Service Specification

Managed Detection and Response Service

Vodafone Business Customers

1. Introduction

The Service is a fully managed service to proactively find, avoid or mitigate cyber attacks and malicious activity before they cause material business impact. Below are some of the key features of the Service:

- **Data Analysis:** Security Data is processed and analysed from security controls, network infrastructure, and endpoints to identify events of interest and correlate these events by source IP;
- **24/7 Alert Monitoring:** 24/7 alert monitoring and analysis is performed, identifying and escalating incidents through industry and Customer specific Intel;
- **Anomaly Detection:** Anomalous Traffic Detection is provided, data mining and statistical analysis for the purpose of identifying known and previously unknown malicious activity;
- **MDR Portal:** the MDR Portal presents a single-pane-of-glass to view account details, incident details, and to access our advanced reporting capability; and
- **Mid-Market Threat Intelligence:** insight provided into threats impacting similar industries and geographies and adversary Tools, Tactics and Procedures.

2. Customer Benefits

The aim of the Service is to help the Customer better manage and reduce its cyber security risk. There are several key benefits that the Service provides:

- **Comprehensive visibility:** MDR focuses on the full attack surface so that known and unknown threats can be detected and remediated;
- **Rapid identification and resolution of incidents:** together, the component parts of the MDR are designed to continuously monitor the Customer's Environment in order to identify anomalous and malicious activity. This enables the Customer to be aware of potential threats at a rapid pace;
- **Extension of the Customer's team:** a joint operating model and deep understanding of the Customer's Environment results in fewer false positives, more actionable insights, and faster remediation**;**
- **Customer experience:** the MDR Portal ensures the easy management of the Service and provides easy to understand data so the Customer can take informed decisions.
- **Simplicity of pricing:** the pricing of the Service is simplified by operating a per-node cost, rather than Events Per Second (EPS).
- **Surface what matters:** the Service brings together unparalleled global threat intelligence, the Log Collection Platform powered by multiple analytic engines, and highly skilled cyber warriors. This allows the Customer to filter through the noise and make informed decisions to mitigate the risk to their business.

3. Technical Architecture and Description

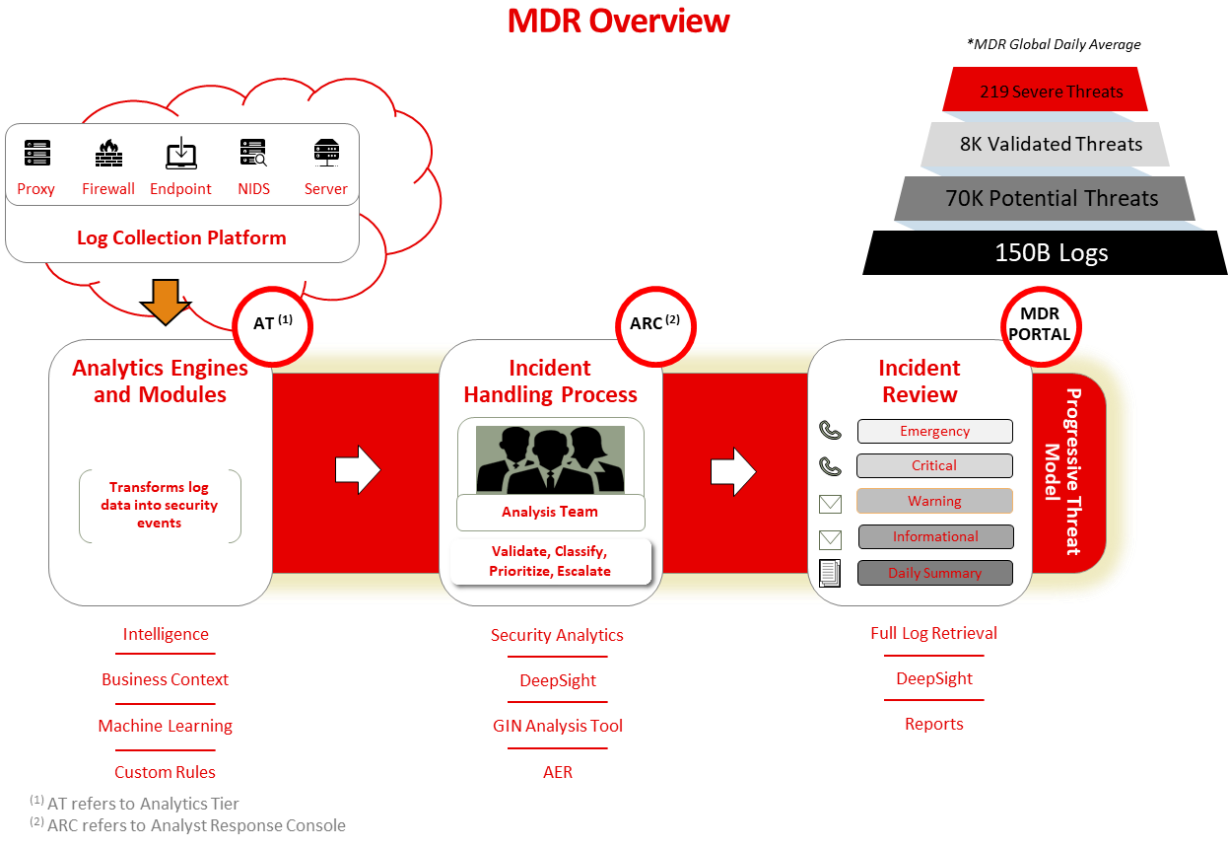


Figure 2: Key Elements of the Service

4. Log Collection & Transportation:

All Security Data is transported securely to the MDR Environment. MDR gathers Security Data from Customer Devices via the Log Collection Platform software. The Log Collection Platform securely and efficiently collects, compresses, and securely delivers Security Data to the MDR Environment for storage, analysis, and correlation. Security Data in transit and Security Data at rest is encrypted.

The Log Collection Platform transmits Security Data approximately every 5 minutes and sends a compressed file (at a ratio of 10:1) to the SOC over TLS. While the actual bandwidth requirement will vary based on the Log Events Per Second, this file is about the equivalent of sending an email with an attachment which for most of our customers is not significant from a bandwidth perspective.

Note: It is recommended to have the Log Collection Platform stood on a separate VM server with dedicated resources. It is not recommended to install it on any server which has high current utilization levels. The MDR team will share the Log Collection Platform Sizing Guide with the Customer and will also help the Customer to accurately scope the system requirements for an Log Collection Platform.

The Log Collection Platform uses syslog, APIs, database connections, or remote agents to collect Security Data from security Devices. Our Supported Product List (SPL), located in the "Downloads" section of the MDR Portal, details not

only what devices we support, but the preferred log collection method. The Service is truly vendor agnostic and we support a broad range of major vendors across endpoint, network, web and email technologies.

Logging Architecture

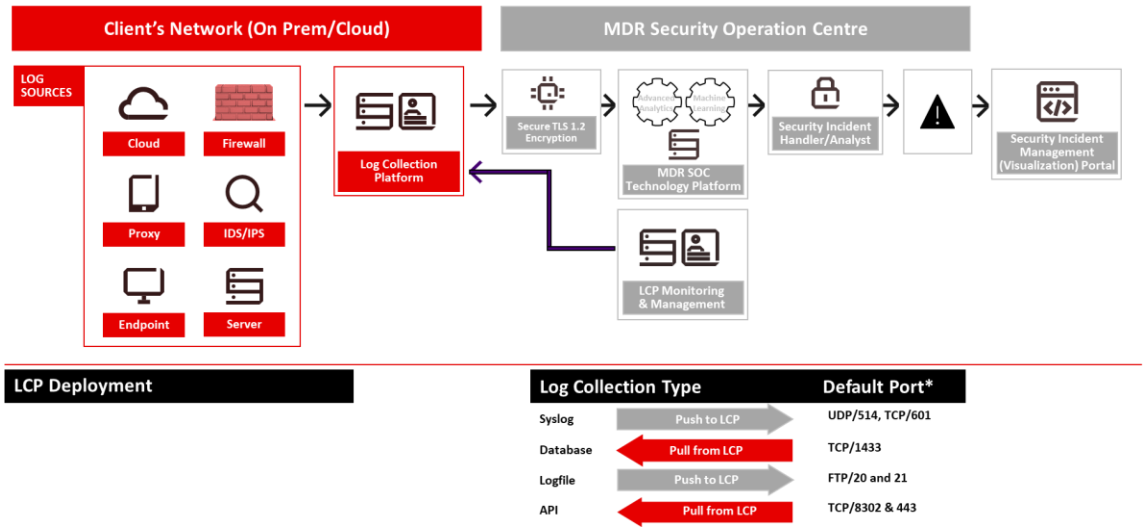


Figure 3: Logging Architecture

5. Analysis & Security Monitoring:

Once the Security Data reaches the Log Collection Platform, a data normalization engine automatically converts the Security Data into a single, standardized format. Normalized data is then stored in a distributed and extensive SQL database architecture. The Customer retains at least one dedicated database, which is used to store and analyse security data extracted from their network. The analytics engine provides continuous real-time analysis of security data that is produced by security devices (firewalls, NIDS, NIPS, HIDS, OS, applications, etc.). The analysis architecture is based upon the intelligent processing of the Log Collection Platform, a proprietary software and system architecture that MDR has designed to rapidly process, analyse, and reconstruct security events. Security data is continuously mined to isolate instances and/or patterns of potentially malicious activity. For example, through the analysis of firewall evidence, the data mining feature identifies hundreds of Trojan and malicious software packages. As part of this security monitoring, there's a focus on devices which generate the most value (as shown in the figure below):

Figure 4: Focus on Devices that Generate the Most Value

6. Security Event Analysis and Response:

Based upon pre-established escalation procedures, security analysts review and respond to potential malicious activity. Once analysts complete their review of a security event, they classify security incidents into four levels:

- **Informational** - Suspected security, compliance or audit activity. An unsuccessful attack which is unlikely to put the Customer's Environment at risk.
- **Warning** - Suspected attack or malicious activity with a low risk to the Customer's Environment. Incident may require additional investigation. Immediate response may not be required.
- **Critical** - Validated attack or malicious activity posing a moderate to high risk to the Customer's Environment. Immediate response to the incident is highly recommended.
- **Emergency** - Validated attack or malicious activity posing a high risk to the Customer's Environment. Immediate response to the incident is required to avoid additional impact to business

The analyst uses their experience, adversary knowledge, the evidence presented to them by Vodafone's analysis and intelligence systems, and the context they have about the Customer's Environment, assets and vulnerabilities to determine the likelihood that negative consequences will, or have, occurred. These two parameters (impact and likelihood) determine the resulting incident severity as described in the table below:

		Likelihood			
		Likely	Possible	Unlikely	Remote
Impact	Severe	Emergency	Critical	Warning	Informational
	High	Critical	Warning	Informational	
	Medium	Warning	Unpublished		
	Low	Informational			

Figure 5: Incident Severity Matrix

7. Presentation of Security Events:

All security incidents escalated to the Customer will be available for review on the MDR Portal. The MDR Portal includes at-a-glance summary pages, information on critical emerging threats, vulnerabilities, and recommendations on MDR's activity in response to security incidents and threats to the Customer's network.

The MDR Portal can be used as a single source to monitor, maintain, and report on an organizations' security posture. The MDR Portal is customizable to meet the Customer's needs with dashboards, KPI, and use filters to display only the most pertinent information to the organization. In addition, we support incident workflow and log query investigation. The Customer may also setup the MDR Portal to separate different internal functions and escalation paths. This allows for role separation and reporting whilst still having visibility across the whole organization.

The MDR Portal presents a real-time view of security incidents and can be used to generate a variety of queries and reports. There are over 100 pre-built reports that can be viewed online or downloaded in various formats. It allows the Customer to conduct reporting and querying of their Security Data received during the past 12 months.

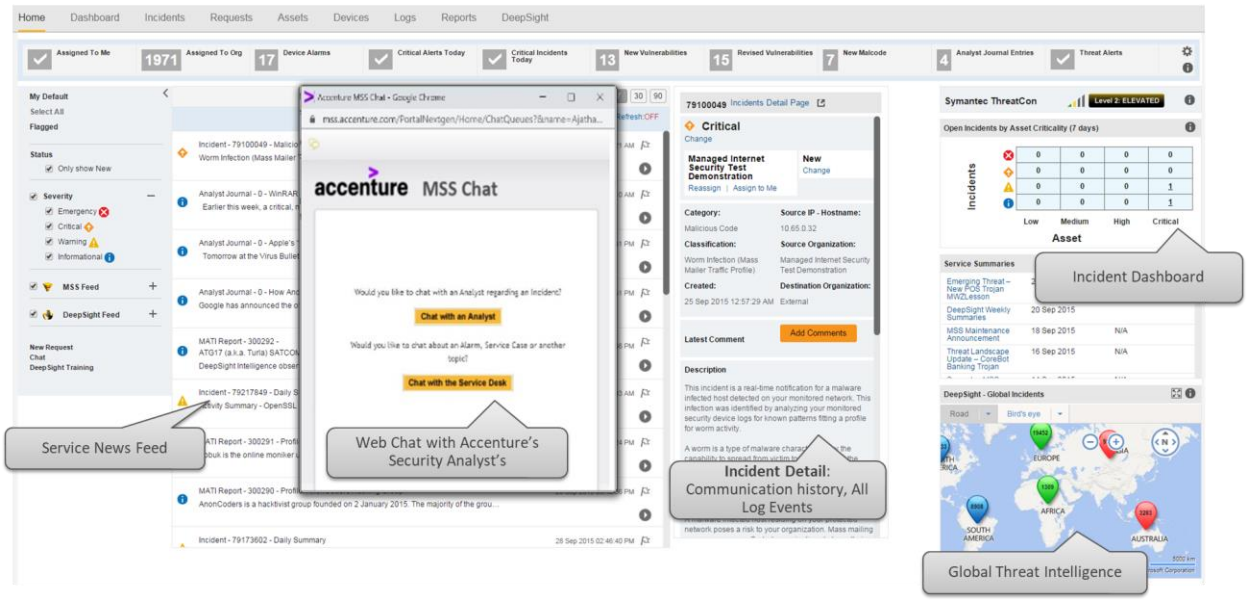


Figure 6: MDR Portal

8. The Onboarding Process

5 key steps are followed for onboarding the Customer for the Service:

- Kick Off Call
- Log Collection Platform Deployment
- Device Configuration
- MDR Backend Configuration
- Security Data Validation

This is shown in the figure below:

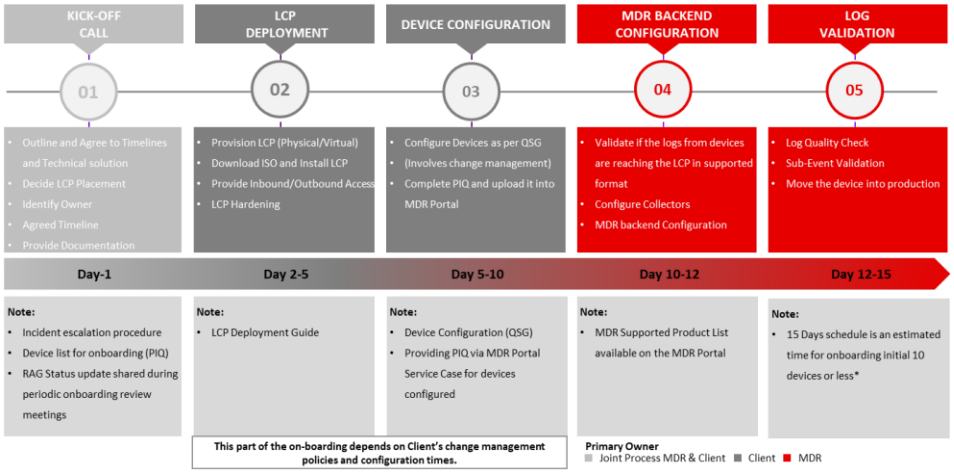


Figure 7: MDR Onboarding Process Overview

9. How the Customer can Interact With Vodafone

Vodafone operational delivery teams are organized to encourage interaction.

On any given day the Customer can interact with security analyst experts and technical engineers who specialize in detection and prevention of threats in their industry or geography and who are familiar with the Customer's teams, processes and infrastructure. This more intelligent focus results in the delivery team having a better understanding of the Customer's Environment and security objectives. A named Service Delivery lead will work with the Customer's teams to train users on using the optimal way to utilize the Service. These sessions can be scheduled via conference calls or virtual sessions. The named service delivery lead is also responsible for scheduling quarterly service reviews with the Customer's teams.

A customer team will consist of the following key roles:

Service Delivery Lead – A named Service Delivery Lead; who is the initial point of contact for questions, training and resolution of service delivery issues. They will act as a trusted advisor and advocate for the Customer inside our business along every step of service delivery.

Security Analysts Team – Will monitor and analyse Security Data using advanced tools and methodologies. They will operate as an extension of the Customer's security team. They investigate security events and incidents in real time, identify attacks, alert Customer contacts to threats and where applicable recommend countermeasures that can be taken.

Onboarding Engineer –A named Onboarding Engineer; who works in conjunction with the Customer's technical resources to integrate devices into the Service. They are responsible for keeping the Customer updated on progress, manage expectations, and help them understand what is required.

Qualifications Engineers Team – This team works closely with the onboarding engineer and technical resources to establish device connectivity and assist the Customer in configuring devices so that they are capable of generating events that we can monitor.

Technical Services Team – A specialized team of tech gurus who strive to ensure that we always receive the right (quality and quantity) Security Data from the monitored environment . They will assist with device configuration, software and security updates. Fix breakdowns and issues impacting the value of the services in a timely manner.

10. How We Provide Local Language Support

The Service operates both a regional as well as a global team to provide 24/7 real time monitoring services to Customer. Customer will be served by the local team based out of respective geographies during workdays and within regular business hours (9am to 5 pm). For requests outside of these hours, Customer will be served by the global team based out of India, in English.

11. Customer Deliverables

As part of the Service, the following key service deliverables will be provided to the Customer:

- Edge to Endpoint Monitoring
- 24*7 access to the MDR Delivery Team for assistance on questions & guidance related to incidents
- Device Onboarding – Log Collection Platform baselining, Hardening & collection configuration
- Realtime Security Data and event correlation
- Realtime security incident validation and notification
- Device logging monitoring and log outage notification
- Secure web portal access
- Standard monthly report & Catalogue reports

12. Service Level Agreements

The Service will be governed by the following SLAs:

SLA Reference	SLA Field	Metric
1	Severe Event Notification	10 minutes
2	SOC Infrastructure Up-time	99.90%
3	Device Onboarding for up to 10 Security Devices	Within 15 Working Days
4	Availability of Customer Monthly Report	5th Working Day of Each Month

13. Appendix

There are over 100 pre-built reports that can be viewed online or downloaded in various formats from the MDR Portal. It allows the Customer to conduct reporting and querying of its Secuirty Data received during the past 12 months.

The below table provides examples of these reports under relevant categories:

PCI	Sarbanes-Oxley Act (SOX)	Practice Guide 13 (GPG-13)	Incident Management	Log Monitoring	Service status
Administrative Access to Systems	Administrative Access to Systems	Administrative Access to Systems	Analyzed vs Validated Incidents	Customer Traffic	On Boarding Service Case Report
Audit Logs Access.	Application Access	Audit Logs Access	Attack Activity by Type	Device Details Report	Security Incident Service Case Detail Report
Audit Policy Changes	Audit Logs Access	Disabled Accounts	Daily Incidents	Device Status by Technology	
Database Rights Granted	Audit Policy Changes	File and Directory Access	Destination IP Addresses for Sub Incident	Device Summary	
Default Username Authentications	Disabled Accounts	Firewall Configuration Changes	Detailed Daily Summary report	Devices Reporting to Log Collection Platform	
Disabled Accounts	File and Directory Access	Logon Failures	Device Incident Summary	Event Logging Trend Report	
Disabled User Accounts with Failed Login Attempts	Logon Failures	Router Configuration Changes	Event Details	Overlapping Netblock Ranges	
Password Changes	Password Change Attempts	User Account Management Changes	Events Details Report	Overlay Device Logging Levels with Alarm Correlation	
User Account Management Changes	Security Log Management	User Accounts Created	External Attacks	Recurring Device Alarms Report	
User Accounts Created	User Account Management Changes	User Accounts Deleted	Hot IP Addresses.	Registered Networks	
User Accounts Deleted	User Group Management Changes	User Group Management Changes	Incident Closure Code Report.	Log Source Status	
User Logouts	User Logins	User Logins	Incident Funnel Count Details		
	User Logouts		Incident Mean Time To Resolution		
	Windows Account Policy Changes		Incident Status Report by Country		
			Incident Summary Report		
			Incident Types by Netblock		

			Incidents by Asset Group		
			Incidents Generated by Devices		
			Incidents Report		
			Incident Updates Report		
			Recurring IP Addresses		
			Reported Network Security Events Report		
			Security Incident Service Case Detail Report		
			Security Incident to Service Case Mappings		
			Security Incidents by Incident Type		
			Security Incidents by Month		
			Security Incidents by Severity		
			Security Incidents Dataset Report		
			Security Incidents for Destination IP		
			Security Incidents for SourceIP		
			Security Incidents Summary		
			Severe Incidents and Primary Signatures 7 Day view		
			Severe Incidents and Recurring Ips by Month		
			Severe Incidents by Month Per Organization		
			Severe Incidents By Org		
			Severe Incidents by Registered Netblock Range		
			Severe Recurring IPs		
			Signatures Triggered by Device.		
			Top Incident Types		
			Top Attacks		
			Top Targeted Assets		
			Top Ports Being Scanned		
			Top Internal Source IP Addresses		
			Traffic Blocked by Intrusion Prevention Systems		

Figure 9: List of Reports Available on the MDR Portal

Below are a selection of snapshots from the monthly customer reports available for download in the MDR Portal:

Security Incidents

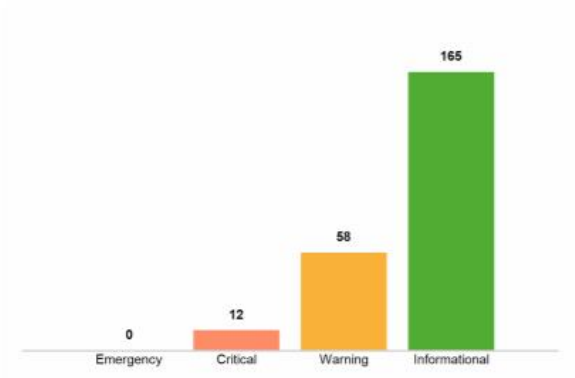
Incidents Monitor for May-2020

The inverted triangle demonstrates the value of the MSS detection, the removal of false positives (Potential versus Actual) and our prioritization of severe incidents. The balanced client portfolio ranges are based on a global sub set of clients who perform strongly on core service measures like technology coverage, incident triage, asset identification etc. The comparison of your detection ratio against the balanced client portfolio ranges is not an indicator of good or bad performance given the many variables involved, however a dramatic variance should be discussed with your service manager to understand the contributing factors.

Details	This Month	Last Month	3 Month Average	Your Detection Ratios	Balanced Client Portfolio Range
Comprehensive Log Collection	30,202,315,062	31,533,289,291	31,229,999,876		
Potential Incidents Analyzed	722	624	690	1 per 45 million Logs	1 per 2-3 million logs
Actual Incidents	235	201	226	1 per 3 Potential Incidents	1 per 5-15 Potential Incidents
Severe Incidents	12	15	21	1 per 10 Actual Incidents	1 per 10-20 Actual Incidents

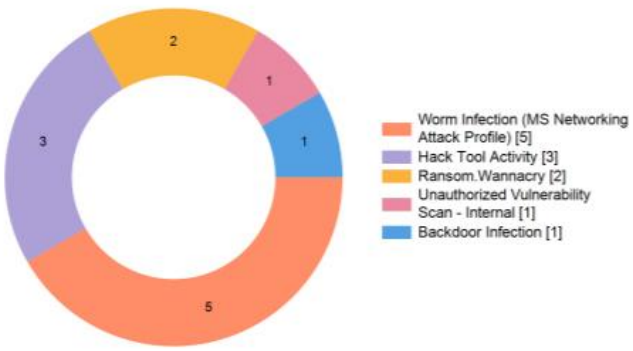
Incidents Validated for May-2020

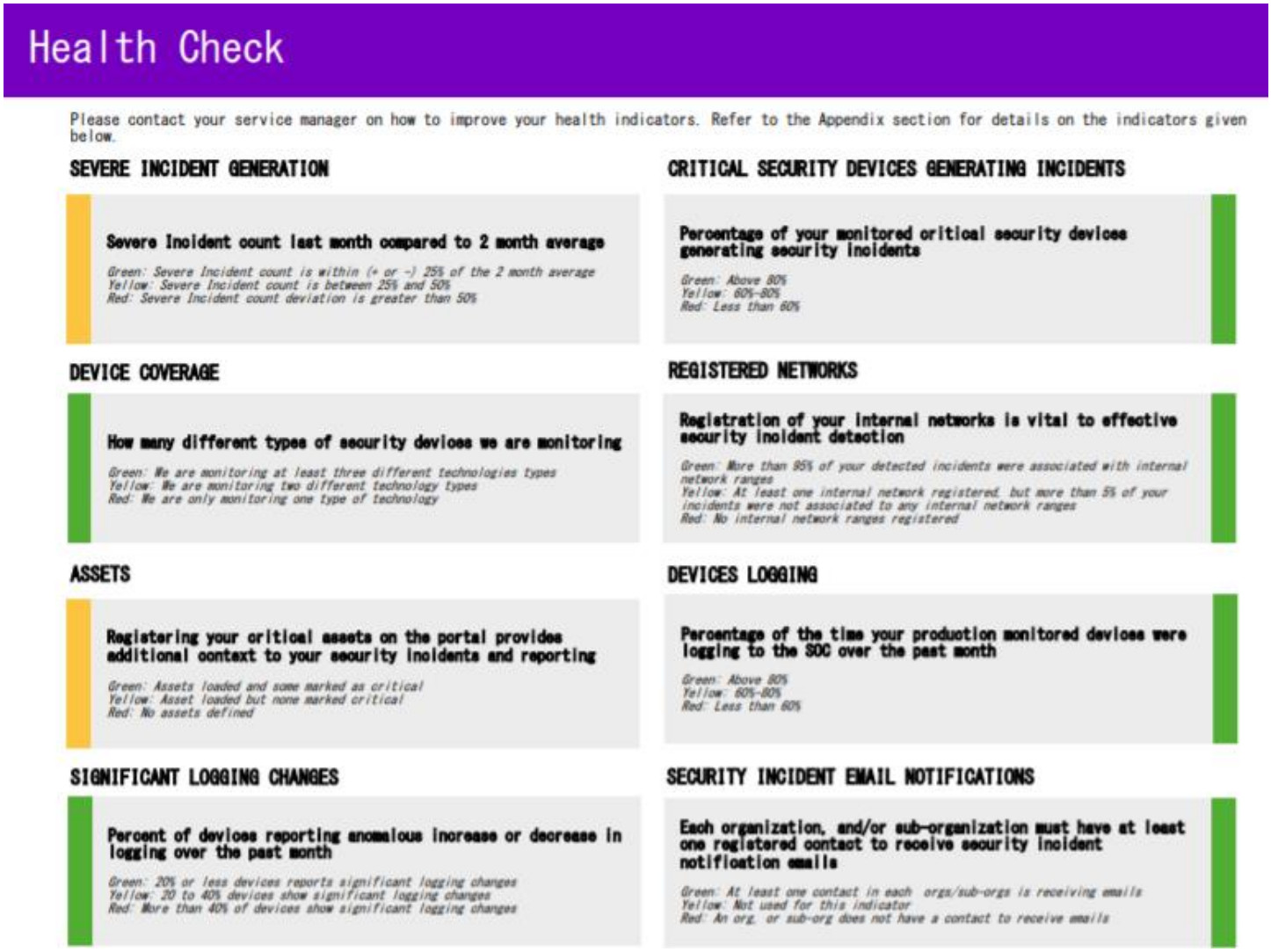
Security Incidents by severity



Emergency and Critical incidents

Top 10 Emergency and Critical incident types for May

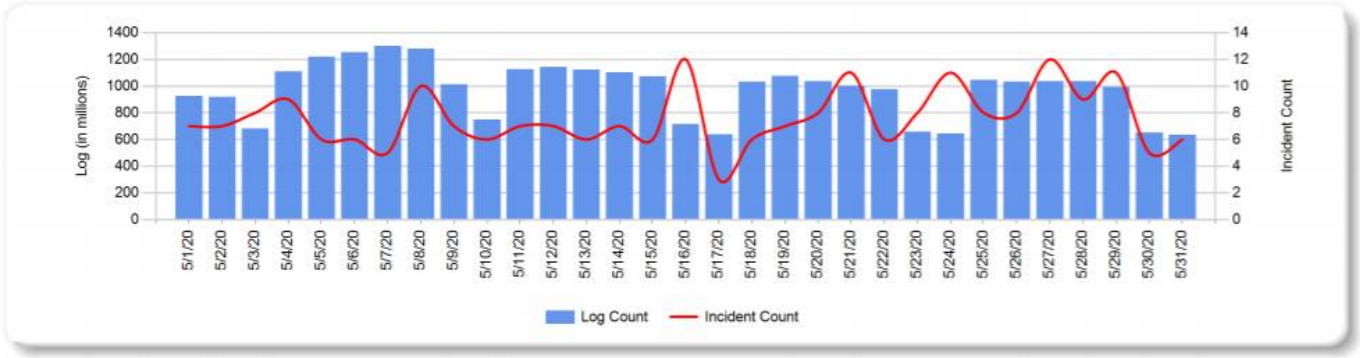




Logs vs Security Incidents

Data comparison of logs and incident for the past calendar month.

Daily Average Logs:**974 Million** Daily Average Incidents:**8**



Historical logging trend for the past 1 year