocols make it possible for devices to interact with each other because of predetermined rules built into devices' software and hardware. Neither local area networks (LAN) nor wide area networks (WAN) could function the way they do today without the use of network protocols.

Source: https://www.comptia.org/en-us/blog/what-is-a-network-protocol/

Due-diligence

Due diligence refers to the thorough research and evaluation carried out to confirm the accuracy of information and assess any potential risks before committing to a transaction, agreement, or important decision. In the financial world, due diligence requires an examination of financial records before entering into a proposed transaction with another party.

Source: https://www.investopedia.com/terms/d/duediligence.asp

SOAR (Security Orchestration, Automation, and Response)

SOAR, for security orchestration, automation and response, is a software solution that enables security teams to integrate and coordinate separate security tools, automate repetitive tasks and streamline incident and threat response workflows.

In large organizations, security operations centers (SOCs) rely on numerous tools to track and respond to cyber threats, oftentimes manually. This manual investigation of threats results in slower overall threat response times.

SOAR platforms give SOCs a central console where they can integrate these tools into optimized threat response workflows and automate low-level, repetitive tasks in those workflows. This console also allows SOCs to manage all the security alerts generated by these tools in one central place.

Source: https://www.ibm.com/think/topics/security-orchestration-automation-response

Role of ITAM in Zero Trust Security Models

The Zero Trust Security Model is a modern framework of cybersecurity aimed at safeguarding organizations from data breaches, ransomware, and insider attacks. Zero Trust differs from conventional security models that take users within the network as secured, instead adopting a strict policy of "Never Trust, Always Verify". No user, device, or app gets access without proving their legitimacy—no exceptions.

With cyberattacks increasing by 300% in the last decade, businesses can no longer rely on outdated firewall-based security. Zero Trust ensures that even if a hacker gains access, they are locked out from sensitive data and resources.

Source: https://www.geeksforgeeks.org/ethical-hacking/zero-security-model/

Zero Trust isn't just a security strategy. It's a mindset. But it starts with knowing what you actually have.

If you don't know which devices are on your network, what software is running, or where your data lives, you can't protect any of it. That's where IT Asset Management (ITAM) comes in. Think of it as the foundation that every smart security decision is built on.

Zero Trust means never assuming anything is safe. Every user, device, and app must be verified before access is granted. But verification depends on visibility. And visibility starts with asset management.

Source: https://assetloom.com/blog/why-itam-is-critical-for-zero-trust-security

Cyber Asset Attack Surface Management (CAASM)

Cyber asset attack surface management (CAASM) is a proactive way to identify, manage and reduce your cyber attack surface. CAASM gives unified visibility across all your assets, including on-prem, cloud and third-party environments.

It helps security teams inventory and correlate data from multiple sources to better understand every connected asset and associated risk.

Source: https://www.tenable.com/cybersecurity-guide/learn/what-is-caasm