Service Attachment (SA) for Cloud Detection and Response Services

SA-CDR V1.3 REVISED 8/31/2021

This Service Attachment for Cloud Detection and Response Services ("SA-CDR") is between Centre Technologies, Inc. a Texas company (sometimes referred to as "Centre," "we," "us," "our," OR "Provider"), and the Customer found on the applicable Quote (sometimes referred to as "you," "your," OR "Customer"). Collectively, these two entities are known as the "Parties". The Service Attachment, the Quote, and the Master Services Agreement form the Agreement between the Parties.

The Parties further agree as follows:

1. SCOPE – SA-CDR SERVICES

Service Description

In connection with the Services listed in detail in your Quote for Centre Cloud Detection and Response Services powered by eSentire esCloud for IaaS (together known as "CDR"), Customers are entitled to the use of all services to be performed within the scope of this Service Attachment.

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

a) Remote Telephone Support shall be available 24 x 7 x 365.
b) Remote Email Support shall be available 24 x 7 x 365.

Centre will undertake problem management as soon as we become aware of an incident. All activity related to a given incident will be formally documented by Centre staff within Centre's Service/Ticket Management system. This will include all updates during the troubleshooting process up to final resolution. If a root cause can be determined it will be documented in the service ticket as well.

CDR is a managed service that provides real-time monitoring of potential threats to Customer systems, with the following standard services capabilities and modules (the "CDR Services"):

CDR combines cloud-native security technology with elite human threat hunting to keep Customer cloud environments safe from disruption, ensuring the Customer's entire cloud infrastructure is under careful watch with real-time visibility and continuous asset discovery. CDR only supports cloud environments hosted within the following cloud infrastructure providers: Amazon Web Service ("AWS"), Google Cloud Platform ("GCP") or Microsoft Azure.

CDR will:

- Pinpoint vulnerabilities, misconfigurations, and identify suspicious behaviors with eSentire's 24x7x365 SOC.
- Prevent cyberattackers from gaining a foothold with automated policy enforcement and proprietary attacker blacklists.
- Confirm malicious activity and eradicate threat presence with an elite team of eSentire Cyber Threat Analysts and Centre staff that act as an extension of Customer's security team.
- Resolve risks and harden Customers' environment against future attack with unlimited incident lifecycle support that ensures their cloud infrastructure is continuously optimized and hardened against evolving cloud risks.

2. CDR KEY BENEFITS

Gain Deep Level Infrastructure Insights

Automated asset discovery with real-time infrastructure insights into users, services and configuration changes establishes always-on infrastructure awareness.

Identify Potential Risks and Anomalous Behaviors

Cloud-native security controls with advanced analytics and purpose-built use cases proactively identifies risks and potential malicious activity.

Hunt Threats and Enforce Policies

Proprietary attacker blacklists, automated policy enforcement and an elite team of cyber threat hunters prevent and identify known and unknown attacks.

Respond and Optimize Cyber-Resiliency

Unlimited embedded incident response ensures threats are eradicated and infrastructure is optimized against future attack.

3. SERVICE CAPABILITIES

Monitoring and Visibility

Always-on infrastructure awareness.

Automatically identifies and tracks assets and changes to Customer's environments.

24x7x365 Monitoring.

Provides around the clock inspection of Customer's cloud infrastructure leveraging eSentire's SOC 2 accredited global Security Operation Centers working together with Centre's Network Operations Center ("NOC") Team and Security Analysts.

Prevention

Global Blacklist Integration.

Automatically addresses activity from malicious IP's, leveraging eSentire's proprietary blacklist of confirmed global attacker sources, curated by eSentire's global threat team.

Automated Policy Enforcement.

Prevents attackers from gaining a foothold within Customer's cloud environment with over 300 integrated best practice policies and automated enforcement.

Risk Identification and Threat Detection

Purpose-built technology with advanced analytics from the industry's leading Managed Detection and Response platform identifies critical exposures and potential threats including:

Anomalous activity.

Flags deviations from baseline behavior correlating changes to user privileges, group policies, access keys, and other configurations.

Exposed Services.

Identifies and remediates critical service exposures before threat actors have the opportunity to exploit.

Automatic crypto mining detection.

Reveals illicit activity that leverages the compute power of Customer's cloud environment to mine cryptocurrencies such as Bitcoin and Ethereum.

Account hijacking attempts and brute force attacks.

Detects potential account hijacking attempts by identifying unusual login activities such as concurrent attempts, peculiar geo-locations, and unknown browsers or operating systems.

Sensitive configuration updates.

Notifies eSentire SOC analysts and Centre NOC Team to sensitive modifications to ensure misconfigurations do not leave Customer's environment in a vulnerable state.

Hunting and Response

Integrated human threat hunting.

Elite security analysts perform deep forensic investigation aggregating and correlating disparate data from Customer's cloud environment and other sources to identify elusive threats.

Rapid remediation of threats and misconfigurations.

eSentire SOC analysts facilitate timely remediation of identified threats and policy violations reducing potential threat actor dwell time and exposures of Customer's cloud assets.

Full incident lifecycle support.

From initial detection to hardening Customer's environment against future attack, security experts support the Customer every step of the way.

Reporting, Compliance and Ongoing Protection

Compliance.

Policies and reporting align with common standards and regulatory bodies such as GDPR, PCI, CIS, and HIPAA.

Ongoing detector development.

Advanced detection, policy, and runbook developments keep the Customer on the cutting edge of anti-adversarial tactics and strategy.

Deployment.

CDR deployment will commence with a kickoff meeting which will provide the information required for onboarding, the associated process and expected timelines as well as a configuration worksheet, which will be used to collect the required information for on boarding.

Incubation and tuning phase.

After onboarding is completed, the CDR will enter an incubation phase, during which the service will not be in production and the SOC will not be monitoring the service 24x7x365. This phase has two goals:

1. **Prevention of alert flooding after onboarding.** Depending upon the cloud account configuration, after the initial on boarding of cloud accounts, there is potential for a flood of alerts. During the incubation and tuning phase, all alerts will be held within the Prisma Cloud service, therefore the Customer will not receive auto-notifications and eSentire's SOC will not receive alert notifications, as the result of detection criteria based on the approximately 400 policies.
2. **Identification of false positives.** eSentire will provide a tuning and incubation phase report outlining all alerts from the initial monitoring period of newly onboarded cloud accounts. Upon review, Centre will outline and advise eSentire which alerts are false positives and therefore should no longer be monitored.

eSentire will take Centre's feedback on false positives from the incubation phase report and dismiss alerts for the specific policy, on the specific cloud resource, ensuring that subsequent alerts for that policy do not fire for the specific cloud resource. The only exception is if the cloud resource is configured to be compliant with a policy but is then modified to be non-compliant again.

Alerts from the incubation report which Centre indicates are legitimate alerts, will be passed on to the production service phase. The incubation report will include instructions to assist the Centre with remediation of the specific alert. The Customer will have 30 days to complete an identified remediation suggestion, before a reminder of the outstanding alert will be issued by eSentire.

Production Service.

During production delivery of CDR, the Customer's instances are monitored in real-time, against the over 400 policies of 2CDR. eSentire's Tactical Threat Unit continuously researches new threats to cloud infrastructure and will publish additional threat detection policies to CDR as required. These new threat detections are added to all Customer instances of 2CDR, at no additional charge. The policies monitor for items such as:

- Misconfiguration of Cloud Resources
- Communication to/from IP's on eSentire's proprietary threat blacklist Anomalies in typical user/resource behavior (UEBA)
- Threats discovered in audit logs
- Potentially malicious network events

Policy Classifications.

The over 400 CDR policies, which define the criteria to fire an alert, are categorized into 4 classifications. Depending on the classification, eSentire will handle alerts as follows:

1. Alerts that are non-remediable by eSentire, non-investigable by eSentire.

   Such alerts are mainly mis-configuration items that will be sent to the Customer directly, via a ServiceNow ticket, since only the Customer can make the required cloud account configuration change or determine that a cloud resource is configured in a specific way for a reason. The alert details will include information on the policy criteria that caused the alert, details on the violating cloud resource and specific steps to remediate the condition.

2. Alerts that are remediable by eSentire, non-investigable by eSentire.

   Such alerts are mainly mis-configuration items that meet two criteria:

   a. eSentire is capable of making the required configuration change and
   b. the configuration violation is severe enough to warrant immediate action.

3. Alerts that are non-remediable by eSentire, investigable by eSentire.

   Such alerts are mainly the result of policies which identify potentially malicious behavior. These alerts will be forwarded to eSentire's SOC for investigation. eSentire's analysts will investigate each alert, attempting to identify information such as the threat actor, impacted cloud resource, severity of threat and remediation suggestions.

4. Alerts that are remediable and investigable by eSentire.

   Such alerts represent a combination of the criteria of sections 2 and 3 above, meaning they are both remediable by eSentire and have potential for investigative action.

Alert States.

The following outlines how alerts behave and the required action:

- **Open state.** Alerts have just been generated by CDR and are awaiting action by eSentire SOC for investigation.
- **Snoozed state.** Alerts are waiting on Customer action.

The Alerts that are non-remediable by eSentire, or alerts that are Non investigable by eSentire, will remain in this state until Centre either performs the remediation steps outlined or advises eSentire that the alert is a false positive and should be dismissed. In the case of an alert which was routed to the eSentire SOC, the eSentire Analyst has engaged Centre for information or provided remediation actions to Centre. The alert will remain in the Snoozed state until Centre performs the remediation steps or advises eSentire that the alert is a false positive.

- **Dismissed state.** Alerts have been identified by either eSentire SOC or Centre to be false positives. When an alert is dismissed, the CDR policy will no longer generate an alert for the specific offending cloud resource.
- **Closed state.** Alerts have had the remediation steps performed and the cloud resource which was identified in the alert is now compliant with the CDR policy criteria.

eSentire SOC Investigation Details

Alerts which are routed to the eSentire SOC for investigation will, in most cases, have a SOC Analyst perform an investigation into the details of the alert. The goal of the investigation will be to discover additional information associated with the alert condition, such as (where applicable):

- User account which made a potentially sensitive configuration change to a cloud resource.
- Unusual user activity, which occurred at the same time as a potentially sensitive configuration change (identification of potential account compromise).
- Identification of abnormal system resource utilization, as a result of malicious activity such as crypto mining.
- Identification of false positive alerts, filtering these out from alerts reported to Centre.

Centre/Customer & eSentire Responsibilities:

Task	Centre/Customer Responsibility	eSentire Responsibility
Grant required permissions within cloud accounts, to enable CDR.	•	
Provide required information to support onboarding of cloud accounts to CDR.	•	
Setup and configuration of cloud accounts within CDR.		•
Preparation of the incubation period report.		•
Return incubation period report to eSentire, complete with input on each alert.	•	
Performing service tuning based on input from Customer via the incubation period report.		•
Perform monitoring of the CDR service 365x24x7.		•
Provide detailed information regarding misconfiguration of cloud resources, enabling the Customer to perform required configuration changes within the cloud account.		•
Where possible and when the Customer has agreed during onboarding, perform remediation activities on behalf of the Customer.		•
Where applicable, perform investigations into the cause of an alert and provide investigation details to the Customer.		•
When requested, provide contextual information to aid in the investigation of an alert.	•	
Answer Customer questions about the CDR service, alerts, configuration or other items.		•
Provide the Customer with the opportunity to review the service status of CDR, including items such as: • Open alerts • Number of alerts triggered for reporting period • License utilization • Cloud accounts under protection		•

In event Customer fails to perform its obligations in the time and manner specified or contemplated above, or should any assumption outlined herein with respect to the CDR Services fail to be valid or accurate, then neither Centre or eSentire will be responsible for any related delay or damages. If Customer fails to notify Centre of network changes as contemplated above, then Centre and eSentire shall be released from any and all obligations to monitor the Customer's network until Customer has notified Centre of such change.

Service Level Objectives

Scope

eSentire will monitor the cloud infrastructure for potential threats and respond accordingly. When potentially malicious activity is identified, eSentire will perform an investigation and will respond according to the identified threat.

Additional confirmation from Centre may be needed depending on the information available to the analyst at the time of the investigation. The ability for the eSentire SOC to perform an investigation and decide whether a threat is malicious, is dependent upon Centre and Customer successfully completing the required configuration steps in the Customer's cloud infrastructure, as outlined in the CDR setup and configuration guide provided during on boarding.

eSentire and Centre establish the following response time goals:

Severity Priority	Description	Notification & Escalation
Low (P3)	Alerts at this level are mainly inclusive of cloud resources which do not comply with industry best practice configuration guidelines.	Alert to Customer directly (via ServiceNow ticket) within 60 minutes of determination of the security event by the SOC after it has been received into the eSentire platform.
Medium (P2)	Alerts at this level include misconfigurations, which have greater impact, suspicious activity which is not linked to an active exploit or other non-critical findings.	Alert to Customer (via ServiceNow ticket) and response, if possible, by eSentire SOC analyst, within 60 minutes of determination of the security event by the SOC after it has been received into the eSentire platform.
High (P1)	Alerts at this level include verified malicious activity.	Alert to Customer (via ServiceNow ticket) and response, if possible, by eSentire SOC analyst, within 20 minutes of determination of the security event by the SOC

		after it has been received into the eSentire platform.

Maintenance Windows

Hardware firmware upgrades are performed only where necessary to resolve a specific issue or to address a critical vulnerability.

Service Provider reserves the right to deploy out of band emergency patches outside of established maintenance windows, with no advance notice, if deemed necessary and appropriate. If out of band patches are applied Centre will notify Customer as soon as possible.

Safety and Security Recommendations

Provider may make recommendations regarding safety and security related to Customer's network and practices. If Customer fails to adopt or implement the recommended protocols, Customer is responsible for any and all damages related to regulatory, security, privacy, or data protection, including but not limited to fines, data breach notification, malware or ransomware costs, restoration, forensic investigation, restoring backups, or any other costs or damages related to Customer's refusal to implement the recommended protocols.

4. NETWORK CHANGE COORDINATION

Significant Changes to Customer's Network

You will notify us via email of all significant proposed network changes and will provide us with at least thirty (30) days advance notice to provide opportunity to comment and follow-up regarding proposed changes.

Research Regarding Network Changes

Evaluation of network change requests sometimes will require significant research, design, and testing by Provider. These types of requests are not covered by this Service Attachment and will be billed at our then-current rates for time and materials.

5. SUITABILITY OF EXISTING ENVIRONMENT

Minimum Standards Required for Services

Customer represents, warrants and agrees that its existing environment meets the following requirements or will obtain upgrades to its existing environment to meet the following requirements:

Customer equipment must be maintained under manufacturer's warranty or maintenance contract or is in proper working order. Provider is not responsible for Customer equipment that is not maintained under manufacturer's warranty or maintenance contract or that is otherwise out of order. All fees, warranties, and liabilities against Provider assume equipment is under manufactures warranty or maintenance contracts or is in working order.

Provider in its reasonable opinion and supported by manufacturer information, may designate certain equipment or software as obsolete, defective or end of life (EOL) and therefore exclude it from coverage and performance metrics under this Agreement. This includes, but is not limited to, specific operating system builds/versions that are end of life and no longer supported by the manufacturer as shown below:

1. All servers with Operating Systems must be running current versions and have all of the latest Critical Updates installed and be patched within 30 days of the last patch.
2. All desktop PC's and notebooks/laptops with Operating Systems must be running current versions of software and have all of the latest Critical Updates installed and be patched within 30 days of the last patch.
3. All server and desktop software must be genuine, licensed and vendor supported.
4. The environment must have a currently licensed, vendor-supported hardware firewall between the internal network and the internet.
5. There must be an outside IP address assigned to a network device, allowing VPN access.

Costs required to bring Customer's environment up to these Minimum Standards are not included in this Agreement and shall be incurred and paid by Customer.

6. EXCLUSIONS

We are not responsible for failures to provide Services that are caused by the existence of any of the following conditions or otherwise that occur during any period of time in which any of the following conditions exist:

Customer Actions or Criminal Activity
Problems resulting from your actions or inactions that were contrary to our reasonable recommendations are covered in the MSA in Section 12.

Customer Responsibilities
Problems resulting from your failure to fulfill any responsibilities or obligations under our agreements.

Customer Resolution
Provider's ability to resolve problems due to Customer re-prioritizing Provider's recommendations.

Factors Beyond Provider's Control
Delays or downtime due to any factor outside of Provider's reasonable control.

Internet Connectivity Loss or Loss of Power
Loss of Internet connectivity or power at your location for any reason.

7. TERM AND TERMINATION

Term

This Service Attachment is effective on the Service Start Date identified in the Quote. Unless properly terminated by either party, this Service Attachment will remain in effect through the end of the term specified on the Quote (the "Initial Term"). Term, Renewal, and Termination are defined in the MSA and are hereby incorporated in this SA-CDR.

The remainder of this page is intentionally left blank.