CHECKLIST

ACSC Essential Eight Compliance Checklist to Reduce Cyber Risk

How eSentire helps your organization build resilience & prevent disruption with a security program that maps to the Essential Eight Maturity Levels One through Three

The Essential Eight is a cybersecurity maturity model developed by the Australian Cyber Security Centre (ACSC) to help protect organizations against cyber threats. The model features eight cyber risk mitigation strategies designed to complement each other and mitigate the most common cyber threats.

First issued in 2017, the model is regularly revised and updated by the ACSC to reflect the cybersecurity measures that can help protect organizations against new and existing attack vectors. Originally developed to mitigate risks within Australian public agencies, the cyber risk mitigation strategies presented in the Essential Eight have been increasingly adopted by the private sector. Although the Essential Eight was originally designed to protect Microsoft Windows-based internet-connected networks, its recommendations for Vulnerability management and patching can be applied across any on-prem environment and cloud services to help prevent attacks, limit attack impact, and ensure data availability.

To help organizations implement the Essential Eight, the ACSC defined three maturity levels:

- **Maturity Level One:** partly aligned with the recommended mitigation strategies
- **Maturity Level Two:** mostly aligned with the best practices but looking to implement a stronger risk-reduction strategy
- **Maturity Level Three:** fully aligned with the intent of the mitigation strategy

In this document, we've broken down the ACSC's Essential Eight Cybersecurity Framework mitigation strategies for each maturity level to provide tangible recommendations on how eSentire, the Authority in Managed Detection and Response, can help you not only comply with the recommendations, but also mitigate cyber risk, and build long term cyber resilience to prevent your business from ever being disrupted.

MATURITY LEVEL ONE				
Mitigation Strategy	**Control Description**	**Test ID**	**Test Description**	**eSentire Service**
Application control	The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.	ML1-AC-01	(Workstations) Executable files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting with endpoint threat prevention and endpoint detection and response capabilities. Our 24/7 SOC Cyber Analysts rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread. We work alongside you to determine the root cause, remediate with corrective actions and ensure you are protected against business disruption. Our best-of-breed MDR approach means we partner with leaders in endpoint protection (EPP) and endpoint detection and response (EDR) to deliver eSentire MDR for Endpoint. **Learn more** **MDR for Endpoint Data Sheet**
		ML1-AC-02	(Workstations) Software library files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	
		ML1-AC-03	(Workstations) Script files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	
		ML1-AC-04	(Workstations) Installer files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	
		ML1-AC-05	(Workstations) Compiled HTML files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	
		ML1-AC-06	(Workstations) HTML applications files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	
		ML1-AC-07	(Workstations) Control panel applet files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	ML1-PA-01	An automated method of asset discovery is run and reviewed at least fortnightly.	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimize vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Cyber Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn more** **Managed Vulnerability Service Data Sheet**
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	ML1-PA-02	A vulnerability scanner with an up-to-date vulnerability database is being used for vulnerability scanning activities.	
	A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.	ML1-PA-03	(Internet-Facing Services) A vulnerability scanner for internet-facing services is run and reviewed daily.	
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	ML1-PA-04	A vulnerability scanner is run and reviewed at least fortnightly to scan the organisation's office productivity suites, web browsers, email clients, PDF software and security products.	
	Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	ML1-PA-05	(Internet-Facing Services) The organisation has a process for identifying vulnerabilities in internet-facing services within 48 hours and has an example of where an available exploit has been identified and patched within 48 hours.	
		ML1-PA-06	(Internet-Facing Services) Applications with an exploit that has been available for greater than 48 hours are patched or mitigated.	
		ML1-PA-07	(Internet-Facing Services) Applications are patched or mitigated within two weeks.	
	Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	ML1-PA-08	The organisation has an effective process for patching office productivity suites, web browsers, email clients, PDF software and security products within one month.	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organization-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. **Learn more** **vCISO Data Sheet**

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Patch applications	Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	ML1-PA-09	Office productivity suites, web browsers, email clients, PDF software and security products do not have security vulnerabilities older than one month.	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimize vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Cyber Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn more** **Managed Vulnerability Service Data Sheet**
	Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	ML1-PA-10	The organisation has removed unsupported internet-facing services from the environment.	
		ML1-PA-11	The organisation has removed unsupported office productivity suites, web browsers, email clients, PDF software and security products from the environment.	
Configure Microsoft Office macro settings	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	ML1-OM-01	A technical solution exists that blocks Microsoft Office macros for users who are not approved under the Microsoft Office macro policy.	
		ML1-OM-02	A record is kept of users that have been approved to allow Microsoft Office macro execution, and this list matches the list of users within the technical solution.	
	Microsoft Office macros in files originating from the internet are blocked.	ML1-OM-03	Microsoft Office files from the internet are unable to execute Microsoft Office macros.	
		ML1-OM-04	Microsoft Office has been configured to block Microsoft Office macros from running in Microsoft Office files from the internet.	
	Microsoft Office macro antivirus scanning is enabled.	ML1-OM-05	The system has macroruntimescope enabled for Microsoft Office applications in registry settings or has an alternative Microsoft Office macro scanning ability in place.	
		ML1-OM-06	System anti-virus successfully detects a virus test signature inside of a Microsoft Office macro in a Microsoft Office file.	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting with endpoint threat prevention and endpoint detection and response capabilities. Our 24/7 SOC Cyber Analysts rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread. We work alongside you to determine the root cause, remediate with corrective actions and ensure you are protected against business disruption. Our best-of-breed MDR approach means we partner with leaders in endpoint protection (EPP) and endpoint detection and response (EDR) to deliver eSentire MDR for Endpoint. **Learn more** **MDR for Endpoint Data Sheet**
	Microsoft Office macro security settings cannot be changed by users.	ML1-OM-07	A standard user is unable to modify the security settings for Microsoft Office macros in all Microsoft Office applications.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
User application hardening	Web browsers do not process Java from the internet.	ML1-AH-01	Java content does not execute in Microsoft Edge.	
		ML1-AH-02	Java content does not execute in Google Chrome.	
		ML1-AH-03	Java content does not execute in Mozilla Firefox.	
	Web browsers do not process web advertisements from the internet.	ML1-AH-04	Web ads do not display in Microsoft Edge.	
		ML1-AH-05	Web ads do not display in Google Chrome.	
		ML1-AH-06	Web ads do not display in Mozilla Firefox.	
	Internet Explorer 11 does not process content from the internet.	ML1-AH-07	Internet Explorer 11 is unable to connect to internet sites. Internet Explorer 11 may be allowed to access internal web applications only.	
	Web browser security settings cannot be changed by users.	ML1-AH-08	Microsoft Edge settings cannot be changed by a standard user.	
		ML1-AH-09	Google Chrome settings cannot be changed by a standard user.	
		ML1-AH-10	Mozilla Firefox settings cannot be changed by a standard user.	
		ML1-AH-11	Internet Explorer 11 settings cannot be changed by a standard user.	
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested.	ML1-RA-01	A process exists and is enforced for granting privileged access to systems.	
	Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.	ML1-RA-02	Privileged accounts (excluding privileged service accounts) cannot access the internet or web services via a web browser or other mechanism.	
		ML1-RA-03	Privileged accounts are not configured with mailboxes and email addresses.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Restrict administrative privileges	Privileged users use separate privileged and unprivileged operating environments.	ML1-RA-04	All administrative activities are performed in an administrative environment that is segmented from the standard user network environment. A separate environment is provisioned for the use of privileged access and is not used for any other purpose.	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organization-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. **Learn more** **vCISO Data Sheet**
	Unprivileged accounts cannot logon to privileged operating environments.	ML1-RA-05	Unprivileged accounts are not able to logon to systems in the privileged environment.	
		ML1-RA-06	Unprivileged user prevented from using the PowerShell remote PSRemote windows feature.	
	Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	ML1-RA-07	A privileged account cannot be used to authenticate and interactively login to standard user workstations, or other unprivileged environments. Limited-permission administrative accounts can be used to meet business requirements in unprivileged environments, such as for help desk personnel.	
		ML1-RA-08	An unprivileged account logged into a standard user workstation cannot raise privileges to a privileged user.	
Patch operating systems	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	ML1-PO-01	An automated method of asset discovery is run and reviewed at least fortnightly.	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimize vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Cyber Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn more** **Managed Vulnerability Service Data Sheet**
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	ML1-PO-02	A vulnerability scanner with an up-to-date vulnerability database is being used for vulnerability scanning activities.	
	A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services.	ML1-PO-03	A vulnerability scanner is run and reviewed daily to scan the organisation's internet-facing services.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Patch operating systems	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices.	ML1-PO-04	A vulnerability scanner is run and reviewed at least fortnightly to scan the organisation's operating systems.	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimize vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Cyber Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn more** **Managed Vulnerability Service Data Sheet**
	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	ML1-PO-05	The organisation has an example of where an available exploit has been identified and patched within 48 hours.	
		ML1-PO-06	Internet-facing system that have a vulnerable operating system with an exploit that has been available for greater than 48 hours are patched or mitigated.	
		ML1-PO-07	Internet-facing systems that have a vulnerable operating system are patched or mitigated within two weeks.	
	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release.	ML1-PO-08	The organisation has an effective process for patching operating systems within one month.	
		ML1-PO-09	Operating systems that have a vulnerability are patched or mitigated within one month.	
	Operating systems that are no longer supported by vendors are replaced.	ML1-PO-10	The organisation has removed unsupported operating systems from the environment.	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organization-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. **Learn more** **vCISO Data Sheet**
Multi-factor authentication	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.	ML1-MF-01	The organisation has a verified and approved list of internet-facing services operating within the organisation.	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organization-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. **Learn more** **vCISO Data Sheet**
		ML1-MF-02	The organisational remote access desktop solution presents a MFA challenge when attempting to authenticate.	
		ML1-MF-03	Organisational internet-facing systems present a MFA challenge when attempting to authenticate.	
	Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	ML1-MF-04	Third-party internet-facing services that hold sensitive data are configured to require users to use MFA.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Multi-factor authentication	Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	ML1-MF-05	Third-party internet-facing services that hold non-sensitive data are configured to require users to use MFA.	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organization-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. **Learn more** **vCISO Data Sheet**
	Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.	ML1-MF-06	The organisational internet-facing services with non-organisational user presents a multi-factor challenge when attempting to authenticate by default.	
Regular backups	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.	ML1-RB-01	The organisation has a business continuity plan (BCP) that outlines their important data, software and configuration settings that require backing up.	
		ML1-RB-02	Important data, software and configuration settings are backed up and retained as per the timeframes outlined within the BCP.	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organization-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. **Learn more** **vCISO Data Sheet**
	Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.	ML1-RB-03	Important data, software and configuration settings are backed up in a synchronised manner using a common point in time.	
	Backups of important data, software and configuration settings are retained in a secure and resilient manner.	ML1-RB-04	Important data, software and configuration settings are backed up and retained in a secure and resilient manner.	
	Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.	ML1-RB-05	The organisation has documented evidence of a disaster recovery exercise being performed. This includes examples of where important data, software and configuration settings have been restored from backups.	
	Unprivileged accounts cannot access backups belonging to other accounts.	ML1-RB-06	Unprivileged users are unable to access backups that do not belong to them.	
	Unprivileged accounts are prevented from modifying and deleting backups.	ML1-RB-07	Unprivileged users are unable to modify and delete backups.	

MATURITY LEVEL TWO				
Mitigation Strategy	**Control Description**	**Test ID**	**Test Description**	**eSentire Service**
Application control	Application control is implemented on workstations and internet-facing servers.	ML2-AC-01	(Workstations & Internet-facing servers) A dedicated application control solution is implemented.	
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	ML2-AC-02	(Workstations & Internet-facing servers) The system is only able to execute approved executables.	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting with endpoint threat prevention and endpoint detection and response capabilities. Our 24/7 SOC Cyber Analysts rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread. We work alongside you to determine the root cause, remediate with corrective actions and ensure you are protected against business disruption. Our best-of-breed MDR approach means we partner with leaders in endpoint protection (EPP) and endpoint detection and response (EDR) to deliver eSentire MDR for Endpoint. **Learn more** **MDR for Endpoint Data Sheet**
		ML2-AC-03	(Workstations & Internet-facing servers) The system is only able to execute approved software libraries.	
		ML2-AC-04	(Workstations & Internet-facing servers) The system is only able to execute approved scripts.	
		ML2-AC-05	(Workstations & Internet-facing servers) The system is only able to execute approved installers.	
		ML2-AC-06	(Workstations & Internet-facing servers) The system is only able to execute approved compiled HTML files.	
		ML2-AC-07	(Workstations & Internet-facing servers) The system is only able to execute approved HTML applications.	
		ML2-AC-08	(Workstations & Internet-facing servers) The system is only able to execute an approved control panel applets.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Application control	Allowed and blocked execution events on workstations and internet-facing servers are logged.	ML2-AC-09	(Workstations & Internet-facing servers) The system is logging the application control product when it allows and blocks execution.	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting with endpoint threat prevention and endpoint detection and response capabilities. Our 24/7 SOC Cyber Analysts rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread. We work alongside you to determine the root cause, remediate with corrective actions and ensure you are protected against business disruption. Our best-of-breed MDR approach means we partner with leaders in endpoint protection (EPP) and endpoint detection and response (EDR) to deliver eSentire MDR for Endpoint. **Learn more** **MDR for Endpoint Data Sheet**
Patch applications	A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	ML2-PA-01	A vulnerability scanner is run and reviewed at least weekly to scan the organisation's office productivity suites, web browsers, email clients, PDF software and security products.	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimize vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Cyber Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn more** **Managed Vulnerability Service Data Sheet**
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.	ML2-PA-02	A vulnerability scanner is run and reviewed at least fortnightly to scan the organisation's other applications.	
	Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.	ML2-PA-03	The organisation has an effective process for patching office productivity suites, web browsers, email clients, PDF software and security products within two weeks.	
		ML2-PA-04	Office productivity suites, web browsers, email clients, PDF software and security products do not have security vulnerabilities older than two weeks.	
	Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release.	ML2-PA-05	Other applications that have a vulnerability are patched or mitigated within one month.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Configure Microsoft Office macro settings	Microsoft Office macros are blocked from making Win32 API calls.	ML2-OM-01	Microsoft Office macros in Microsoft Office files are unable to make Win32 API calls.	
	Allowed and blocked Microsoft Office macro execution events are logged.	ML2-OM-02	Allowed execution of a Microsoft Office macro within a Microsoft Office file is logged.	**eSentire MDR for Log** eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises, or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting-edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM. **Learn More** **MDR for Log Data Sheet**
		ML2-OM-03	Blocked execution of a Microsoft Office macro within a Microsoft Office file is logged.	
User application hardening	Microsoft Office is blocked from creating child processes.	ML2-AH-01	Microsoft Office files cannot create child processes.	
	Microsoft Office is blocked from creating executable content.	ML2-AH-02	Microsoft Office files cannot create executable content.	
	Microsoft Office is blocked from injecting code into other processes.	ML2-AH-03	Microsoft Office files cannot inject code into other processes.	
	Microsoft Office is configured to prevent activation of OLE packages.	ML2-AH-04	Microsoft Office files do not execute OLE packages.	
	Microsoft Office security settings cannot be changed by users.	ML2-AH-05	Microsoft Office security setting are unable to be modified by a standard user account.	
	PDF software is blocked from creating child processes.	ML2-AH-06	PDF software cannot create child processes.	
	PDF software security settings cannot be changed by users.	ML2-AH-07	PDF software security settings are unable to be modified by a standard user account.	
	ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.	ML2-AH-08	The Microsoft guidance for hardening Microsoft Edge is implemented.	
		ML2-AH-09	The Google guidance for hardening Google Chrome is implemented.	
		ML2-AH-10	The ACSC guidance for hardening Microsoft Office is implemented OR The Microsoft guidance for hardening Microsoft Office is implemented.	
		ML2-AH-11	Vendor guidance for hardening PDF software is implemented.	
	Blocked PowerShell script execution events are logged.	ML2-AH-12	PowerShell scripts that have been blocked are logged.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Restrict administrative privileges	Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.	ML2-RA-01	A process for disabling known privileged accounts exists and is enforced. Users are made aware of this requirement when being provisioned with a privileged account.	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organization-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. **Learn more** **vCISO Data Sheet**
		ML2-RA-02	There are no privileged accounts that have an Active Directory expiry date that is greater than 12 months or do not have an expiry date.	
	Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	ML2-RA-03	A process for disabling privileged accounts that have not been used for 45 days exists and is enforced by the entity. Evidence exists for the usage of the 45 days inactive disabling process, including support tickets or administrative logs that show accounts were disabled.	
		ML2-RA-04	There are no enabled privileged accounts that have a LastLogonDate that is greater than 45 days.	
	Privileged operating environments are not virtualised within unprivileged operating environments.	ML2-RA-05	Where a privileged environment is virtualised, the virtualised image is not located in an unprivileged environment. This includes virtual machines on a standard unprivileged SOE.	
	Administrative activities are conducted through jump servers.	ML2-RA-06	Servers are configured to not allow remote access traffic or connections from systems that are not jump servers.	
	Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.	ML2-RA-07	The Microsoft Local Administrator Password Solution (LAPS) or a similar solution is implemented on Windows workstations and servers.	
		ML2-RA-08	Services account passwords are generated to be long, unique and unpredictable. Service account passwords are stored in a secure location, such as a password manager or a Privileged Access Management solution.	
		ML2-RA-09	Passwords should be changed at least once every 12 months.	
	Privileged access events are logged.	ML2-RA-10	Successful and failed logins of privileged accounts are logged.	**eSentire MDR for Log** eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises, or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting-edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM. **Learn More** **MDR for Log Data Sheet**
	Privileged account and group management events are logged.	ML2-RA-11	Changes made to privileged accounts and groups within Active Directory are logged.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Patch operating systems	A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices.	ML2-OM-01	A vulnerability scanner is run and reviewed at least weekly to scan the organisation's operating systems.	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimize vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Cyber Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn more** **Managed Vulnerability Service Data Sheet**
	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release.	ML2-OM-02	The organisation has an effective process for patching operating systems within two weeks.	
		ML2-OM-03	Operating systems that have a vulnerability are patched or mitigated within two weeks.	
Multi-factor authentication	Multi-factor authentication is used to authenticate privileged users of systems.	ML2-MF-01	A privileged user who is performing administrative activities is required to respond to an MFA challenge at some point in the authentication lifecycle. This can be implemented when authenticating to a machine (such as a jump server) or when attempting to raise privileges. The organisation has a list of systems that have privileged users or support privileged functions.	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organization-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. **Learn more** **vCISO Data Sheet**
	Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	ML2-MF-02	The organisation requires that internet-facing services use multi-factor authentication that uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	
		ML2-MF-03	The organisation requires that privileged users utilise multi-factor authentication that uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	
	Successful and unsuccessful multi-factor authentication events are logged.	ML2-MF-04	The organisation's internet-facing systems log successful MFA attempts.	**eSentire MDR for Log** eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises, or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting-edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM. **Learn More** **MDR for Log Data Sheet**
		ML2-MF-05	Administrative access connections log successful MFA attempts.	
		ML2-MF-06	The organisation's internet-facing systems log unsuccessful MFA attempts.	
		ML2-MF-07	Administrative access connections log unsuccessful MFA attempts.	
Regular backups	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.	ML2-RB-01	Privileged users (excluding backup administrator accounts) are unable to access backups that do not belong to them.	
	Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	ML2-RB-02	Privileged users (excluding backup administrator accounts) are unable to modify and delete backups.	

MATURITY LEVEL THREE				
Mitigation Strategy	**Control Description**	**Test ID**	**Test Description**	**eSentire Service**
Application control	Application control is implemented on workstations and servers.	ML3-AC-01	(Servers) A dedicated application control solution is implemented.	
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set.	ML3-AC-02	(Servers) The system is only able to execute approved executables.	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting with endpoint threat prevention and endpoint detection and response capabilities. Our 24/7 SOC Cyber Analysts rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread. We work alongside you to determine the root cause, remediate with corrective actions and ensure you are protected against business disruption. Our best-of-breed MDR approach means we partner with leaders in endpoint protection (EPP) and endpoint detection and response (EDR) to deliver eSentire MDR for Endpoint. **Learn more** **MDR for Endpoint Data Sheet**
		ML3-AC-03	(Servers) The system is only able to execute approved software libraries.	
		ML3-AC-04	(Servers) The system is only able to execute approved scripts.	
		ML3-AC-05	(Servers) The system is only able to execute approved installers.	
		ML3-AC-06	(Servers) The system is only able to execute approved compiled HTML files.	
		ML3-AC-07	(Servers) The system is only able to execute approved HTML applications.	
		ML3-AC-08	(Servers) The system is only able to execute approved control panel applets.	
		ML3-AC-09	(Workstations & Servers) The system is only able to execute approved drivers.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Application control	Microsoft's 'recommended block rules' are implemented.	ML3-AC-10	(Workstations & Servers) The Microsoft recommended Block rules are configured on the system.	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting with endpoint threat prevention and endpoint detection and response capabilities. Our 24/7 SOC Cyber Analysts rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread. We work alongside you to determine the root cause, remediate with corrective actions and ensure you are protected against business disruption. Our best-of-breed MDR approach means we partner with leaders in endpoint protection (EPP) and endpoint detection and response (EDR) to deliver eSentire MDR for Endpoint. **Learn more** **MDR for Endpoint Data Sheet**
	Microsoft's 'recommended driver block rules' are implemented.	ML3-AC-11	(Workstations & Servers) The Microsoft recommended driver Block rules are configured on the system.	
	Application control rulesets are validated on an annual or more frequent basis.	ML3-AC-12	The organisational list of allowed applications rules are reviewed for accuracy with current business requirements and threat profiles.	
	Allowed and blocked execution events on workstations and servers are centrally logged.	ML3-AC-13	(Workstations & Servers) Application control event logs are sent to a centralised location.	**eSentire MDR for Log** eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises, or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting-edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM. **Learn More** **MDR for Log Data Sheet**
	Event logs are protected from unauthorised modification and deletion.	ML3-AC-14	Application control event logs are protected from unauthorised modification and deletion.	
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-AC-15	Application control event logs are monitored for signs of compromise.	
		ML3-AC-16	The organisation has an example where they investigated or responded to signs of compromise triggered by application control monitoring.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Patch applications	Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, or within 48 hours if an exploit exists.	ML3-PA-01	The organisation has an effective process for patching office productivity suites, web browsers, email clients, PDF software and security products within 48 hours, and has an example of where an available exploit has been identified and patched within 48 hours.	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimize vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Cyber Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn more** **Managed Vulnerability Service Data Sheet**
		ML3-PA-02	Office productivity suites, web browsers, email clients, PDF software and security products do not have security vulnerabilities older than 48 hours.	
	Applications that are no longer supported by vendors are removed.	ML3-PA-03	The organisation has removed unsupported applications from the environment.	
Configure Microsoft Office macro settings	Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.	ML3-OM-01	Microsoft Office is configured to only allow Microsoft Office macros to execute from trusted locations. OR Microsoft Office is configured to only allow Microsoft Office macros digitally signed by a trusted publisher to execute. OR Microsoft Office macros are only executed from within a sandbox environment.	
	Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.	ML3-OM-02	The organisational has a defined standard for validating and accepting Microsoft Office macros in Microsoft Office files before adding them to the trusted location.	
		ML3-OM-03	A user is not able to write a file into locations contained within the trusted locations list.	
	Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.	ML3-OM-04	Microsoft Office macros signed by an untrusted publisher are unable to execute, and users cannot change configuration or otherwise allow execution.	
	Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.	ML3-OM-05	The organisation has a process for validating the listed of trusted publishers on an annual or more frequent basis.	
	Allowed and blocked Microsoft Office macro execution events are centrally logged.	ML3-OM-06	Microsoft Office macro execution event logs are sent to a centralised location.	**eSentire MDR for Log** eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises, or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting-edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM. **Learn More** **MDR for Log Data Sheet**
	Event logs are protected from unauthorised modification and deletion.	ML3-OM-07	Microsoft Office macro execution event logs are protected from unauthorised modification and deletion.	
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-OM-08	Microsoft Office macro execution event logs are monitored for signs of compromise.	
		ML3-OM-09	The organisation has an example where they investigated or responded to signs of compromise triggered by Microsoft Office macro execution monitoring.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
User application hardening	Internet Explorer 11 is disabled or removed.	ML3-AH-01	Internet Explorer 11 has been uninstalled from the system. OR Internet Explorer 11 is not able to be opened due to an application control policy, group policy setting, or another mechanism.	
	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.	ML3-AH-02	.NET Framework 3.5 has been removed from the system by unselecting it from the list of optional Windows Features.	
		ML3-AH-03	Older .NET Frameworks are unable to be found in the registry.	
	Windows PowerShell 2.0 is disabled or removed.	ML3-AH-04	PowerShell 2.0 and below has been removed from the system and traces of it cannot be found in the registry.	
		ML3-AH-05	PowerShell cannot be downgraded to version 2.0 or below.	
	PowerShell is configured to use Constrained Language Mode.	ML3-AH-06	The default configuration for PowerShell on the system is to start in Constrained Language Mode.	
		ML3-AH-07	PowerShell will not allow a user to change to Full Language mode.	
	Blocked PowerShell script execution events are centrally logged.	ML3-AH-08	PowerShell script execution event logs are sent to a centralised location.	**eSentire MDR for Log** eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises, or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting-edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM. **Learn More** **MDR for Log Data Sheet**
	Event logs are protected from unauthorised modification and deletion.	ML3-AH-09	PowerShell script execution event logs are protected from unauthorised modification and deletion.	
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-AH-10	PowerShell script execution event logs are monitored for signs of compromise.	
		ML3-AH-11	The organisation has an example where they investigated or responded to signs of compromise triggered by PowerShell script execution monitoring.	
Restrict administrative privileges	Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.	ML3-RA-01	The existing users of systems and applications are provided with the correct level of privilege required to perform their duties.	
	Privileged accounts are prevented from accessing the internet, email and web services.	ML3-RA-02	Service accounts cannot access the internet or web services via a web browser or other mechanism. This might be due to a proxy configuration, system configuration, or another solution.	
		ML3-RA-03	Service accounts are not configured with mailboxes and email addresses. Note tests for Maturity Level One already cover internet restrictions for privileged accounts excluding service accounts.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Restrict administrative privileges	Just-in-time administration is used for administering systems and applications.	ML3-RA-04	Groups that are identified as having privileged access to systems and applications contain no active users.	
		ML3-RA-05	Users that are approved access to privileged administration groups are provided with access for a limited time to fulfil their duties. A Just-in-time administration solution has been successfully deployed and configured.	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimize vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Cyber Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn more** **Managed Vulnerability Service Data Sheet**
	Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.	ML3-RA-06	Windows Defender Credential Guard is enabled on the system.	
		ML3-RA-07	Windows Defender Remote Credential Guard is enabled on the system.	
	Privileged access events are centrally logged.	ML3-RA-08	Privileged access event logs are sent to a centralised location.	
	Privileged account and group management events are centrally logged.	ML3-RA-09	Privileged account and group management event logs are sent to a centralised location.	
	Event logs are protected from unauthorised modification and deletion.	ML3-RA-10	Privileged access event logs are protected from unauthorised modification and deletion.	
		ML3-RA-11	Privileged account and group management event logs are protected from unauthorised modification and deletion.	
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-RA-12	Privileged access event logs are monitored for signs of compromise.	
		ML3-RA-13	The organisation has an example where they investigated or responded to signs of compromise triggered by privileged access monitoring.	
		ML3-RA-14	Privileged account and group management event logs are monitored for signs of compromise.	
		ML3-RA-15	The organisation has an example where they investigated or responded to signs of compromise event triggered by privileged account and group management monitoring.	

eSentire MDR for Log

eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises, or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting-edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM.

Learn More
MDR for Log Data Sheet

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Patch operating systems	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, or within 48 hours if an exploit exists.	ML3-PO-01	Operating systems vulnerable to an exploit that has been available for greater than 48 hours are patched or mitigated.	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimize vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Cyber Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn more** **Managed Vulnerability Service Data Sheet**
	The latest release, or the previous release, of operating systems are used for.	ML3-PO-02	The minimum version of the operating system is the current, or previous release (N-1 version).	
Multi-factor authentication	Multi-factor authentication is used to authenticate users accessing important data repositories.	ML3-MF-01	The organisation has a list of important data repositories.	**eSentire Virtual CISO (vCISO) - Security Program Maturity Assessment** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measure your ability to address the latest cyber threats. As part of every engagement, we conduct an organization-wide Security Program Maturity Assessment (SPMA) based on the NIST framework. The assessment provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time. **Learn more** **vCISO Data Sheet**
		ML3-MF-02	Data repositories that have been listed as important require MFA to access.	
	Multi-factor authentication is phishing-resistant and uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	ML3-MF-03	The MFA implementation requires the use of a phishing-resistant solution.	
	Successful and unsuccessful multi-factor authentication events are centrally logged.	ML3-MF-04	MFA event logs are sent to a centralised location.	**eSentire MDR for Log** eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises, or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting-edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM. **Learn More** **MDR for Log Data Sheet**
	Event logs are protected from unauthorised modification and deletion.	ML3-MF-05	MFA event logs are protected from unauthorised modification and deletion.	
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-MF-06	MFA event logs are monitored for signs of compromise.	
		ML3-MF-07	The organisation has an example where they investigated or responded to signs of compromise triggered by MFA monitoring.	

Mitigation Strategy	Control Description	Test ID	Test Description	eSentire Service
Regular backups	Unprivileged accounts cannot access backups belonging to other accounts, nor their own accounts.	ML3-RB-01	Unprivileged users are unable to access backups, including their own.	
	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts, nor their own accounts.	ML3-RB-02	Privileged users (excluding backup administrator accounts) are unable to access backups, including their own.	
	Privileged accounts (including backup administrator accounts) are prevented from modifying and deleting backups during their retention period.	ML3-RB-03	Privileged users (including backup administrator accounts) are unable to modify and delete backups during their retention period.	

Build Resilience & Prevent Disruption with eSentire

Our cybersecurity services portfolio is designed to build cyber resilience, so your business can effectively anticipate, withstand, and recover from a cyberattack.

We provide 24/7 threat protection that is proactive, personalized and cost-effective.

Our powerful cloud-native, open eSentire XDR Platform ingests network, cloud, log, endpoint and identity signals, correlating indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes.

Our Cyber Resilience Team, comprised of 24/7 SOC Cyber Analysts, Elite Threat Hunters, Threat Response Unit (TRU), and your named Cyber Risk Advisor, acts as an expert extension of your team to investigate, contain and stop threats that have the potential to bypass automated security controls.

ANTICIPATE

Exposure Management Services

TAKE CONTROL OF CYBER RISK

Strategic services including Vulnerability Management, vCISO and Managed Phishing & Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.

WITHSTAND

Managed Detection & Response

PREVENT THREATS BECOMING BUSINESS DISRUPTING EVENTS

We deliver Response + Remediation you can trust. By combining our cutting-edge XDR platform, 24/7 threat hunting and security operations leadership, we hunt and disrupt known and unknown threats before they impact your business.

RECOVER

Incident Response & Digital Forensics

BE READY WITH THE WORLD'S FASTEST THREAT SUPPRESSION

Battle-tested Incident Commander level expertise, crime scene reconstruction and digital forensics investigations that can bear scrutiny in a court of law. The world's fastest threat suppression with a 4-hour SLA available with our IR Retainer.

Reach out to connect with an eSentire security specialist and build a more resilient security operation today.

Contact Us

If you're experiencing a security incident or breach, contact us 1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.