Security Information & Event Management

Version 5.1

Date – 04/08/2020

Document Ownership – Cyber Defence Center Team

genpact

Transformation
Happens Here

NOTICE

Version Control

Version No.	Version Date	Type of Changes	Author	Approver	Date of Next Review
1.0	July 2007	Initial Version	Srinivas Kalava	Surinder Rait	July 2008
1.1	Dec 2007	New Devices Added	Srinivas Kalava	Surinder Rait	Dec 2008
1.2	May 2008	New Devices Added	Srinivas Kalava	Surinder Rait	Dec 2008
1.3	Oct 2008	Device instance update	Srinivas Kalava	Surinder Rait	Dec 2008
1.4	Dec 2008	Document Revised	Vasant Raj	Surinder Rait	Jun 2009
1.5	31/03/2009	Change of NF Version	Srinivas Kalava	Surinder Rait	31/09/2009
1.6	08/06/2009	New location added	Sambit Kumar	Surinder Rait	31/12/2009
1.7	03/08/2009	Guatemala location added	Srinivas Kalava	Surinder Rait	31/12/2009
1.8	08/10/2009	Genpact Logo Changed & Team Structure Removed	Srinivas Kalava	Surinder Rait	31/12/2009
1.9	31/12/2009	Document Reviewed & New location added	Sambit Kumar	Satish Jagu	01/06/2010
2.0	27/04/2010	New locations added/ Poles Added (China & Europe)	Sambit Kumar	Satish Jagu	30/06/2010
2.1	01/07/2010	New Location Added for SMS Site	Sambit Kumar	Satish Jagu	31/12/2010
2.2	31/12/2010	Document Reviewed	Jinshu	Satish Jagu	01/06/2011
2.3	18/01/2011	Free signature download and risk mitigation	Jinshu	Satish Jagu	17/01/2012
2.4	01/08/2011	Document Reviewed	Jinshu	Satish Jagu	17/01/2012
2.5	18/01/2012	New Location Added for DDN, DUBAI, NF Agent installation in HYD-SEZ,	SOCNS	Satish Jagu	17/07/2012

2.5	25/09/2012	Reviewed	Md. Ateef	Satish Jagu	31/12/2012
2.5	30/12/2012	Reviewed	Sivaram	Satish Jagu	31/12/2013
2.6	10/02/2013	New Location Added	Sivaram	Satish Jagu	31/12/2013
2.7	30/12/2013	Reviewed	Nithin	Mandeep Singh	30/06/2014
2.8	26th June 14	Reviewed	Deepak	Mandeep Singh	27th Dec 2014
2.9	29th Dec 14	Content updated	Hemant Kumar	Mandeep Singh	29th June 2015
3.0	15-June-2015	Renamed document and elaborated details of deployment and architecture	Hemant Kumar	Vivek Attri	14-June-2016
3.0	15-May-2016	Reviewed, no change. Keeping expiry date as Q3 due to migration being done to Q-Radar	Neeraj Kumar	Vivek Attri	15-Sep-2016
4.0	09-Aug-2016	Updated document with QRadar details	Shyam Gubba	Satish Jagu	08-Aug-2017
4.1	10-Aug-2017	Document reviewed and updated; name of document changed	Aritra Gautam	Vivek Attri	09-Aug-2018
4.2	14-aug-2018	Document reviewed and updated, change in template, roles and responsibilities and team structure	Aritra Gautam	Vivek Attri	13-Aug-2019
4.3	13-Aug-2019	Document updated	Aritra Gautam	Vivek Attri	12-Aug-2020
4.4	11-Sep-2019	Document updated with changes in IR process	Aritra Gautam	Vivek Attri	10-Sep-2020
5.0	11-Mar-2020	Added the section on retention period, EPS calculation and annexure	Aritra Gautam	Vivek Attri	10-Mar-2021
5.1	04-Aug-2020	Added sections on Change management, threat intel and modifications in governance process	Aritra Gautam	Vivek Attri	03-Aug-2021

Contents

1. VIEWERSHIP

Cyber Defense Center, Compliance team & InfoSec Team

2. ABBREVIATIONS

NS: Network Security

WMG: Workstation Management group

EUC: End user computing

NIDS: Network Intrusion Detection System

SOC: Security Operating Center

DAPS: Data Availability and Prevention Service

NMG: Network Management Group

SMG: Server Management Group

SIM: Security Information Management

SIEM: Security Incident & Event Management

CDC: Cyber Defense Center

3. OBJECTIVE

This SOP is prepared as part of the Genpact Information security requirement. The primary purpose of this document is to create systematic work instructions on installation, deployment & configuration of QRadar SIEM. This document will form a basis for the Cyber Defense Center (CDC) procedures, which are more specific and dependent on infrastructure and Security tools.

4. SCOPE

The document is applicable for global usage while installing, deploying, configure, end-to-end operations and investigation of QRadar.

5. STAKEHOLDERS

Cyber Defense Center, Network Team, SUN Team, InfoSec, Corp IT

6. DEFINITION

This document explains implementation and operation of SIEM in Genpact environment. QRadar contain agents (collectors), database (processor) and GUI interface (console) which work together in order to provide functionality of SIEM tool. This implementation is in-line; document intends to detail the features and implementation procedures of said solution.

7. GUIDELINES

📖 Genpact Information Security Policy

Note: Passwords mentioned in this document are for explanatory purpose only.

8. INTRODUCTION

IBM® QRadar® SIEM consolidates log events and network flow data from thousands of servers, network devices and applications distributed throughout an organization. It normalizes and correlates raw data to identify security offenses and uses an advanced Sense Analytics engine to baseline normal behaviour, detect anomalies, uncover advanced threats, and remove false positives. As an option, this software incorporates IBM X-Force® Threat Intelligence, which supplies a list of potentially malicious IP addresses including malware hosts, spam sources and other threats. IBM QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents.

Provides real-time visibility

- Senses and detects inappropriate use of applications, insider fraud, and advanced low and slow threats that can be lost among millions of daily events.
- Collects logs and events from several sources including network assets, security devices, operating systems, applications, databases, and identity and access management products.
- Collects network flow data, including Layer 7 (application-layer) data, from switches and routers.
- Obtains information from identity and access management products and infrastructure services such as Dynamic Host Configuration Protocol (DHCP); and receives vulnerability information from network and application vulnerability scanners.

Reduces and prioritizes alerts

- Performs immediate event normalization and correlation for threat detection and compliance reporting.
- Reduces billions of events, flows into a handful of actionable offenses, and prioritizes them according to business impact.
- Performs activity baselining and anomaly detection to identify changes in behavior associated with applications, hosts, users and areas of the network.
- Uses IBM X-Force Threat Intelligence optionally to identify activity associated with suspicious IP addresses, such as those suspected of hosting malware.

Enables more effective threat management

- Senses and tracks significant incidents and threats, providing links to all supporting data and context for easier investigation.
- Performs event and flow data searches in both real-time streaming mode or on a historical basis to enhance investigations.

- Enables the addition of IBM QRadar QFlow and IBM QRadar VFlow Collector appliances for deep insight and visibility into applications (such as enterprise resource management), databases, collaboration products and social media through deep packet inspection of Layer 7 network traffic.
- Detects off-hours or unusual use of an application or cloud-based service, or network activity patterns that are inconsistent with historical usage patterns.
- Performs federated searches throughout large, geographically distributed environments.

Delivers security intelligence in cloud environments

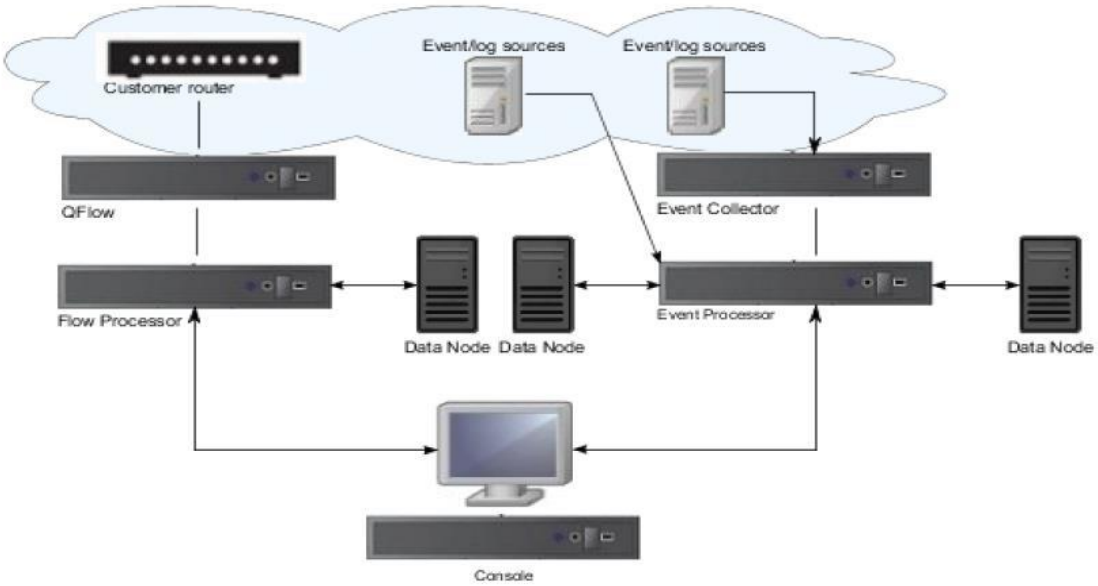
- Provides soft layer cloud installation capability
- Collects events and flows from applications running in both the cloud and on-premises
- Leverages the threat intelligence expertise of the IBM X-Force research and development team to provide a pre-emptive approach to security, and permits access to the IBM Security App Exchange for threat collaboration and management

Produces detailed data access and user activity reports

- Tracks all access to customer data by username and IP address to ensure enforcement of data-privacy policies.
- Includes an intuitive reporting engine that does not require advanced database and report-writing skills.
- Provides the transparency, accountability and measurability to meet regulatory mandates and compliance reporting.

9. QRADAR IMPLEMENTATION

9.1 QRADAR SIEM ARCHITECTURE



9.2 QRADAR SIEM COMPONENTS

9.2.1 QRadar QFlow Collector

Passively collects traffic flows from your network through span ports or network taps. The IBM Security QRadar QFlow Collector also supports the collection of external flow-based data sources, such as NetFlow. You can install a QRadar QFlow Collector on your own hardware or use one of the QRadar QFlow Collector appliances.

Restriction: The component is available only for QRadar SIEM deployments.

9.2.2 QRadar Console

Provides the QRadar product user interface. The interface delivers real-time event and flow views, reports, offenses, asset information, and administrative functions. In distributed QRadar deployments, use the QRadar Console to manage hosts that include other components.

9.2.3 Magistrate

A service running on the QRadar Console, the Magistrate provides the core processing components. You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events.

The Magistrate component processes events against the custom rules. If an event matches a rule, the Magistrate component generates the response configured in the custom rule.

For example, the custom rule might indicate that when an event matches the rule, an offense is created. If there is no match to a custom rule, the Magistrate component uses default rules to process the event. An offense is an alert processed by using multiple inputs, individual events, and events combined with analyzed behavior and vulnerabilities. The Magistrate component prioritizes the offenses and assigns a magnitude value based on several factors, including number of events, severity, relevance, and credibility.

9.2.4 QRadar Event Collector

Gathers events from local and remote log sources. Normalizes raw log source events. During this process, the Magistrate component, on the QRadar Console, examines the event from the log source and maps the event to a QRadar Identifier (QID). Then, the Event Collector bundles identical events to conserve system usage and sends the information to the Event Processor

When to deploy Event Collectors:

- Use the QRadar Event Collector 15xx in remote locations with slow WAN links. The Event Collector appliances do not store events locally. Instead, the appliances collect and parse events before sending events to an Event Processor appliance for storage.
- The Event Collector can use bandwidth limiters and schedules to send events to the Event Processor to avoid WAN limitations.
- The Event Collector is assigned an EPS license that matches the connected Event Processor.

9.2.5 QRadar Event Processor

Processes events collected from one or more Event Collector components. The Event Processor correlates the information from QRadar products and distributes the information to the appropriate area, depending on the type of event.

The Event Processor also includes information gathered by QRadar products to indicate behavioral changes or policy violations for the event. When complete, the Event Processor sends the events to the Magistrate component.

When to deploy Event Processors:

- If your event rate exceeds the rating for a standard Qradar collector, i.e. 5000 EPS, you must add a QRadar Event Processor 16xx or 18xx.
- If you collect and store events in a different country or state, you may need to add Event Processors to comply with local data collection laws.

9.2.6 Data Node

Data Nodes enable new and existing QRadar deployments to add storage and processing capacity on demand as required. Data Notes increase the search speed on your deployment by allowing you to keep more of your data uncompressed.

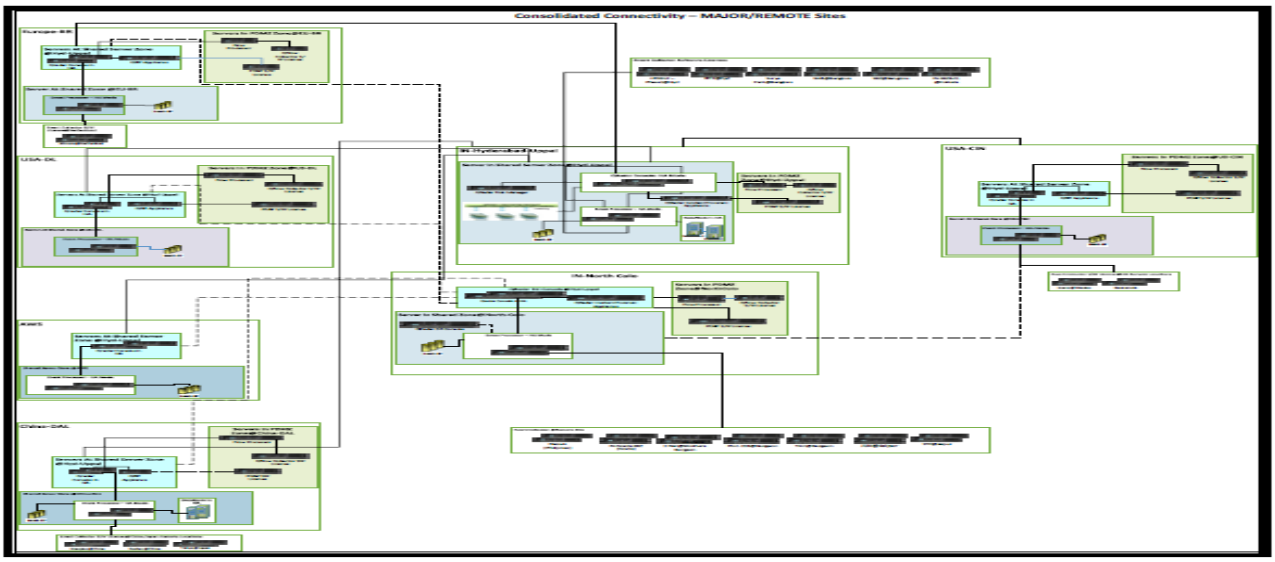
When to deploy Data nodes:

- When the event rate exceeds the rating for a standard Qradar processor, i.e. 40,000 EPS
- When you required additional processing and computational power as well as increased storage capacity

9.3 DEPLOYMENT (ARCHITECTURE) DIAGRAM

9.3.1 The Physical Nodes relationship diagram

Provides a detailed illustration of logical QRadar Architecture and connection details



9.3.2 Logical Node Mapping Diagram

The physical mapping of the QRadar appliances for each Genpact India Data Centre in scope is provided, along with the cluster QRadar appliance pair where deployed. Details in term of IP connectivity attributes assigned to each Physical Node provided within a dedicated section.

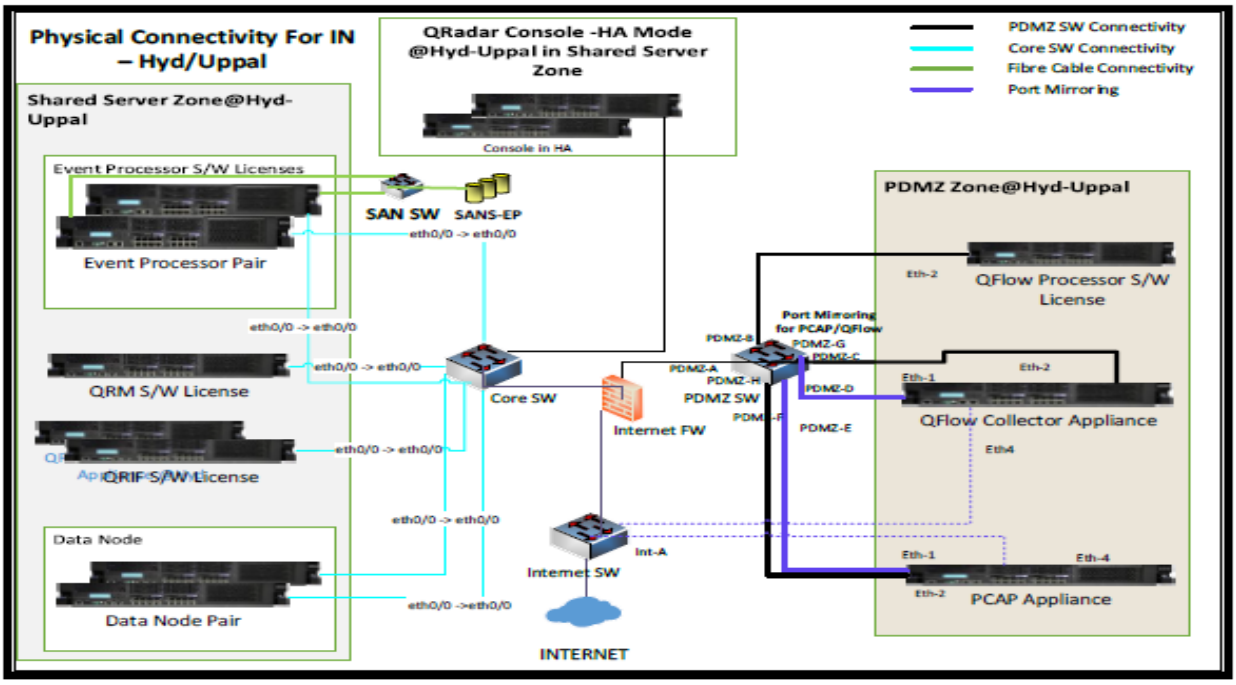


Fig – Physical Connectivity for IN-Hyd/Uppal

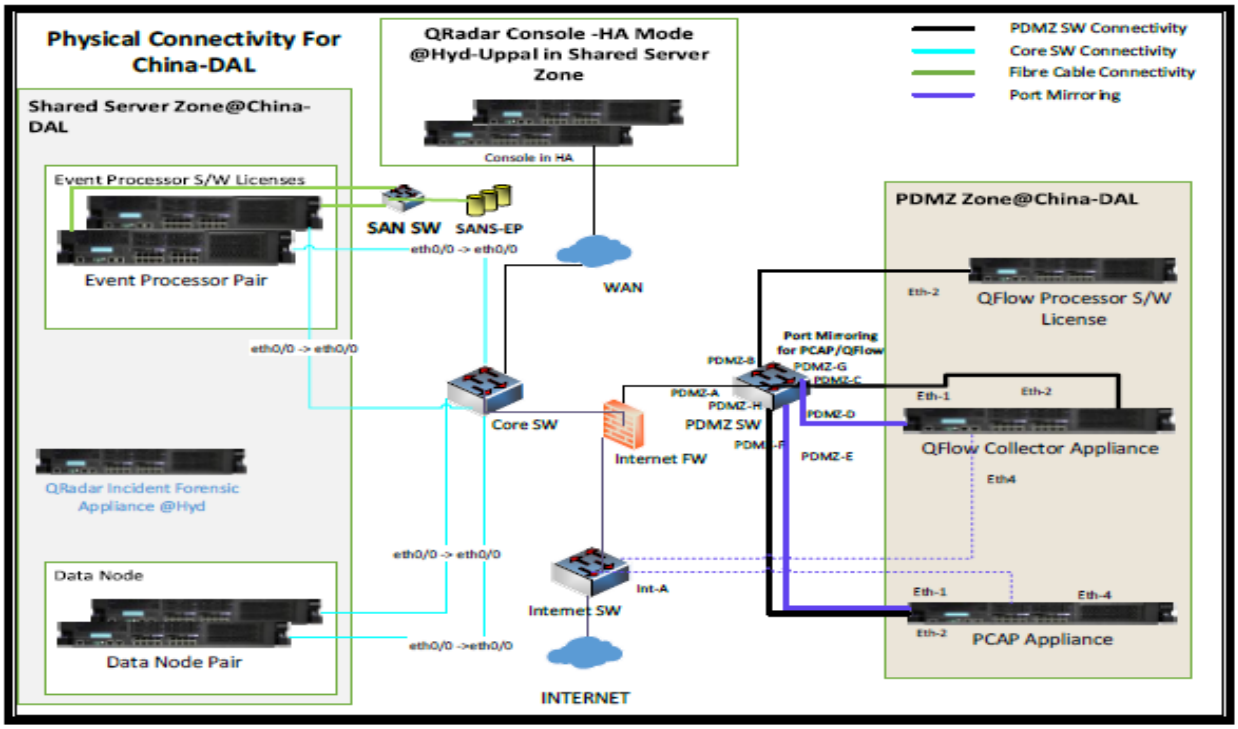


Fig – Physical Connectivity for China-DAL

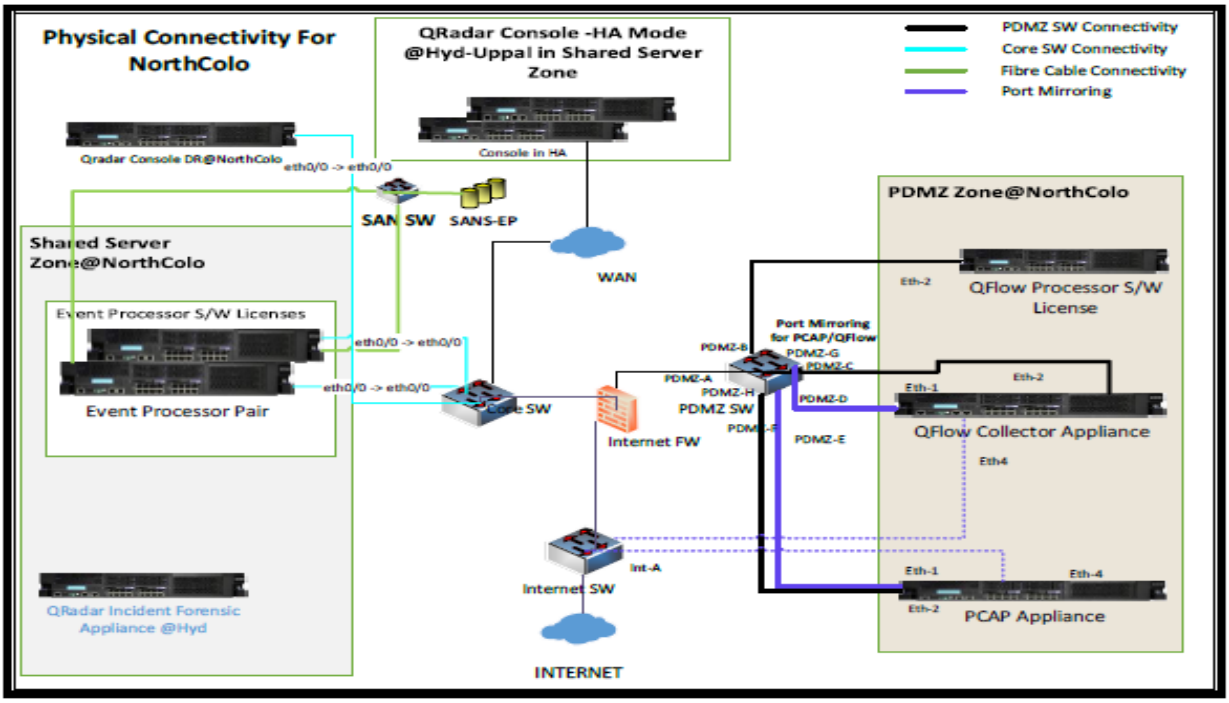


Fig – Physical Connectivity for NorthColo

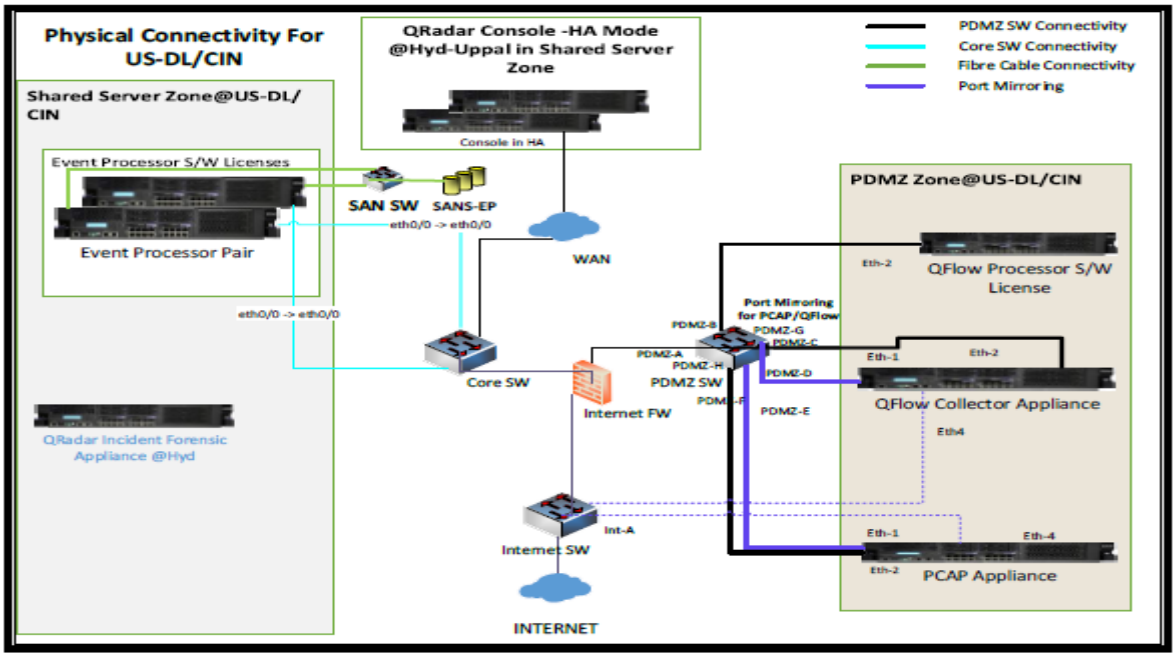


Fig – Physical Connectivity for US-DL/CIN

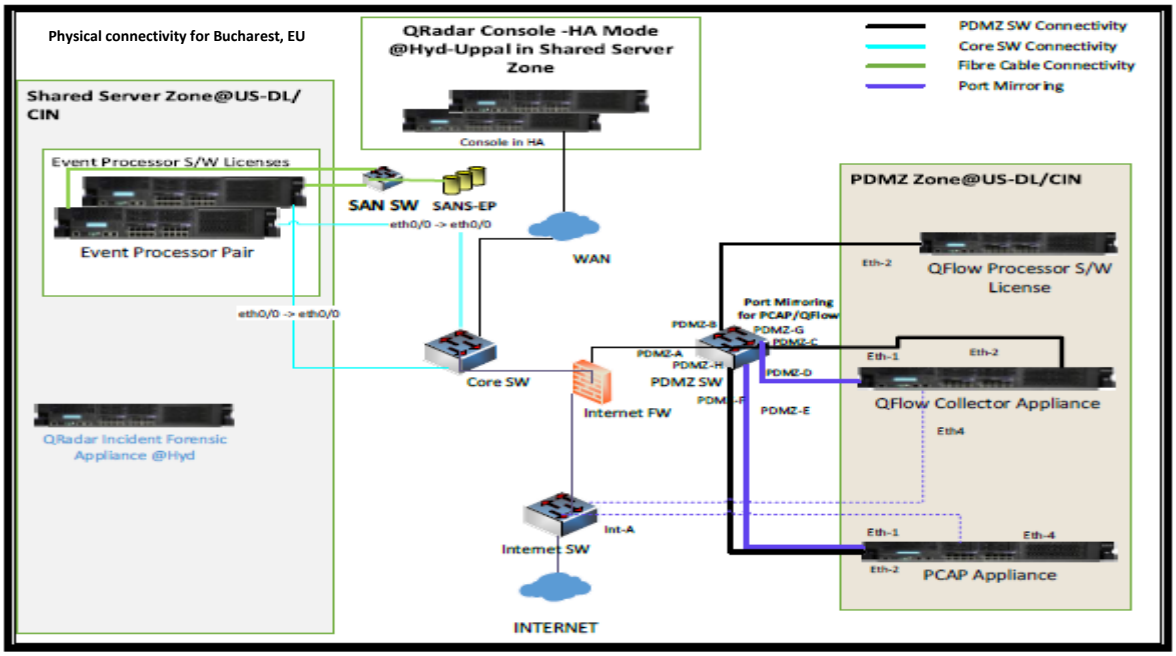


Fig - Physical connectivity for Bucharest, EU

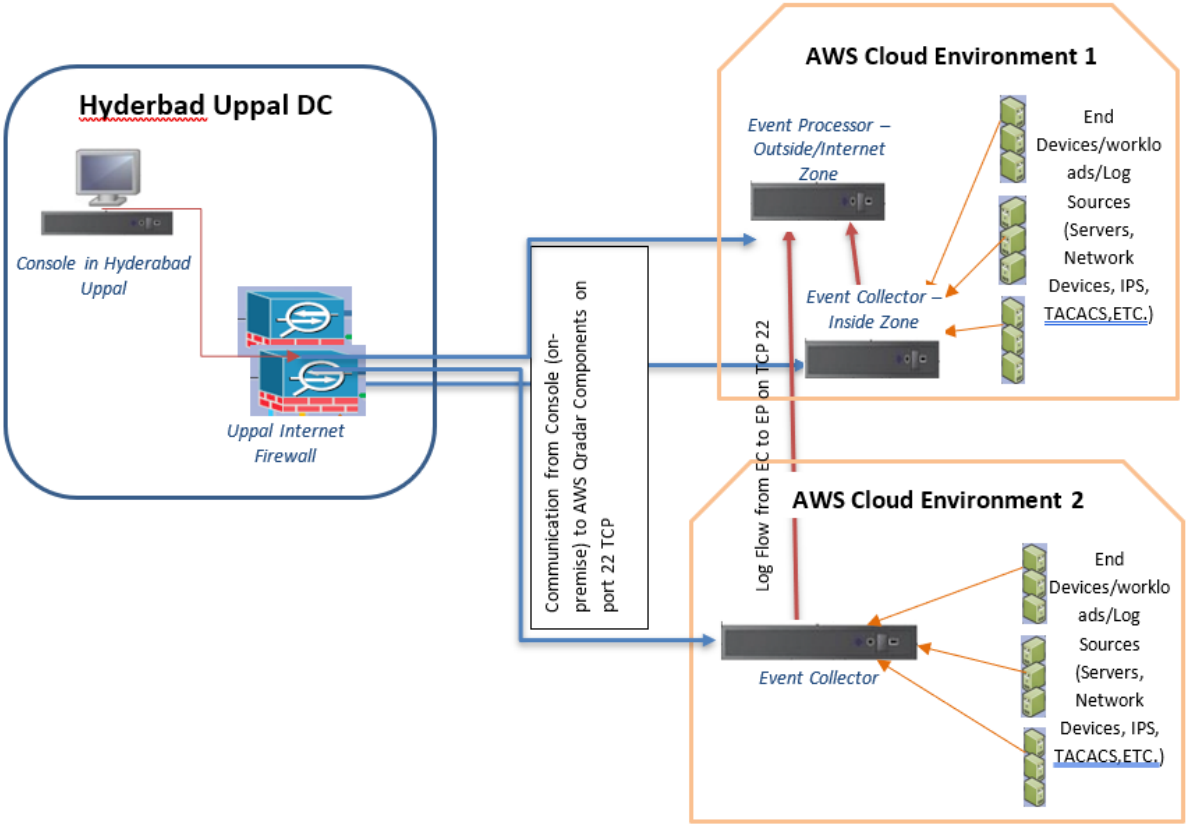


Fig - Logical connectivity for AWS environment

10. OPERATING PROCEDURE

10.1 DEVICES IN SCOPE FOR MONITORING

Any network, server, application, database or IT component which can be labelled with one or more of the categories below are covered in integration scope for monitoring.

- Is owned or managed by Genpact
- Has capability to log events
- Hosts critical applications or data
- Is in scope of audit (internal or external)
- Is either in production or is hosted in production environment
- Is hosted in critical zones such as public or DMZ, or
- Is required by process/business to be monitored for security alerts/incidents

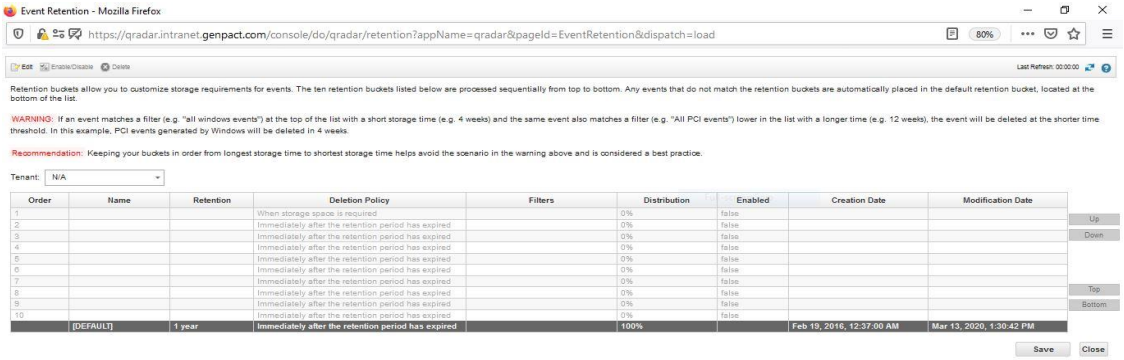
10.2 CATEGORY WISE LOGGING LEVEL BASELINES

Category	Logging Level
Firewalls	Upto Informational Level
Routers & Switches	Upto Informational Level
IDS and IPS	Alert and Audit Logs
Web Gateways	Web Traffic Logs
Anti-Virus Solutions	Application Functionality and Audit Logs
Servers (Windows OS)	Windows Advanced Logging
Servers (Linux OS)	Upto Informational Level
VPN Solutions	VPN Traffic Logs
Authentication Managers	Authentication and Audit Logs
Domain Controllers	Windows Advanced Logging
DHCP and DNS	Windows Advanced Logging
Virtualization Products	Authentication, System and Audit Logs
Wireless Access Managers	Authentication, System and Audit Logs
Exchange Servers	Windows Advanced Logging
Web Servers	Web Traffic Logs
Physical Access Systems	Access and Audit Logs
Patch Management and Software Distribution	Application Functionality Logs
Applications (SaaS and Hosted)	Application Functionality and Audit Logs
Vulnerability Management Solution	Vulnerability and Audit Logs
Other Monitoring Platforms	Alert and Audit Logs

10.3 EVENT RETENTION ON QRADAR SIEM

The default event retention policy configured on QRadar irrespective of location, device type or process is 12 months (1 year), which includes a minimum of 3 months of data in online + offline i.e. searchable mode and 9 months of data in offline only i.e. archived mode.

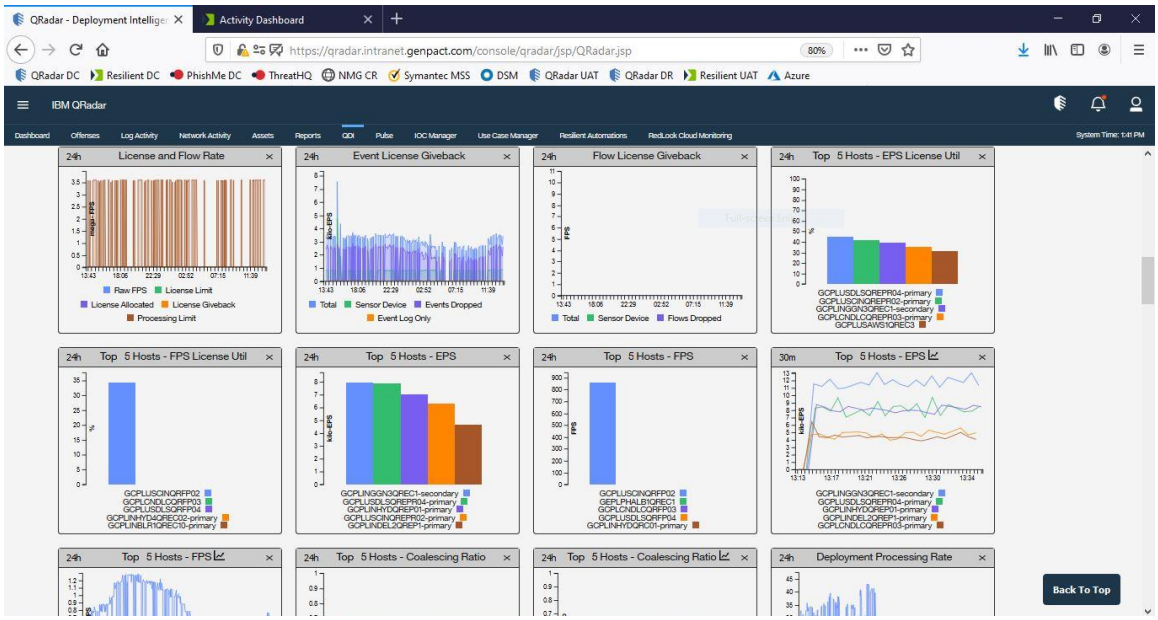
Qradar creates backup archive of online data on daily basis. The online data is present locally on the server. Archived data is stored either on local storage, offboard SAN/NAS storage devices or internal cloud storage resources such as S3.



Note: In case a different event retention policy is prescribed in the MSA agreement for a specific process, the arrangement would overrule the default policy. In such cases, refer the MSA agreement of the respective process for the agreed upon period of retention.

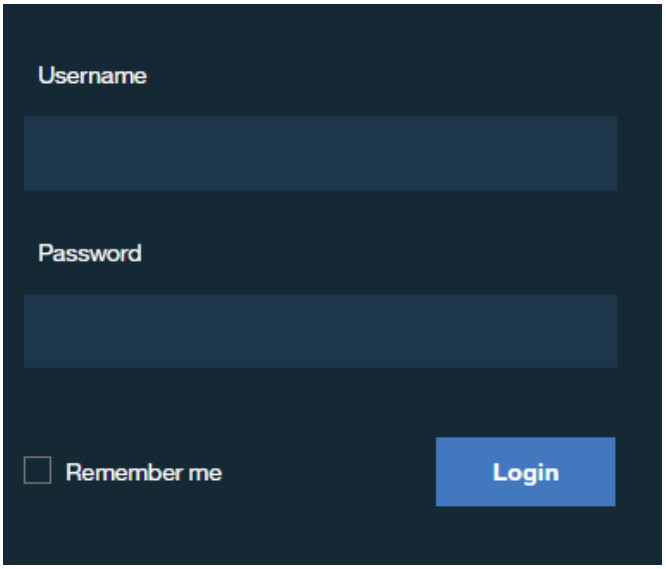
10.4 EPS CALCULATION AND MANAGEMENT

EPS is calculated through Qradar Deployment Intelligence. QDI consolidates historical data, on a per-host basis, of status, up-time, notifications, event and flow rates, system performance metrics, and other metrics specific to QRadar components.



10.5 CENTRALIZED QRADAR WEB CONSOLE

Evolution: Login to QRadar web console.

Steps	Work Instructions	Screen shots/Links
	• Go to URL =https://qradar.intranet.genpact.com/ • Login to console *Enter username:* *Enter password:*	

Following options are available in QRadar web Console.

- Dashboards
- Offenses
- Log Activity
- Network Activity
- Assets
- Reports
- Admin

10.5.1 QRadar Console

SIEM allows saving pointers to tabs with the specific settings you will frequently use. Users may consistently use the same queries or parameters when they use a particular tab.

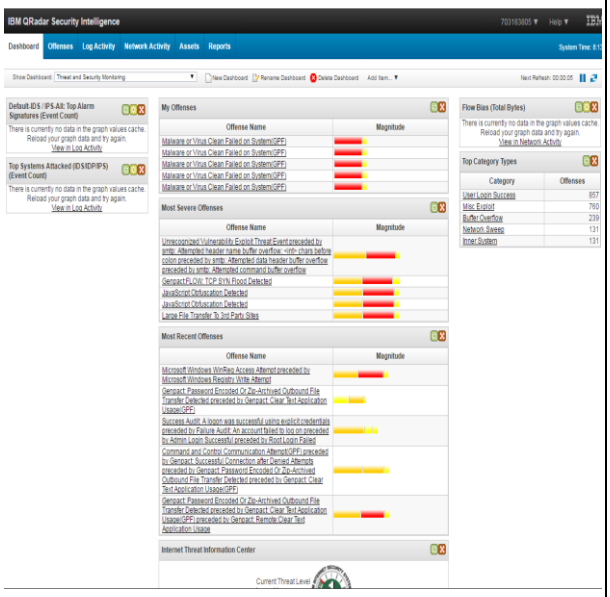
10.5.2 Log Activity

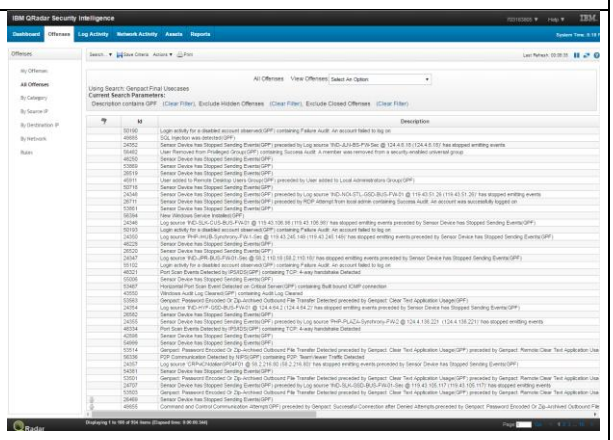
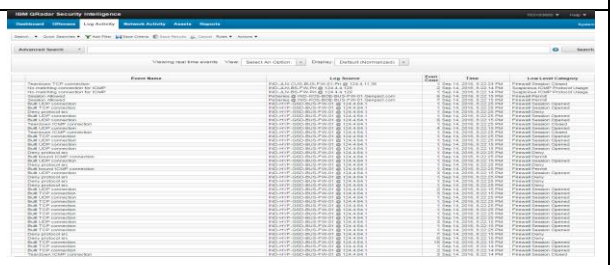
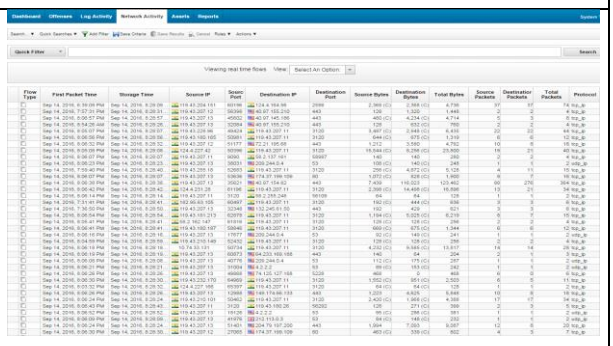
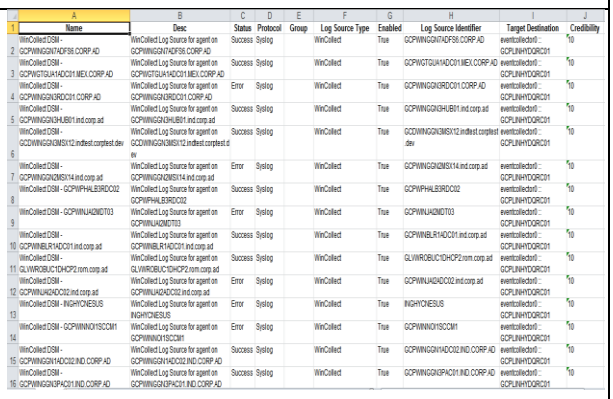
The Log Activity section of the QRadar provides access to several hundred “views” that have been organized into the below categories listed:

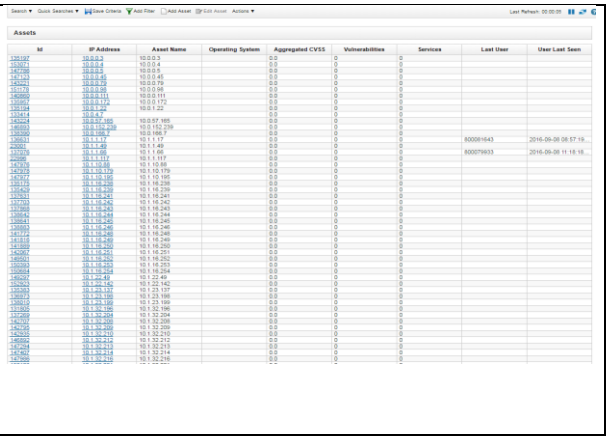
- Privileged Access Monitoring
- Malware
- Identify and Access Management

- Back Doors
- Third Party Monitoring
- Social (e.g. Phishing, Threat Intel.)
- Vulnerability Management
- Anomaly (Behaviour)
- Insider Threat
- DLP
- DDOS
- Configuration
- Key Control monitoring
- Secure workplace (Internal threats)
- Cloud
- Application
- Data Privacy
- Mobile
- Real Time Forensics
- Physical Security
- Business Policy
- Fraud
- AML

This tab will allow you to view security events/incidents that occur on network, which you can locate by using various navigation options or through detailed searches. From the investigation tab, you can investigate security events/incidents to determine the root cause of an issue.

Steps	Work Instructions	Screen shots/Links
a)	**Dashboard:** The dashboard tab provides a workspace environment that supports multiple dashboards on which you can display your views of network security (Top attack, top source, top destination etc.), activity. Each dashboard contains items that provide summary and detailed information about Offense that occur on network. You can also create a custom dashboard allow you to focus on your security or network operations responsibilities. **CDC Dashboards:** a) Real time log status. b) User login-log out activity. c) Component status	

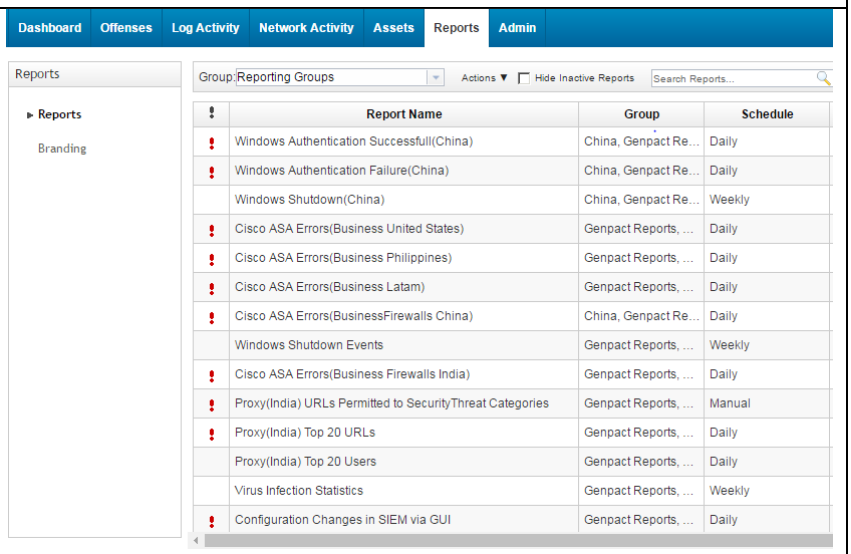
b)	**Offenses:** This is to identify the offense from each device and originating country and the associated event count per Intruder.	
c)	**Log Activity:** This show the entire live network traffic activity.	
d)	**Network Activity:** This view shows Network device traffic events for all the devices communicating with organization.	
e)	**Assets:** Devices which are integrated QRadar to generate an offense	

f)	**Use cases list:** CDC team analysed impact on organization and identified list of use case, which helps to mitigate the risk. **Sample use cases are listed in adjacent panel**	

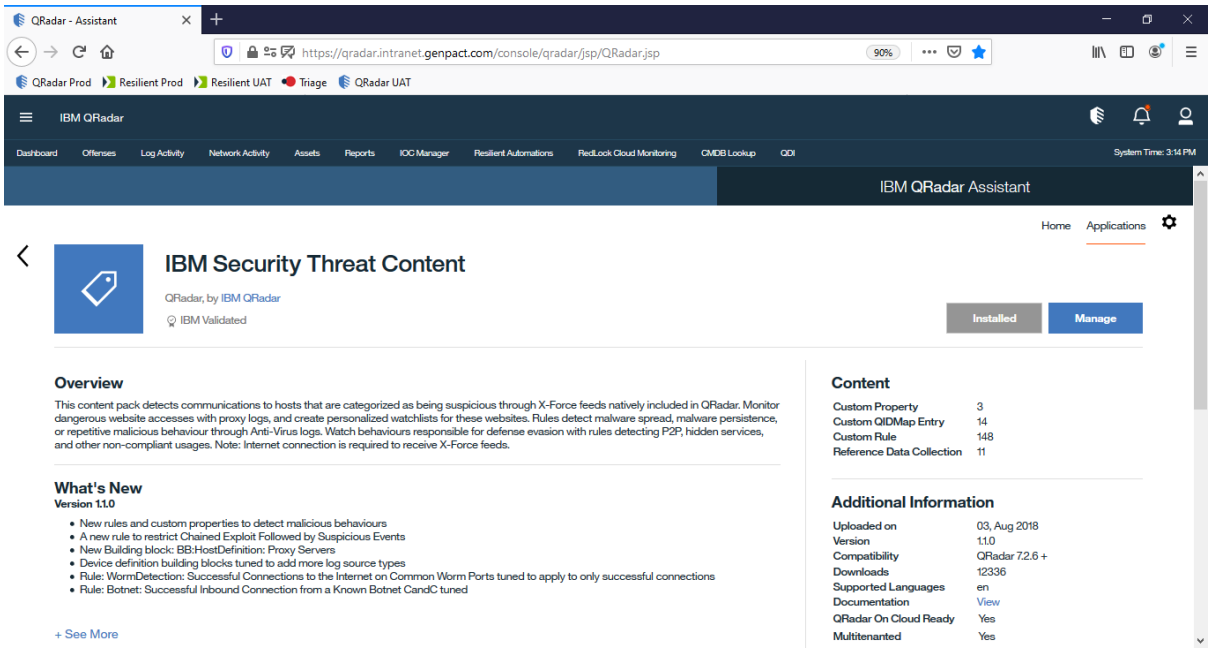
S No.	Rule Name
1	Genpact: Windows Audit Log Cleared
2	Genpact: Password Change on a Privileged Account
3	Genpact: Windows Device Stop Sending Events
4	Genpact: User removed from Privileged Group
5	Genpact: User Added to Privileged Group
6	Genpact: User Added to Domain Admin Group
7	Genpact: Unix based Sever Stop Sending Events
8	Genpact: Unauthorized Usage of Service Account
9	Genpact: Revocation of User Priviledge Detected
10	Genpact: System getting infected by same virus
11	Genpact: Monitor of use of disable username

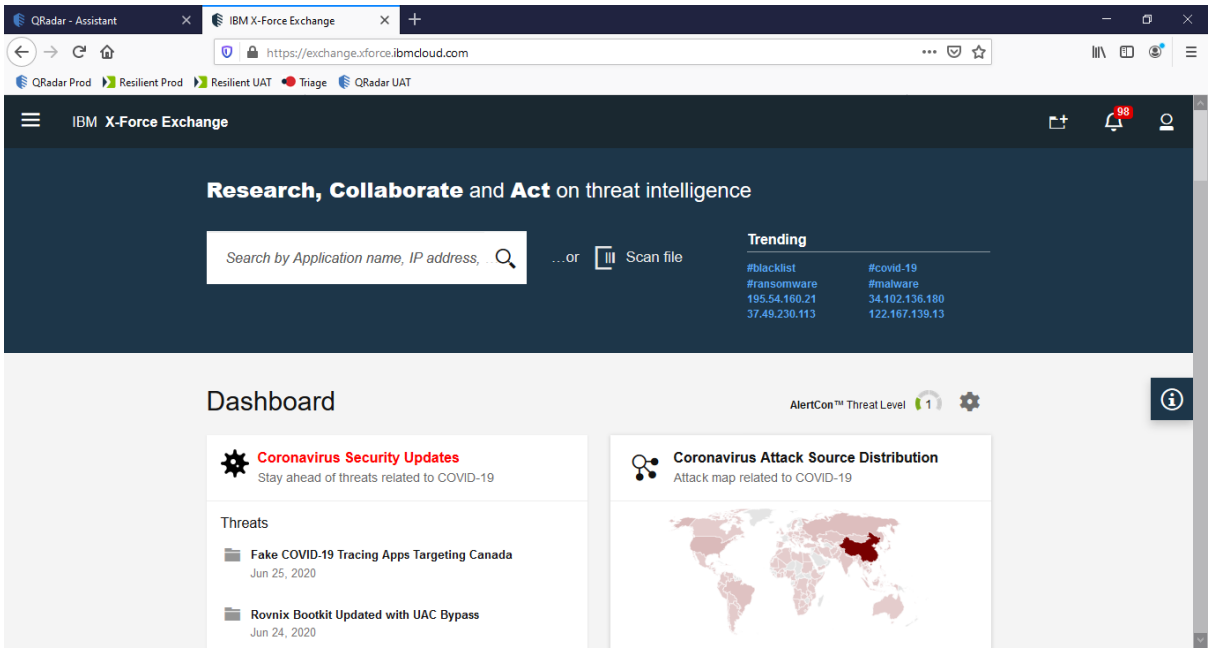
3.4.7	**Reports**: Reports will run on schedule basis. All reports are scheduled Hourly, Daily, Weekly.	



10.6 THREAT INTELLIGENCE

IBM Qradar leverages IBM X-Force Exchange for security threat feeds. X-Force is a cloud-based threat intelligence sharing platform enabling users to rapidly research the latest security threats, aggregate actionable intelligence and collaborate with peers. It is supported by human- and machine-generated intelligence leveraging the scale of IBM X-Force, enabling access and sharing of data about threats by exploiting IBM X-Force research. Integration with QRadar allows us to incorporate intelligence with security operations for near-real time threat alerting in our environment.





11. INCIDENT ANALYSIS & REMEDIATION/MITIGATION

11.1 LOG REVIEW PROCESS

CDC carries out log review in near real-time on 24x7 basis for all alerts through QRadar console.

Note: Every offense generated by a production rule on IBM Qradar is forwarded to IBM Resilient, denoted by string "GPF" in the offense nomenclature. CDC will analyze the offense in IBM Resilient, wherein the notes, base events, assignment details and resolution summary would be automatically synced with Qradar.

Notes	Username	Creation Date
Incident 24666 closed 2019-08-15T10:14:26+00:00 UTC by pradeep.thatiparthy@genpact.com with reason: Duplicate. The offenses generated from the phishme intel database could be closed as no suspicous traffic has been seen and are reverse traffic which are session denied. So closing this duplicate since analysis for all the IP's triggered on different offenses is being worked on master incident# 140904.	API_token: Resilient	Aug 15, 2019, 3:45 PM
pradeep.thatiparthy@genpact.com: Task Owner Changed:Task ID : 2510486 TaskName : Supporting Closure Evidence New Owner : pradeep.thatiparthy@genpact.com on Thu Aug 15 15:44:06 IST 2019	API_token: Resilient	Aug 15, 2019, 3:44 PM
pradeep.thatiparthy@genpact.com: Task Owner Changed:Task ID : 2510489 TaskName : Check if False Positive notification New Owne pradeep.thatiparthy@genpact.com on Wed Aug 14 14:54:23 IST 2019	API_token: Resilient	Aug 14, 2019, 2:54 PM
pradeep.thatiparthy@genpact.com: Task Owner Changed:Task ID : 2510487 TaskName : Check Legitimacy of Activity New Owner : pradeep.thatiparthy@genpact.com on Wed Aug 14 14:53:13 IST 2019	API_token: Resilient	Aug 14, 2019, 2:53 PM
jagadeesh.mudduluru@genpact.com: Task Owner Changed:Task ID : 2510488 TaskName : Review alert and validate information received New Owner : jagadeesh.mudduluru@genpact.com on Sun Aug 11 20:53:50 IST 2019	API_token: Resilient	Aug 11, 2019, 8:54 PM

Fig - Notes auto-synced from Resilient in QRadar

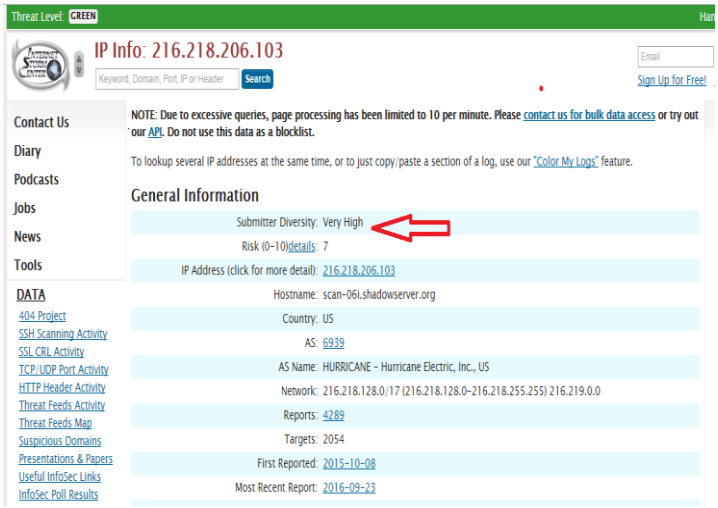
11.2 PROFOUND ANALYSIS

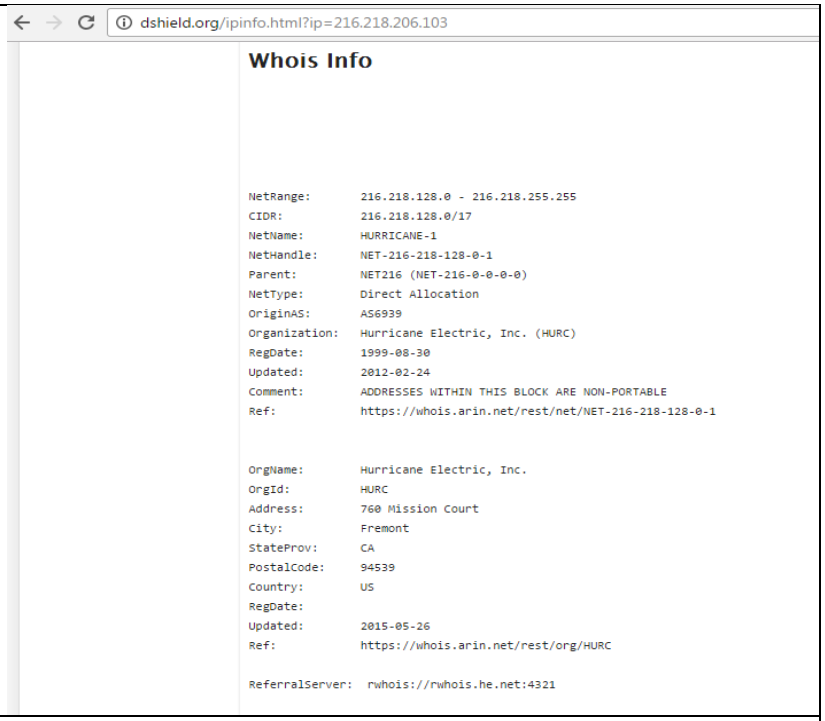
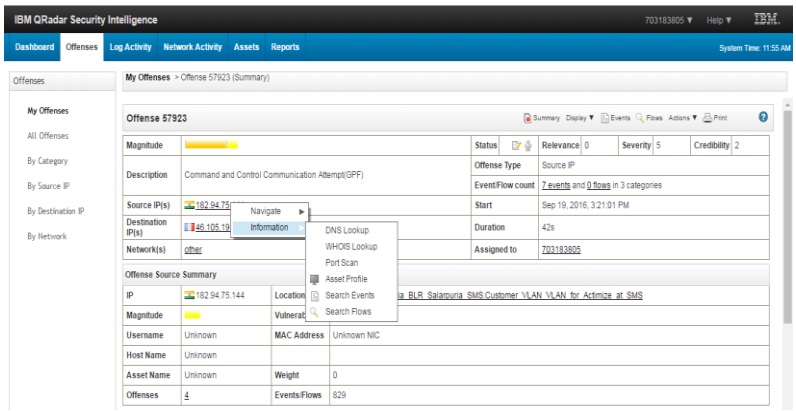
Note: For detailed incident response procedure, and guidelines adhered by CDC, refer Genpact Information Security Response Plan

CDC IR analyst should perform detail investigation on IBM QRadar SIEM and gather below information as per stage 2. If IM requires help from SI team, they must assist on the same.

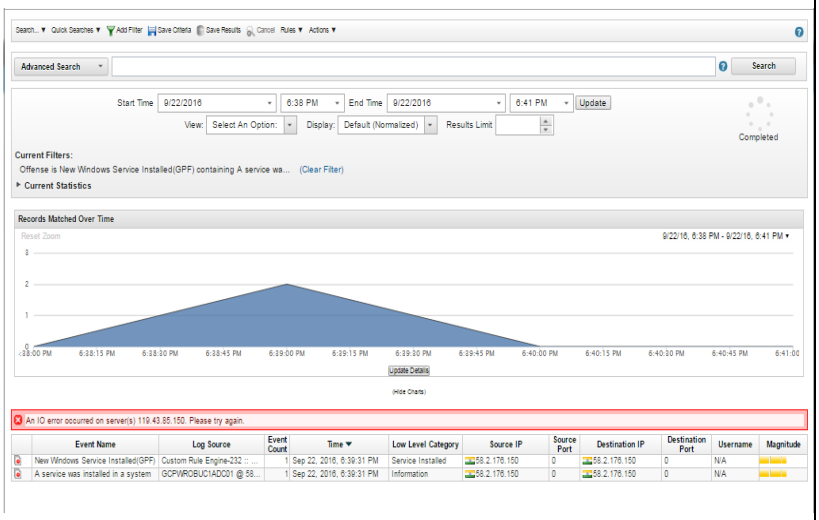
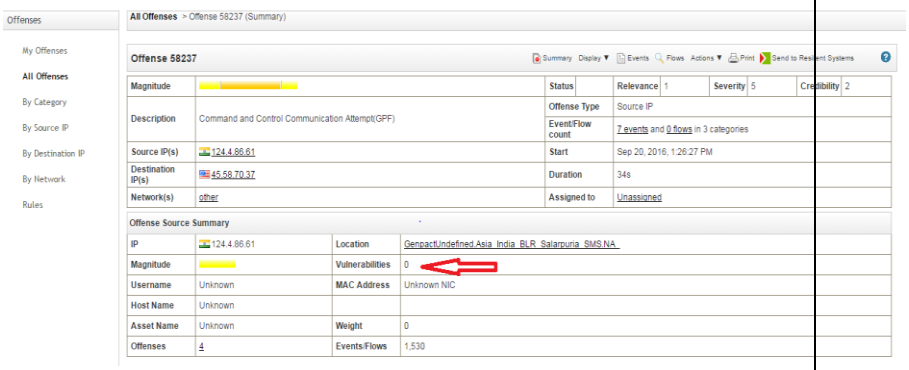
- Attacker Identification
- Target Identification
- Threat Identification

11.2.1 Attacker Identification

Steps	Work Instructions	Screen shots/Links
a)	Events/offence details from SIEM. **IP Reputation:** IP reputation can best be summed up as "past performance is an indicator of future results." **NOTE:** There are so many ways to identify the IP reputation of the IP's.	• IP address investigation. • Click on this link. Link will open the below window (Example).  • Enter the IP address which is highlighted in red. • Analyze output and identify the reputation of IP 

b)	**GetIpDetails/Whois:** Enter the IP as mentioned in point a) in dshield.org and scroll down to see whois info.	
c)	To know more information on source IP/destination IP navigate to QRadar as shown in the figure and right click on IP address it will navigate to information as shown in screenshot	

11.2.2 Target Identification

Steps	Work Instructions	Screen shots/Links
a)	Events details from SIEM • Navigate to offence events • Click on Events and idetify the IP/Host/user targetted	
b)	• **Asset Vulnerability Information** Vulnerability Assessment information will help us to identify this information • Running applications • Ports open • Patch status • Asset Owner – Point of Contact. **Pre-requisite:** • Import vulnerability feeds from customer. • Flow information.	

11.2.3 Threat Identification

Steps	Work Instructions	Screen shots/Links
a)	Refer attached file for selection of online tools/websites to identify the threats. Selection of Online Tools	• This is a selection of online tool that can be used during analysis of incidents and incident response. • Use these tools to know more on threats. For eg., • Identifying malware schemas etc. • Identifying Hashes for known-bad and known-good files • Identifying positive and negative reputation rates of IP address. • Identifying network information lookup tools and many more.

11.3 RISK AND SEVERITY LEVELS

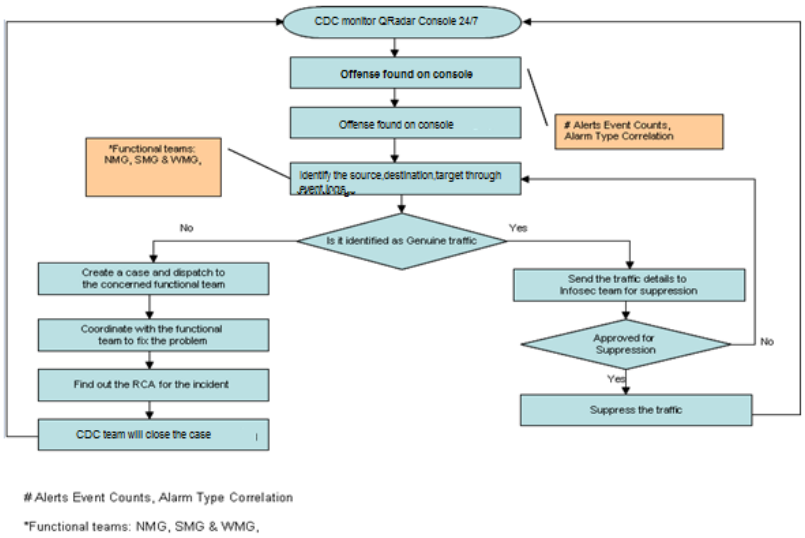
The severity of the incidents is based on the Genpact Incident Response Plan "Documentation of Incident Response Actions".

11.4 INCIDENT HANDLING

CDC analyst would refer to CDC documents on SharePoint while handling Security alert & their mitigation steps

https://genpactonline.sharepoint.com/sites/Cyber_Defense_Center/SitePages/Home.aspx

For every true positive offense identified on QRadar, CDC will open a Security Incident and process map is as follows:



11.5 SLA

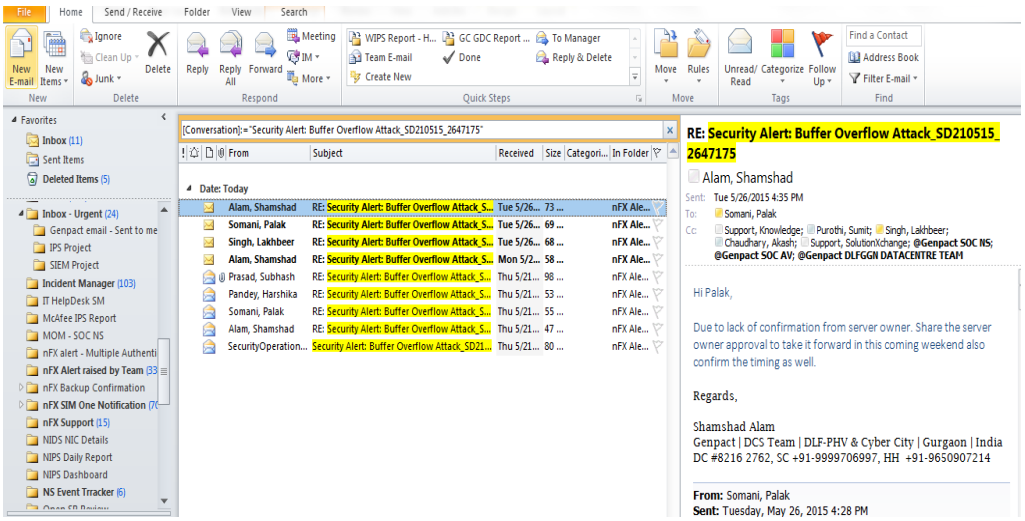
CDC Team is running their own incident management process while working on security incident/alerts with EUC/DCS/Wintel/MNS & Firewall team. Genpact Incident Response Plan "Communication Plan" determines the communication plan for incidents based on risk ratings.

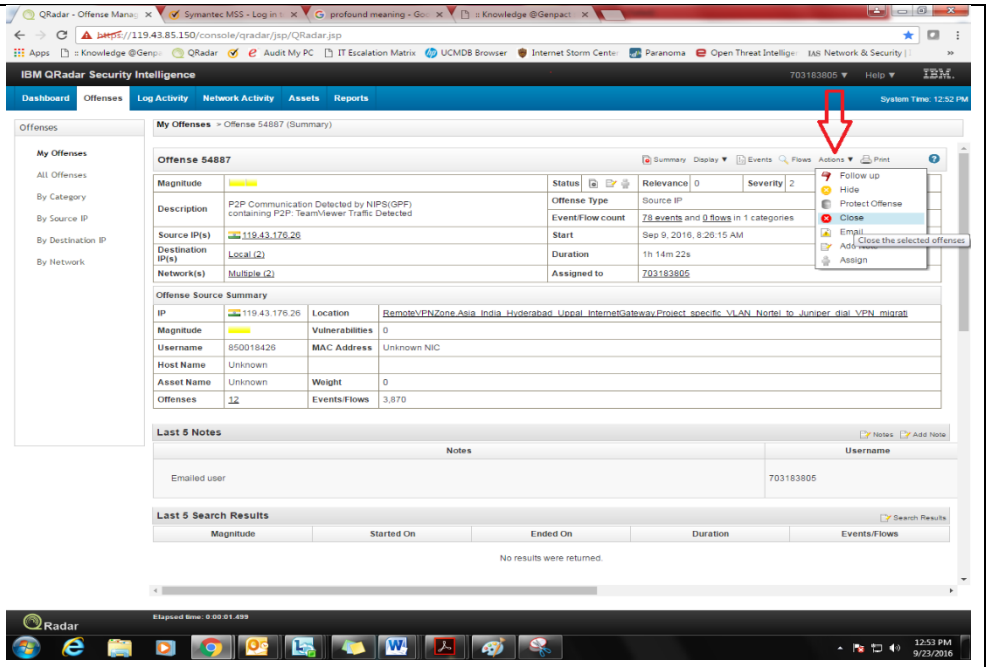
11.6 INCIDENT MITIGATION & CLOSURE

- CDC IR Analyst to analyse the response coming from respective team (EUC/Wintel/DCS/Firewall/Network/SOC AV) & provide their confirmation for closure of incident post confirmation from respective team.

- CDC IR Analyst to Make the final analysis and close the ticket or provide their confirmation to concerning team for closure who are working on security incident i.e. AV team performed VA scan & assign the ticket to EUC/DCS to fix the vulnerability. Once vulnerabilities are fixed, ticket can be closed.

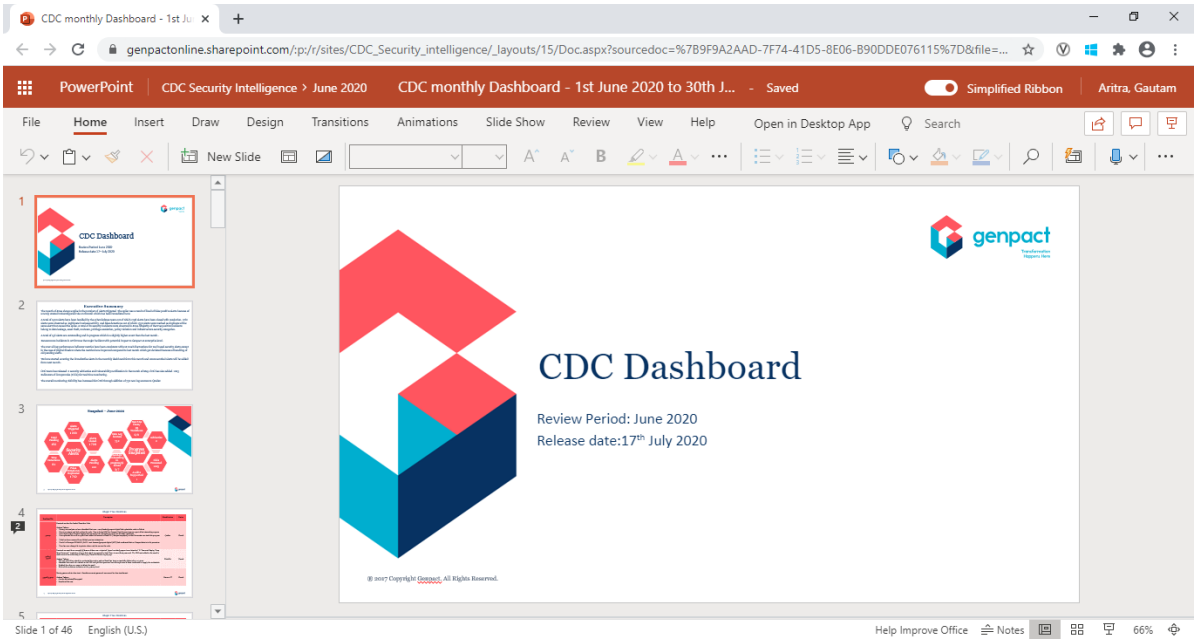
- CDC IR Analyst to update the closure remarks on the ticket and update the leanings from the incident.

Work Instructions	Screen shots/Links
CDC IR Analysts has to monitor CDC@genpact.com email inbox in a 24/7 basis. • Monitoring emails. • Follow up's. • Monitoring closure emails. • Learnings from incidents and any containment details from customers.	
Once team provides the feedback on initial and detailed analysis	• Verify resolver should be from resolver group. • Get a summary report/evidence of containment. • Analyze the system and user information is matching with initial communication

Incident closure in QRadar: Navigate to offence and click on action then close the offense as shown in screenshot	• 

11.7 INCIDENT REVIEW PROCESS

CDC publishes open security incident dashboards on periodic basis to Global Information Security Leader for review.



12. SIEM GOVERNANCE

12.1 RACI MATRIX

#	Activity	Particulars	Responsibility	Accountability	Contributor	Informed
1	Monitoring and Alerting	IBM QRadar console Monitoring	CDC Team	InfoSec	NA	Business/Device owner
2	Mitigation/Alert closure	Containment and Incident closure	CDC Team	Vertical head	CDC Team	InfoSec
3	False Positive analysis and suspension	Identifying false positive, change in rule for suspension	CDC Team	InfoSec	CDC Team	Business/Device owner
4	Root cause analysis	Identifying root cause of alert	CDC Team	Vertical head	CDC Team	CDC and InfoSec
5	Reporting	Reports Incident details/Dashboard	CDC Team	InfoSec	NA	InfoSec and Business

12.2 ROLES AND RESPONSIBILITIES

Incident Response Team	**Incident Analysts:** • First line incident handlers respond to alerts and offenses on Qradar • Responsible for 24*7 monitoring of SIEM solution for detection and managing incidents • Execute containment, eradication, and recovery steps • Perform malware and threat analytics wherever applicable
	Incident Response Leader: Coordinate response efforts and serve as the main point of contact for incidents
Security Intelligence Team	**Engineers:** Administrator role on platform, Responsible for Device Integration, Content Development, Automation & custom development and workflow management
	SME: Overall application SME and serve as main point of contact pertaining to application and managed components

12.3 EXCEPTION HANDLING

- CDC team monitors for only production (GPF) offenses found in the QRadar console while the rest of the alerts from the Console are an exception to this process.
- Alerts established as false positive with the help of functional teams are considered as exceptions.
- Monitoring is not performed when SIEM component is down
- Devices which are not integrated are out of monitoring scope
- Daily report is not published when the QRadar tool is under maintenance

12.4 ESCALATION MATRIX

- Escalation matrix is maintained at the SharePoint location: Cyber Defense Escalation Matrix

12.5 CHANGE MANAGEMENT

- Changes in SIEM and associated components that affect Qradar functionality are carried out in non-production hours in order to minimize hindrance in operations in case of service disruptions.
- All changes are deployed by authorized CDC Security Intelligence engineers only after necessary approvals from application owner and SME
- Operations and InfoSec stakeholders are notified in case of high-risk changes or changes that involve extended downtimes
- Planning, approval process and tracking of changes are made on IT change management tool in adherence to Infra Change Management Process

12.6 POTENTIAL RISK POINTS

- Any critical alert not attended on time can lead to serious security breach.
- Any missed alerts from the console may go undetected
- Lack of clarity of the guidelines used to determine the kind of alert will need a clarify request to be raised

13. ANNEXURE

- **Document Reference List**

Please refer the ISMS Master List of Documents.

- **Abbreviation and Definition**

Please refer this Link