Dziękujemy za odpowiedź na wszystkie pytania poziomujące z zakresu cyberbezpieczeństwa.

W wyniku rozwiązania testu poziomującego otrzymujesz:

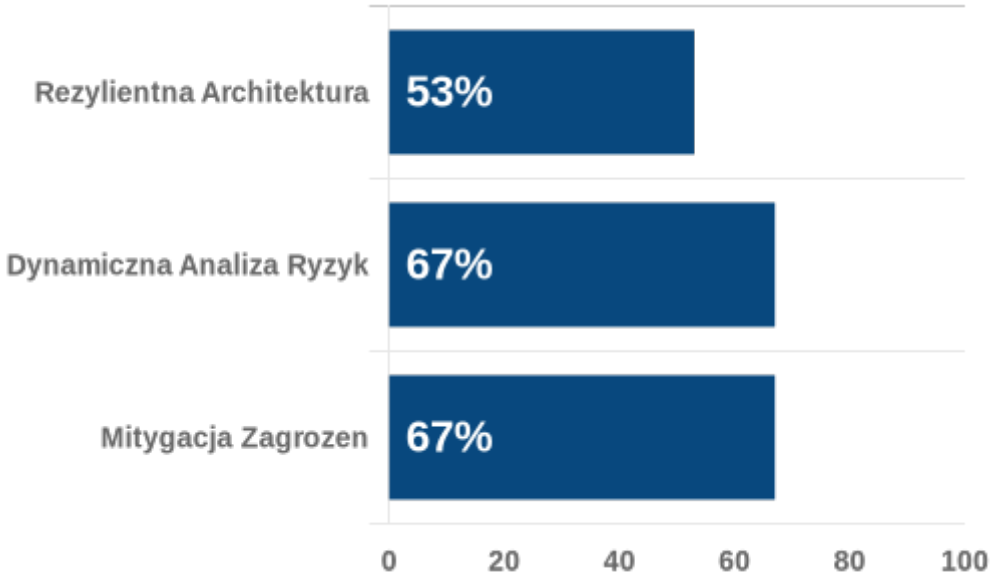
- ocenę stanu zaawansowania technologicznego Twojej firmy
- spersonalizowane rekomendacje ekspertów dotyczące produktów i usług dedykowanych dla Twojej organizacji
- wykaz korzyści wynikających z wdrożenia rekomendowanych produktów i usług
- korzyści wynikające z osiągnięcia wyższego poziomu zaangażowania technologicznego infrastruktury IT w Twojej firmie

Jakie korzyści płyną z wypełnienia ścieżki Cyber Resilience

Lorem ipsum dolor sit amet consectetur. Id nec ut eu dolor ac. Duis egestas nec feugiat diam. Aliquet massa id feugiat sagittis tincidunt pellentesque sed lorem. Faucibus adipiscing nisi ultricies augue rutrum sit lacus. A in nibh augue at. Ut adipiscing gravida ut sapien faucibus placerat.

Poziom zaangażowania technologicznego Twojej organizacji

Spersonalizowanego i bezpiecznego środowiska pracy hybrydowej w Twojej organizacji



0 - 35% - poziom podstawowy / digital laggards
35 - 60% - poziom średniozaawansowany / digital followers
60 - 85% - poziom zaawansowany / digital evaluators
85 - 100% - poziom wysoce zaawansowany / digital leaders

Rekomendacje technologiczne z obszaru cyberbezpieczeństwa

Przygotowane przez naszych ekspertów rekomendacje opierają się na Twoich odpowiedziach w teście stanu zaawansowania technologicznego w wybranej ścieżce IT. Na tej podstawie opracowaliśmy zestaw rekomendowanych działań, które powinieneś wdrożyć. Do tego dopasowaliśmy konkretne produkty i usługi Dell Technologies i Partnerów oraz wykaz korzyści, które zyskasz po ich implementacji.

Rezylientna architektura

Twoj wynik z rezylientnej architektury to **53%**. Żebys mogl wejść na wyższy poziom zaawansowania musisz podjąć:

DZIAŁANIA: jakie powinieneś wdrożyć	**KORZYŚCI:** co zyskasz po wdrożeniu rekomendowanego działania	**PRODUKTY:** rekomendowane rozwiązania technologiczne	**USŁUGI:** rekomendowane rozwiązania technologiczne
Wykorzystaj Infrastructure as Code, by bezpieczniej zarządzać konfiguracją	Dzięki IaaC zarządzanie konfiguracją staje się kontrolowanym procesem z wersjonowaniem, audytowaniem i rozliczalnością. Automatyzacja tego procesu poprzez IaaC sprawia, że infrastruktura jest weryfikowana pod kontem compliance z dowolną częstotliwością	API, Moduły Ansible, Terraform Providers, VMware Aria Automation Config for Secure Hosts, VMware Aria Automation Orchestrator, VMware Aria Operations, VMware vSphere, Dell OpenManage Enterprise	Usługi konsultingowe Dell Technologies Infrastructure as a Code oferują wdrożenie zestawu narzędzi i opisu infrastruktury jako kod. Dodatkowo wdrożenie produktów wspierających SecOps, dla zapewnienia pełnej zgodności konfiguracji tworzonych elementów infrastruktury i usług z wymaganymi standardami cyberbezpieczeństwa oraz jej ciągłego wymuszania w całym procesie użytkowania

DZIAŁANIA: jakie powinieneś wdrożyć	**KORZYŚCI:** co zyskasz po wdrożeniu rekomendowanego działania	**PRODUKTY:** rekomendowane rozwiązania technologiczne	**USŁUGI:** rekomendowane rozwiązania technologiczne
Przeprowadź wdrożenie systemu zarządzania podatnościami w infrastrukturze IT Twojej organizacji	Organizacja zyskuje wiedzę o tym, w którym miejscu infrastruktury istnieje dziura w kontekście historycznych i najnowszych podatności na cyberataki	Secureworks Taegis VDR, VMware Carbon Black, Microsoft Defender	-

DZIAŁANIA: jakie powinieneś wdrożyć	**KORZYŚCI:** co zyskasz po wdrożeniu rekomendowanego działania	**PRODUKTY:** rekomendowane rozwiązania technologiczne	**USŁUGI:** rekomendowane rozwiązania technologiczne
Przeprowadź wdrożenie klasyfikacji danych pod kątem ich wrażliwości oraz uprawnień dostępu do nich	Brak wiedzy gdzie znajdują się wrażliwe dane i kto ma do nich dostęp, uniemożliwia przygotowanie polityki ochrony tych danych	Superna Eyeglass, Varonis w zakresie systemów NAS i Object	-

DZIAŁANIA: jakie powinieneś wdrożyć	**KORZYŚCI:** co zyskasz po wdrożeniu rekomendowanego działania	**PRODUKTY:** rekomendowane rozwiązania technologiczne	**USŁUGI:** rekomendowane rozwiązania technologiczne
Przeprowadź wdrożenie systemu automatycznej reakcji (powiadomienie lub blokada użytkownika) na próbę kradzieży wrażliwych danych - masowy odczyt	Podniesienie szans na wykrycie kradzieży danych	Superna Eyeglass w zakresie systemów NAS i Object	-

DZIAŁANIA: jakie powinieneś wdrożyć	**KORZYŚCI:** co zyskasz po wdrożeniu rekomendowanego działania	**PRODUKTY:** rekomendowane rozwiązania technologiczne	**USŁUGI:** rekomendowane rozwiązania technologiczne
Regularnie testuj kopie bezpieczeństwa pod kątem poprawności danych	Minimalizuje prawdopodobieństwo błędu w kopii lub w procesie tworzenia kopii	Dell PowerProtect DD, DM, Avamar, NetWorker	Usługi konsultingowe Dell Technologies Infrastructure as Code oferują wdrożenie zestawu narzędzi i opisu infrastruktury jako kod, jak również stworzenie usług automatycznego przywracania kopii danych i ich testowania

DZIAŁANIA: jakie powinieneś wdrożyć	**KORZYŚCI:** co zyskasz po wdrożeniu rekomendowanego działania	**PRODUKTY:** rekomendowane rozwiązania technologiczne	**USŁUGI:** rekomendowane rozwiązania technologiczne
Zastosuj zasadę 3-2-1 (3 kopie danych, przechowywane na co najmniej 2 nośnikach i dodatkowo 1 kopia offline). Zasada 3-2-1 wykorzystuje mechanizm "air-gap" w celu izolacji kopii na najbardziej krytycznych aplikacjach - witalnych	Przy zachowaniu tej zasady kopie bezpieczeństwa znajdują się poza zasięgiem penetracji atakującego, w tym również atakującego insidera.	Dell Cyber Recovery Vault	Usługi konsultingowe Dell Technologies Cyber Recovery Solution pozwalają opracować i wdrożyć strategię ostatniej linii obrony przed atakami, takimi jak oprogramowanie ransomware z wykorzystaniem wyizolowanego bunkra cyfrowego, zaawansowanych napędów analitycznych i gotowego środowiska uruchomieniowego dla najbardziej krytycznych aplikacji i danych

DZIAŁANIA: jakie powinieneś wdrożyć	KORZYŚCI: co zyskasz po wdrożeniu rekomendowanego działania	PRODUKTY: rekomendowane rozwiązania technologiczne	USŁUGI: rekomendowane rozwiązania technologiczne
W izolowanej enklawie Twojej infrastruktury IT przeprowadź wdrożenie gotowego środowiska uruchomieniowego oraz procedur niezbędnych do uruchomienia witalnych aplikacji	Skraca czas potrzebny na uruchomienie awaryjne najbardziej krytycznych aplikacji w przypadku udanego ataku i kompromitacji ośrodka podstawowego	Dell Cyber Recovery Vault	Usługi konsultingowe Dell Technologies Cyber Recovery Solution pozwalają opracować i wdrożyć strategię ostatniej linii obrony przed atakami, takimi jak oprogramowanie ransomware z wykorzystaniem wyizolowanego bunkra cyfrowego, zaawansowanych napędów analitycznych i gotowego środowiska uruchomieniowego dla najbardziej krytycznych aplikacji i danych

DZIAŁANIA: jakie powinieneś wdrożyć	KORZYŚCI: co zyskasz po wdrożeniu rekomendowanego działania	PRODUKTY: rekomendowane rozwiązania technologiczne	USŁUGI: rekomendowane rozwiązania technologiczne
Wprowadź zasadę braku zaufania na poziomie użytkownika poprzez silną autentykację dynamicznego warunkowego dostępu	Eliminacja niezaufanych użytkowników z infrastruktury DC	VMware Workspace ONE Access/Intelligence	-

DZIAŁANIA: jakie powinieneś wdrożyć	KORZYŚCI: co zyskasz po wdrożeniu rekomendowanego działania	PRODUKTY: rekomendowane rozwiązania technologiczne	USŁUGI: rekomendowane rozwiązania technologiczne
Wprowadź zasadę braku zaufania na poziomie aplikacji poprzez SSO na bazie silnej autentykacji oraz izolacji aplikacji	Strategia Zero Trust w stosunku do aplikacji wykorzystuje takie mechanizmy jak SSO, i izolacja aplikacji	VMware Workspace ONE UEM/Access	-

Dynamiczna analiza ryzyk

Twoj wynik z dynamicznej analizy ryzyk to **67%**. Żebys mogl wejść na wyższy poziom zaawansowania musisz podjąć:

DZIAŁANIA: jakie powinieneś wdrożyć	KORZYŚCI: co zyskasz po wdrożeniu rekomendowanego działania	PRODUKTY: rekomendowane rozwiązania technologiczne	USŁUGI: rekomendowane rozwiązania technologiczne
Przeprowadź organizacyjną i techniczną (w oparciu o dokumentację i działania techniczne) identyfikację zasobów podlegających analizie ryzyka	Pozwala na skuteczne i pozbawione wad podejścia organizacyjne, tj. ograniczenie dużych kosztów utrzymania, identyfikowanie wszystkich zasobów i dynamiczne zbieranie informacji o nich, jako kluczowych obiektach ICT oraz potencjalnych źródłach danych, wykorzystywanych w analizie ryzyka, ale również np.: w systemach zarządzania incydentami	ITAM	-

DZIAŁANIA: jakie powinieneś wdrożyć	KORZYŚCI: co zyskasz po wdrożeniu rekomendowanego działania	PRODUKTY: rekomendowane rozwiązania technologiczne	USŁUGI: rekomendowane rozwiązania technologiczne
Przeprowadź wdrożenie automatycznego wyliczania ryzyka cyberzagrożeń dla poszczególnych procesów biznesowych	Daje narzędzie do ewentualnego wykorzystania informacji o ryzyku bezpośrednio w komórkach biznesowych, bez konieczności zaawansowanych i kosztownych konsultacji merytorycznych z działami technicznymi	Dynamic Risk Assessment Templates	-

DZIAŁANIA: jakie powinieneś wdrożyć	KORZYŚCI: co zyskasz po wdrożeniu rekomendowanego działania	PRODUKTY: rekomendowane rozwiązania technologiczne	USŁUGI: rekomendowane rozwiązania technologiczne
Wprowadź stosowanie monitoringu i prowadzenia dokumentacji wartości oddziaływania cyberzabezpieczeń oraz wyliczania skutków finansowych odnotowywanych cyberataków	Wykazanie wartości i potencjału praktycznego wykorzystania obliczeń ROSI w działalności organizacji	-	-

DZIAŁANIA: jakie powinieneś wdrożyć	KORZYŚCI: co zyskasz po wdrożeniu rekomendowanego działania	PRODUKTY: rekomendowane rozwiązania technologiczne	USŁUGI: rekomendowane rozwiązania technologiczne
Ustal zakres i dynamikę transformacji w przypadku zmiany charakteru ryzyka, w tym kategoryzację kompetencji ze względu na ich sposób zapewnienia (własne, outsourcing, hybrydowe)	Zrozumienie intensywności oddziaływania ryzyk na ekosystem cyberbezpieczeństwa, co daje podstawę do poprawnego planowania jego rozwoju	-	-

Mitygacja zagrożeń i incydentów

Twoj wynik z mitygacji zagrożeń i incydentów to **67%**. Żebys mogl wejść na wyższy poziom zaawansowania musisz podjąć:

DZIAŁANIA: jakie powinieneś wdrożyć	KORZYŚCI: co zyskasz po wdrożeniu rekomendowanego działania	PRODUKTY: rekomendowane rozwiązania technologiczne	USŁUGI: rekomendowane rozwiązania technologiczne
Przeprowadź wdrożenie systemu zbierania logów klasy SIEM realizującego analizę, agregację, korelację danych oraz generowanie alertów, który będzie zarządzany przez zespół IT	Wspiera działania śledcze, stanowi źródło wczesnego ostrzegania	Secureworks Taegis XDR	Usługi konsultingowe Dell Technologies Managed Detection and Response monitorują, wykrywają, badają i reagują na zagrożenia na punktach końcowych z agentami Secureworks, czy elementach chmur prywatnych i publicznych z wykorzystaniem rozwiązań Secureworks Taegis XDR i zespołów Security Operations Center (SOC) dostępnych 24/7. Wdrożenie agenta Secureworks jest bezpłatne, a pomoc przy wdrożeniu opcjonalnych rozwiązań, takich jak VMware Carbon Black czy Microsoft Defender jest możliwa w ramach dodatkowych usług zabezpieczenia i monitorowania punktów końcowych

DZIAŁANIA: jakie powinieneś wdrożyć	KORZYŚCI: co zyskasz po wdrożeniu rekomendowanego działania	PRODUKTY: rekomendowane rozwiązania technologiczne	USŁUGI: rekomendowane rozwiązania technologiczne
Przeprowadź wdrożenie SIEM bazującego na informacjach przesyłanych z wielu organizacji	Poprzez wykorzystanie SIEM zlokalizowanego w chmurze, który agreguje informacje wysyłane z wielu organizacji, osiągamy efekt korelacji cross-org. Algorytmy AI/ML SIEM uczą się na dużo większym zbiorze danych, dzięki czemu mogą proaktywnie ostrzegać organizacje, w których pojawią się pierwsze symptomy ataku lub ataki, które nie są jeszcze znane	Secureworks Taegis XDR. Algorytmy uczenia maszynowego bazują na danych z ponad 4200 organizacji	Usługi konsultingowe Dell Technologies Managed Detection and Response monitorują, wykrywają, badają i reagują na zagrożenia na punktach końcowych z agentami Secureworks, czy elementach chmur prywatnych i publicznych z wykorzystaniem rozwiązań Secureworks Taegis XDR i zespołów Security Operations Center (SOC) dostępnych 24/7. Wdrożenie agenta Secureworks jest bezpłatne, a pomoc przy wdrożeniu opcjonalnych rozwiązań, takich jak VMware Carbon Black czy Microsoft Defender jest możliwa w ramach dodatkowych usług zabezpieczenia i monitorowania punktów końcowych

Dziękujemy za Twoje zaangażowanie

Poznałeś rekomendacje technologiczne dla Twojej organizacji w ścieżce:

Cyber Resilience

Sprawdź jaki jest poziom zaawansowania technologicznego Twojej organizacji w pozostałych ścieżkach:

Entangled Worlds

Data Induced Everything

Stack Redefinition

Wdrożenie zalecanych produktów i usług we wszystkich poziomach pozwoli Twojej organizacji osiągnąć najwyższy poziom dojrzałości technologicznej.

Jeśli zainteresował Cię projekt Future Builders, zachęcamy do pobrania stworzonego przez grupę ekspertów specjalnego raportu. Zawarliśmy w nim propozycje kierunków zmian i rozwiązań odpowiadających na zdefiniowane cztery najważniejsze wyzwania w czterech strategicznych obszarach IT, które pomogą na upgrade technologiczny Twojej organizacji i realizować strategiczne cele biznesowe. Raport pobierzesz na stronie futurebuilders.pl. Dziękujemy za zainteresowanie i udział w naszym teście.

futurebuilders.pl