FAQs

CUSTOMER SECURITY OPERATIONS CENTER (CSOC)

IS THERE REDUNDANCY BUILT INTO CSOC SUPPORT?

CSOC and all security analysts maintain the ability to remotely monitor and respond to security events within our customer environments if the CSOC is unavailable.

HOW IS THE CSOC SAFEGUARDED?

All CSOC hosts and systems are safeguarded by two-factor authentication (badge and fingerprint scan). Access is granted only to CSOC members and appropriate Rackspace personnel.

WHAT IS RACKSPACE'S APPROACH TO BACKGROUND CHECKS OR SCREENINGS FOR EMPLOYEES, CONTRACTORS, CONSULTANTS AND VENDORS ASSOCIATED WITH ANY ASPECT OF THE CSOC?

All personnel undergo an extensive background check prior to being offered employment with Rackspace Managed Security.

DOES RACKSPACE PERMIT ON-SITE CSOC VISITS? IF SO, WHAT IS THE PROCESS FOR PLANNING THE VISIT?

On-site CSOC visits are permitted. They must be scheduled through your account team or the Rackspace Managed Security Customer Experience Team. Although customer entry into the CSOC is not permitted, there is a secure viewing area that can be visited during the CSOC tour and briefing.

DOES RACKSPACE MANAGED SECURITY MANAGE CUSTOMER FIREWALLS?

No. Rackspace Managed Security does not manage or maintain customer firewalls. However, the CSOC will ingest firewall logs as an additional level of context and visibility to aid in monitoring customer environments.

DOES RACKSPACE HAVE A MANAGED/MONITORED FIREWALL SERVICE?

Yes. Rackspace Firewall Manager lets you manage your security in real time via our customer portal. When you want to change permit rules or view destination server IP addresses and static rules, you can do it yourself.

Frequently Asked Questions

ARE THE SERVICES BEING OFFERED FOR ALL DEVICES WE HAVE AT RACKSPACE?

Rackspace Managed Security believes in providing customers with security solutions that enable their businesses. That means providing a consistent level of security across all devices and platforms that customers use to drive their businesses. Having launched in January 2016, Rackspace Managed Security is prioritizing the addition of Rackspace-supported platforms to the portfolio, and the service will be available on all supported platforms by mid-2017.

WHO IS RESPONSIBLE FOR RESOLVING IDENTIFIED SECURITY ISSUES?

Rackspace is responsible for remediating issues (with the customer's approval). After identifying a problem, we will develop a remediation plan. If the required actions were preapproved during the customer onboarding process, we will proceed to execute. However, if remediation falls outside the preapproved actions list, we will first seek approval from the customer before leveraging CSOC system administrators or other Rackspace support teams in order to the execute the remediation plan.

WHAT MONITORING AND NOTIFICATION PROCEDURES WILL BE IN PLACE FOR THIS SERVICE?

Monitoring and notification procedures will be outlined in the service-level agreements (SLAs) executed during the onboarding process for compliance assistance.

MANAGED SECURITY OFFERING – HOST AND NETWORK PROTECTION

WHAT ARE THE SYSTEM REQUIREMENTS FOR THE MONITORED ENVIRONMENT?

Host-based monitoring requires Windows 2008 R2 and above or REHL/CentOS 6.2 and above. Additional platform support (Debian/Ubuntu) is in development and should be available in Q3 of 2016.

HOW IS DATA GATHERED IN THE CSOC?

Rackspace integrates the Alert Logic platforms into the CSOC. This includes both processed alerts raised from the Alert Logic Security Operations Center and base data, such as NetFlow traffic data. The CSOC combines this information with the other monitoring being performed (e.g., host monitoring), as well as threat intelligence about the attack space and our knowledge of the environment, in order to develop a remediation plan for any alert.

WILL RACKSPACE MAINTAIN AND UPDATE SIGNATURES? HOW WILL THOSE SIGNATURES BE DETERMINED? CAN WE REQUEST THAT A SIGNATURE BE IMPLEMENTED BASED ON OUR INTEL? IF SO, WHAT IS THE SLA?

Signature updates are pulled from several sources, including the supplier of the product (e.g., CrowdStrike, Alert Logic, Imperva). We augment this information with Rackspace Threat Intelligence. We also have the capability within the CSOC to generate our own rules and could implement a rule based on your intel. However, this would be considered an ad hoc request and wouldn't be covered by an SLA.

HOW DO YOU PROVIDE METRICS, SUCH AS INFORMATION ABOUT THREATS THAT HAVE BEEN BLOCKED?

This information is incorporated into our incident reports and/or into our weekly and monthly reporting.

IS THERE A METHOD FOR RETRIEVING INCIDENT RESPONSE LOGS AND INVESTIGATION LOGS?

Yes. Customers have access to a web portal that provides direct access to all logging.

HOW IS THE LOG DATA DESTROYED AFTER DATA-RETENTION REQUIREMENTS EXPIRE?

Data expiration (deletion) is based on the customer data-retention policy specified in the sales contract. While log-retention periods range from 90 days to multiple years, customers frequently license for one year, in accord with the PCI-DSS mandate. Alert Logic utilizes a first-in-first-out (FIFO) method of deleting data that exceeds the retention-policy time period. A data volume that extends beyond the retention period is disconnected from SAN storage, whereupon the data volume is no longer accessible via the UI and can no longer accept new data. The storage vendor's delete functionality is utilized to completely delete the LUN from the SAN and then prepare the data block for re-utilization.

SECURITY ANALYTICS

WHAT IS SECURITY ANALYTICS? HOW DOES THE RACKSPACE CSOC GATHER AND ANALYZE DATA?

Security analytics is the method by which the CSOC ingests monitored environmental activity, alert and event data and all logs into a single platform, enabling a holistic view of event analysis and event identification for CSOC analysts. The analysts combine a traditional security information and event management (SIEM) platform with a best-in-breed big-data capability to create a "single pane of glass" for all event, log and environmental activity. This enables deeper investigation of alerts triggered by security tools, as well as analysis of raw data to identify anomalies on systems and customer networks that would not be detected by the tools themselves..

HOW WILL I BE NOTIFIED WHEN AN ISSUE IS IDENTIFIED, AND HOW QUICKLY?

Notification logistics will be outlined in service-level agreements (SLAs) during the onboarding process, and notifications will occur within 30 minutes of event identification.

HOW DOES THE CSOC ADDRESS FALSE POSITIVES?

The CSOC ingests and correlates all events and logging for all RMS customers into a big-data analytics solution, which acts as a "single pane of glass" for CSOC analysts and for rule and correlation generation. This allows CSOC analysts to quickly query, identify inefficiencies in rules and execute rule tuning from a central location across all customers to reduce false positives and monitor rules more efficiently.

WILL WE HAVE VISIBILITY INTO THE SIEM? WILL WE BE ABLE TO PULL REPORTS?

Reporting will be provided in accordance with SLAs. However, there is no direct access to the SIEM.

IS THERE A PORTAL FOR REVIEWING REPORTS, ALERTS AND THE STATUS OF SERVICE TICKETS?

Customers will continue to have access to tactical and ticket activity via their my.rackspace.com portal. Additionally, RMS will be developing a web portal that provides insight into their current security posture, as well as a repository for the reports that are delivered as part of RMS services.

VULNERABILITY MANAGEMENT

WHAT IS VULNERABILITY MANAGEMENT?

Rackspace utilizes scanning and agent technologies in order to understand the customer's environment, and then uses this data to tailor CSOC responses to threats and attacks in that environment.

HOW ARE THE SCANS DONE, AND HOW OFTEN?

The CSOC leverages Alert Logic Threat Manager IDS to execute vulnerability scans, using devices on individual customer networks for internal scans and shared scanning infrastructure for external scans. Vulnerability scans are performed every four weeks, and vulnerability data is analyzed by the CSOC Threat Intelligence Team, which further evaluates the risk to customers, taking into account their industry vertical. (The data is included in each customer's monthly security report.) The team then incorporates the data into customer-specific cyber hunting missions and daily security-monitoring operations to identify exploitation of known vulnerabilities. There are no limitations on the number of hosts, scope, etc.

ARE SCANS BASED ON A STANDARD LIKE PCI? FOR PCI SCANS, WILL AN AOC BE PROVIDED? ARE OTHER SCAN OPTIONS AVAILABLE?

By default, scanning is based on the PCI standard. However, scans are targeted to best suit a customer's architecture, data requirements, etc. Scans can also be configured by the customer.

COMPLIANCE ASSISTANCE OFFERING

DO YOU ACCOMMODATE AUDITORS FOR SECURITY CONTROLS AND COMPLIANCE?

Yes. The SLA will outline the reporting and notification necessary in order to meet auditing requirements.

CAN YOU MANAGE THE COMPLIANCE OF MY ENVIRONMENT?

No. Rackspace lessens the burden of compliance by providing the technical controls and associated reporting relevant to PCI. The Compliance Assistance Team also provides an advisory service to assist customers in understanding their compliance obligations.

DO YOU OFFER PENETRATION TESTING?

Yes. We currently partner with third-party vendors to provide this service.

DO YOU OFFER HARDENING OF IMAGES?

The Compliance Assistance Team will monitor your hosts and provide recommendations to ensure that the hardened state of those hosts is compliant. These recommendations can be approved by the customer and submitted to Rackspace support teams via the normal ticketing process.

rackspace®

Learn more at www.**rackspace**.com/**managed-security**