eSENTIRE

Cloud Services – IaaS

The Service name was updated by eSentire from "esCLOUD for IaaS" to "Cloud Services - IaaS". All other content remains the same.

Service Description

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

Cloud Services will:

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

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.

Service Capabilities

Monitoring and Visibility

- **Always-on infrastructure awareness.** Automatically identifies and tracks assets and changes to Client's environments.
- **24x7x365 Monitoring.** Provides around the clock inspection of Client's cloud infrastructure leveraging eSentire's SOC 2 accredited global Security Operation Centers.

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.

Copyright © 2022 eSentire, Inc. All Rights Reserved.

- **Automated Policy Enforcement.** Prevents attackers from gaining a foothold within Client'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 can exploit.
- **Automatic crypto mining detection.** Reveals illicit activity that leverages the compute power of Client'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 to sensitive modifications to ensure misconfigurations do not leave Client'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 Client'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 Client's cloud assets.
- **Full incident lifecycle support.** From initial detection to hardening Client's environment against future attack, security experts support Client 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 Client on the cutting edge of anti-adversarial tactics and strategy.

Deployment

Cloud Service 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 onboarding.

Incubation and Tuning Phase

After onboarding is completed, the Cloud Service 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:

Copyright © 2022 eSentire, Inc. All Rights Reserved.

1. Prevention of alert flooding after onboarding. Depending upon the cloud account configuration, after the initial onboarding 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 Client 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, Client will outline and advise eSentire which alerts are false positives and therefore should no longer be monitored.

   eSentire will take the client'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 a client indicates are legitimate alerts, will be passed on to the production service phase. The incubation report will include instructions to assist Client with remediation of the specific alert. The client 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 Cloud for IaaS, Client's instances are monitored in real-time, against the over 400 policies of Cloud for IaaS. eSentire's Tactical Threat Unit continuously researches new threats to cloud infrastructure and will publish additional threat detection policies to Cloud for IaaS as required. These new threat detections are added to all Client instances of Cloud for IaaS, at no additional charge. The policies monitor for items such as:

1. Misconfiguration of cloud resources
2. Communication to/from IP's on eSentire's proprietary threat blacklist
3. Anomalies in typical user/resource behavior (UEBA)
4. Threats discovered in audit logs
5. Potentially malicious network events

Policy Classifications

The over 400 Cloud Service 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 Client directly, via a ServiceNow ticket, since only Client 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

Copyright © 2022 eSentire, Inc. All Rights Reserved.

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 bullets 1 and 2 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:

1. **Open State**. Alerts have just been generated by the Cloud Service and are awaiting action by eSentire SOC for investigation.
2. **Snoozed State.** Alerts are waiting on Client action.

The Alerts that are non-remediable by eSentire, or alerts that are non-investigable by eSentire, will remain in this state until Client 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 Client for information or provided remediation actions to Client. The alert will remain in the Snoozed state until Client performs the remediation steps or advises eSentire that the alert is a false positive.

1. **Dismissed State**. Alerts have been identified by either eSentire SOC or Client to be false positives. When an alert is dismissed, the Cloud Service policy will no longer generate an alert for the specific offending cloud resource.
2. **Closed State**. Alerts have had the remediation steps performed and the cloud resource which was identified in the alert is now compliant with the Cloud Service 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):

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

Client & eSentire Responsibilities

Task	Client responsibility	eSentire responsibility
Grant required permissions within cloud accounts, to enable the Cloud Service.	X	
Provide required information to support onboarding of cloud accounts to Cloud Service.	X	
Setup and configuration of cloud accounts within Cloud Service.		X
Preparation of the incubation period report.		X
Return incubation period report to eSentire, complete with input on each alert.	X	
Performing service tuning based on input from client via the incubation period report.		X
Perform monitoring of the Cloud Service 365x24x7.		X

Copyright © 2022 eSentire, Inc. All Rights Reserved.

Task	Client responsibility	eSentire responsibility
Provide detailed information regarding misconfiguration of cloud resources, enabling the client to perform required configuration changes within the cloud account.		X
Where possible and when the client has agreed during onboarding, perform remediation activities on behalf of the client.		X
Where applicable, perform investigations into the cause of an alert and provide investigation details to the client.		X
When requested, provide contextual information to aid in the investigation of an alert.	X	
Answer Client questions about the Cloud Service, alerts, configuration, or other items.		X
Provide the client with the opportunity to review the service status of Cloud Service, including items such as: • Open alerts • Number of alerts triggered for reporting period • License utilization • Cloud accounts under protection		✓

Service Level Objectives

The service levels outlined in this section will apply to the Cloud Services, in lieu of those contained on the Managed Detection and Response landing page. eSentire will monitor the Cloud Services 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 Client 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 Client successfully completing the required configuration steps its cloud infrastructure, as outlined in the Cloud Service setup and configuration guide provided during onboarding.

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 client 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 client (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 client (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

Copyright © 2022 eSentire, Inc. All Rights Reserved.