FUTURE BUILDERS THINKERS

POWERED BY DELL Technologies

Individual technological recommendations in the area of

Cyber Resilience

Thank you for answering all of the relevant questions on effective management and the use of data.

As a result of passing the placement test, you will receive:

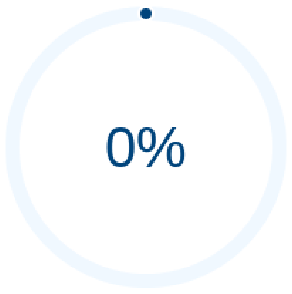
- an assessment of your company's technological advancement
- personalized expert recommendations of dedicated products and services for your organization
- a list of benefits resulting from the implementation of the recommended products and services
- benefits that result from your company's IT infrastructure reaching a higher level of technological involvement

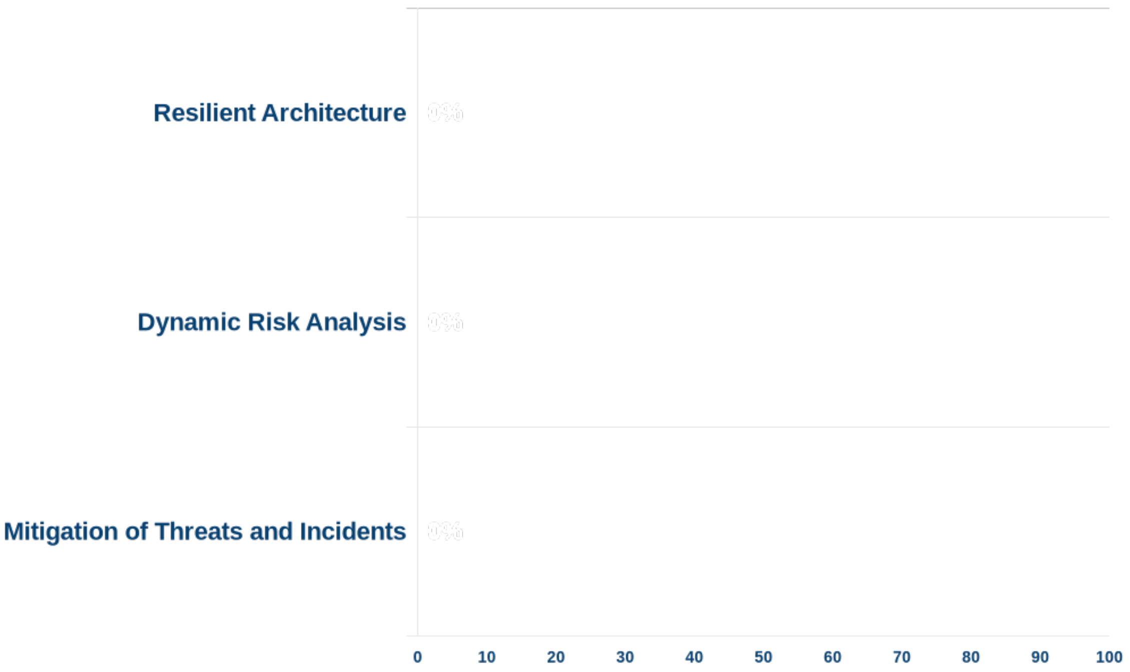
Using the recommended services will let your company, among other things, to:

- avoid migrating large volumes of data and the amount of work in managing permissions
- highlight the value of data from different sources and unify the experimental environment to share knowledge and results more easily
- Ehave full confidence in the information you send
- process incoming data on an ongoing basis with the option to postpone data that requires longer retention
- use artificial intelligence for image recognition from many data aggregation sources on a large scale

Optimal management over an increasing amount of data and their appropriate use is a huge challenge for every company. Yours can deal with this more effectively.

Your organization's level of technology involvement





0 - 35% - elementary level / digital laggards
35 - 60% - intermediate level / digital followers
60 - 85% - advanced level / digital evaluators
85 - 100% - highly advanced level / digital leaders

Technological recommendations in the areas of effective management and use of data

The recommendations prepared by our experts are based on the answers you gave on the techno logical advancement assessment within the selected IT approach. Based on this, we have developed a set of recommended actions that you should introduce. We have matched specific Dell Technologies’ and Partners’ products and services, as well as a list of benefits that you can acquire after implementing them.

Resilient architecture

Your resilient architecture score is **0%**. In order to achieve a higher level of technological maturity, you need to::

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Fill in the analysis of your organization's current HW/SW supply chains.	Increases resilience to attacks in the supply chain	Secure Supply Chain - Dell Technologies uses the Secure Development Lifecycle (SDL) during the software development process, as well as also including firmware and software provided by sub-suppliers. Secure software is digitally signed and verified each time the system starts up.	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Increase their supply chain securities for the organization, e.g. by working with trusted suppliers.	Increases resilience to attacks in the supply chain	Secure Supply Chain - Dell Technologies uses the Secure Development Lifecycle (SDL) during the software development process, as well as also including firmware and software provided by sub-suppliers. Secure software is digitally signed and verified each time the system starts up.	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Utilize Infrastructure as Code for more secure configuration management	Thanks to IaaC, configuration management becomes a controlled process with versioning, auditing, and accountability. The automation of this process via IaaC means that the infrastructure is verified for compliance at any interval.	API, Ansible Modules, Terraform Providers, VMware Aria Automation Config for Secure Hosts, VMware Aria Automation Orchestrator, VMware Aria Operations, VMware vSphere, Dell OpenManage Enterprise	Dell Technologies Infrastructure as a Code consulting services offer the implementation of tools and infrastructure description as code. Additionally, the implementation of products supporting SecOps ensures the full compliance of the configuration of the created infrastructure elements and services with the required cybersecurity standards and its continuous implementation throughout the entire process of use.

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Keep endpoints and parts of private or public clouds secure, including NGAV	Increases the ability to detect a potential attack and automates the reaction process	Secureworks Taegis XDR, VMware Carbon Black, Microsoft Defender	Dell Technologies Managed Detection and Response consulting services monitor, detect, investigate and respond to endpoint threats with Secureworks agents, elements of private and public clouds using Secureworks Taegis XDR solutions, and Security Operations Center (SOC) teams are available 24/7. Implementation of the Secureworks agent is free. Assistance with optional solution deployments such as VMware Carbon Black or Microsoft Defender is possible under additional endpoint security and monitoring services.

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Introduce a vulnerability management system to your organization's IT infrastructure	The organization gains insights as to where a gap in infrastructure is in terms of past and recent cyberattack vulnerabilities	Secureworks Taegis VDR, VMware Carbon Black, Microsoft Defender	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Use network and system recordings of instances for data access on a storage system	Incident auditing and accountability on storage systems	PowerScale, ObjectScale systems	ProDeploy Plus for Enterprise enables the implementation of various Dell Technologies infrastructure components and monitoring tools.

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Use network and system recordings of instances for data access on a storage system	Incident auditing and accountability on an application	PowerScale, ObjectScale systems	ProDeploy Plus for Enterprise enables the implementation of various Dell Technologies infrastructure components and monitoring tools.

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Deploy data classification implementation regarding susceptibility and access rights	Lack of knowledge of the location of sensitive data and who has access to it makes it impossible to prepare a data protection policy	Superna Eyeglass, Varonis for NAS and Object systems	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Deploy data classification implementation regarding susceptibility to loss of confidentiality	Lack of knowledge of the location of sensitive data and who has access to it makes it impossible to prepare a data protection policy	Superna Eyeglass, Varonis for NAS and Object systems	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Verification of access rights depending on data sensitivity classification	Lack of knowledge of the location of sensitive data and who has access to it makes it impossible to prepare a data protection policy	Superna Eyeglass, Varonis for NAS and Object systems	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Deploy an automatic reaction system (to notify or block user) for an attempt to encrypt or damage data - mass data modification	The first response stage to data encryption	Superna Eyeglass, Varonis for NAS and Object systems	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Deploy an automatic reaction system (to notify or block user) for an attempt to steal sensitive data - mass reading	Increasing the chances to detect data theft	Superna Eyeglass, Varonis for NAS and Object systems	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Introduce a mechanism to automatically create backup copies and store outside of the source medium	Minimal digital hygiene rules when making copies and making copies available when needed	Dell PowerProtect DD, DM, Avamar, NetWorker	ProDeploy Plus for Data Protection Suite and Cloud Adoption Package makes it possible to deploy various elements of Dell Technologies data protection solutions. These include: Data Domain Virtual Edition with Avamar Virtual Edition, NetWorker Virtual Edition, PowerProtect Data Manager, Data Domain Management Center (DDMC) in multicloud environments

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Implement the 3-2 rule (3 copies of data, stored on at least 2 mediums)	Increases the probability of having a valid copy	Dell PowerProtect DD, DM, Avamar, NetWorker	ProDeploy Plus for Data Protection Suite and Cloud Adoption Package makes it possible to deploy various elements of Dell Technologies data protection solutions. These include: Data Domain Virtual Edition with Avamar Virtual Edition, NetWorker Virtual Edition, PowerProtect Data Manager, Data Domain Management Center (DDMC) in multicloud environments

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Regularly test backup copies for data accuracy	Minimizes the likelihood of an error in the copy or during the copying process	Dell PowerProtect DD, DM, Avamar, NetWorker	Dell Technologies Infrastructure as Code consulting services offer the implementation of a set of tools and infrastructure description as code, as well as the creation of automatic data recovery and testing services

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Running the hardening process for your storage medium backup copies, e.g. in accordance with the STIG standard	The security mechanisms implemented in the medium itself significantly increase the security of copies in the event of a successful ransomware attack	Dell PowerProtect DD	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Enable WORM protection in your backup medium	Security mechanisms implemented in the medium itself significantly increase the security of copies in the event of a successful ransomware attack, as well as against human error	Dell PowerProtect DD	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Do you follow the 3-2-1 rule (3 copies of data, stored on at least 2 mediums, plus 1 offline copy). The 3-2-1 rule uses the "air-gap" mechanism to isolate copies on the most critical - vital applications.	While following this rule, backup copies are beyond an attacker's penetration range, including that of an inside attacker.	Dell Cyber Recovery Vault	Dell Technologies Cyber Recovery Solution consulting services allows for the development and implementation of a last line of defense strategy against attacks such as ransomware using an isolated digital bunker, advanced analytical drives and a ready runtime environment for the most critical applications and data

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Employ an isolated enclave backup analysis for ransomware encryption	Backup copies can be used for analysis as an early warning process. This lets the organization know when encryption started, from where in the network, and which is the latest valid copy	Dell PowerProtect CyberSense	Dell Technologies Cyber Recovery Solution consulting services allows for the development and implementation of a last line of defense strategy against attacks such as ransomware using an isolated digital bunker, advanced analytical drives and a ready runtime environment for the most critical applications and data

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Implement a ready-made runtime environment in an isolated enclave of your IT infrastructure	Reduces the time needed for an emergency start for the most critical applications in the event of a successful attack and a compromised primary site	Dell Cyber Recovery Vault	Dell Technologies Cyber Recovery Solution consulting services allows for the development and implementation of a last line of defense strategy against attacks such as ransomware using an isolated digital bunker, advanced analytical drives and a ready runtime environment for the most critical applications and data

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Implement the procedures necessary to run vital applications in an isolated enclave of your IT infrastructure	Reduces the time needed for an emergency start for the most critical applications in the event of a successful attack and a compromised primary site	Dell Cyber Recovery Vault	Dell Technologies Cyber Recovery Solution consulting services allows for the development and implementation of a last line of defense strategy against attacks such as ransomware using an isolated digital bunker, advanced analytical drives and a ready runtime environment for the most critical applications and data

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Implement a no-trust policy for devices by authenticating the management of each device	Elimination of untrusted devices from the DC infrastructure reduces risks and increases security	VMware Unified Access Gateway, Workspace ONE UEM, Carbon Black	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Implement a no-trust policy for users with strong authentication for dynamic conditional access	Elimination of untrusted users from the DC infrastructure	VMware Workspace ONE Access/Intelligence	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Implement a no-trust policy for transport by segmenting and filtering all network traffic for VM-to-VM	Elimination of network traffic that does not meet the organization's policy and implementation of the 'least privilege access' rule	VMware NSX	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Implement a no-trust policy for applications through SSO based on strong authentication	Increased security by utilizing a Zero Trust strategy for applications. The Zero Trust strategy for applications uses mechanisms such as SSO and application isolation	VMware Workspace ONE UEM/Access	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Implement a no-trust policy for applications through application isolation	Increased security by utilizing a Zero Trust strategy for applications. The Zero Trust strategy for applications uses mechanisms such as SSO and application isolation	VMware Workspace ONE UEM/Access	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Implement a no-trust policy for data through DLP and data security	The Zero Trust strategy regarding data increases security by using encryption to protect data, mechanisms ensuring data immutability and ensuring data integrity	VMware Workspace ONE UEM, NSX, Horizon, PowerScale, Unity, PowerSstore	-

Dynamic risk analysis

Your dynamic risk analysis score is **0%**. In order to achieve a higher level of technological maturity, you need to::

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Conduct an organizational inventory (based on documentation) of resources subject to risk analysis	This enables identification of all the necessary resources and specifies how to include this information in the risk analysis system. However, due to its organizational nature it causes the risk of high costs for managing the information base	-	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Conduct organizational and technical (based on documentation and technical activities) identification of resources subject to risk analysis	This allows for an effective and defect-free organizational approach, i.e. reducing high maintenance costs, identifying all resources, and dynamically collecting information about them as key ICT objects and potential data sources used in risk analysis, as well as, for example, in incident management systems	ITAM	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Introduce resource valorization based on BIA (Business Impact Analysis)	This enables the assignment of appropriate values to resources based on their importance and necessity in the business processes implementation	BIA Toolkits	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Conduct the implementation of organizational risk communication dedicated to specific areas of the organization	This builds the level of awareness of cyber threats and their impact on the operation of specific organizational units	Dynamic Risk Assessment Templates	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Implement automatic calculation of cyber threat risk for specific business processes	This provides a tool for the potential use of direct risk information in business units without the need for advanced and costly substantive consultations with technical departments	Dynamic Risk Assessment Templates	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Introduce a feedback system for risk based on decisions in the business process management field	This allows for the correct presentation of risk in the organization, as well as taking corrective actions of an organizational and technical nature into account	-	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Establish a budget for cybersecurity as a part of IT	Establishing communication based on business value. This is crucial for smooth cooperation between technical departments, primarily responsible for cyber security and structures responsible for the implementation of business activities	ROSI calculators	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Introduce a system for continuous acquisition of information on the likelihood and impact of individual types of cyber threats	Establishing communication based on business value. This is crucial for smooth cooperation between technical departments, primarily responsible for cyber security and structures responsible for the implementation of business activities	ROSI calculators	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Introduce the use of monitoring and documenting the value of cybersecurity effects	Demonstration of the value and potential of the practical use of ROSI calculations in the organization's activities	https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/@@download/fullReport	-

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Introduce the calculation for financial effects of recorded cyberattacks	Demonstration of the value and potential of the practical use of ROSI calculations in the organization's activities	https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/@@download/fullReport	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Implement a dynamic ROSI calculation based on all signals documenting cybersecurity performance	Introduce a practical tool that catalyzes the widespread use of calculated ROSI in planning and budgeting all business ventures	-	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Implement a dynamic ROSI calculation based on all signals documenting cybersecurity performance	Introduce a practical tool that catalyzes the widespread use of calculated ROSI in planning and budgeting all business ventures	-	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Identify the competence areas necessary for the required risk mitigation	Establishing maps detailing relationships between risks for the organization and the functioning of the organization's cybersecurity ecosystem elements (people, processes, technology)	-	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Determine the scope and dynamics of transformation in the event of a change in the nature of a risk, including the categorization of competencies on the basis in which they are provided (own, outsourcing, hybrid)	Understanding the intensity of risks impact on the cybersecurity ecosystem, which provides the basis for the proper planning of its development	-	-

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Prepare proposals for management decisions for direct consideration/decision by management. Ultimately, at several defined management levels.	Facilitating cybersecurity ecosystem management through the possibility of evaluating decision proposals generated by the expert system	-	-

Mitigation of threats and incidents

Your mitigation of threats and incidents score is **0%**. In order to achieve a higher level of technological maturity, you need to::

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Implement a standard IT administrator-managed logging system	A central log storage location permits the performance of post-incident analysis and determines the type and source of attack	Solutions embedded in the OS or open source solutions	ProDeploy Plus for Enterprise allows for the deployment of various Dell Technologies infrastructure components and monitoring tools

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Implement a SIEM class log collection system that conducts analysis, aggregation, data correlation and alert generation and will be managed by the IT team	Supports investigative activities, is a source of early warning	Secureworks Taegis XDR	Dell Technologies Managed Detection and Response consulting services monitor, detect, investigate and respond to threats on endpoints with Secureworks agents, private and public cloud elements using Secureworks Taegis XDR solutions and 24/7 Security Operations Center (SOC) teams. Implementation of the Secureworks agent is free, and assistance with the deployment of optional solutions such as VMware Carbon Black or Microsoft Defender is possible concerning additional endpoint security and monitoring services

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Direct a dedicated team of SOC specialists to support SIEM	Having a dedicated team to handle incidents increases the quality of their support. This defines responsibilities and creates security domains with different functions and purposes	Secureworks Taegis XDR operates in a cloud model that includes a virtual SOC team work service (24x7) who: - analyzes threat alerts, - provides assistance in the event of an attack (response to the attack and corrective actions)	Dell Technologies Managed Detection and Response consulting services monitor, detect, investigate and respond to threats on endpoints with Secureworks agents, private and public cloud elements using Secureworks Taegis XDR solutions and 24/7 Security Operations Center (SOC) teams. Implementation of the Secureworks agent is free, and assistance with the deployment of optional solutions such as VMware Carbon Black or Microsoft Defender is possible concerning additional endpoint security and monitoring services

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Introduce a SIEM system so that it uses AI/ML mechanisms to automate the identification of known and new threats	This increases the chances of detecting a threat that was missed by classic algorithms based on varying heuristics	Secureworks Taegis XDR uses AI-based detection and is equipped with an integrated DL threat detection engine	Dell Technologies Managed Detection and Response consulting services monitor, detect, investigate and respond to threats on endpoints with Secureworks agents, private and public cloud elements using Secureworks Taegis XDR solutions and 24/7 Security Operations Center (SOC) teams. Implementation of the Secureworks agent is free, and assistance with the deployment of optional solutions such as VMware Carbon Black or Microsoft Defender is possible concerning additional endpoint security and monitoring services

ACTIONS: what you should implement	**BENEFITS:** what you will gain after implementing the recommended action	**PRODUCTS:** recommended technological solutions	**SERVICES:** recommended technological solutions
Implement a SIEM based on information sent from many organizations	We can achieve the effect of cross-org correlation by using using SIEM located in the cloud, which aggregates information sent from many organizations. AI/ML SIEM algorithms learn from a much larger data set, thanks to which they can proactively warn organizations where the first symptoms of an attack(s) appear but are not yet known	Secureworks Taegis XDR. Machine learning algorithms are based on data from more than 4,200 organizations	Dell Technologies Managed Detection and Response consulting services monitor, detect, investigate and respond to threats on endpoints with Secureworks agents, private and public cloud elements using Secureworks Taegis XDR solutions and 24/7 Security Operations Center (SOC) teams. Implementation of the Secureworks agent is free, and assistance with the deployment of optional solutions such as VMware Carbon Black or Microsoft Defender is possible concerning additional endpoint security and monitoring services

ACTIONS: what you should implement	BENEFITS: what you will gain after implementing the recommended action	PRODUCTS: recommended technological solutions	SERVICES: recommended technological solutions
Conduct a SIEM implementation with the most developed concept of SOAR class incident management automation (Security Orchestration, Automation and Response)	Reducing security incident response time (MTTR) through automation. Automating manual tasks improves the efficiency of cybersecurity team members	Secureworks Taegis XDR.	Dell Technologies Managed Detection and Response consulting services monitor, detect, investigate and respond to threats on endpoints with Secureworks agents, private and public cloud elements using Secureworks Taegis XDR solutions and 24/7 Security Operations Center (SOC) teams. Implementation of the Secureworks agent is free, and assistance with the deployment of optional solutions such as VMware Carbon Black or Microsoft Defender is possible concerning additional endpoint security and monitoring services

Thank you for your participation

You now know about the technological recommendations for your organization in the approach of:

Cyber Resilience

Check your organization's current IT infrastructure level of technological maturity and familiarize yourself with expert recommendations in other approaches:

- Entangled Worlds
- Data Induced Everything
- Stack Redefinition

Implementing recommended products and services at all levels will make it easier for your organization to achieve the highest level of technological maturity.

If you are interested in the Future Builders project, we encourage you to download a special report created by a group of experts. We included proposals for the direction of changes and solutions that match the four most defined important challenges in four strategic IT areas, which can help upgrade your organization's technology and reach strategic business goals. You can download the report at futurebuilders.pl. Thank you for your interest and participation in our test.

futurebuilders.pl