Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

MANAGED SECURITY SERVICES

The purpose of the Managed Security Services is to protect a clients' data through a cohesive and highly responsive network security service, based on recognized security standards and industry best practices.

Managed Security Services consist in the management of the infrastructure through a base set of monitoring and operational service activities provided by onsite and remote technical resources, and delivering all relevant network security components. Capgemini also provides optional and specialized activities that are available for the client as an enhancement to the base set of service activities.

For the purposes and scope of this document and deliverable, Managed Security Services will encompass the following:

- Security Management
- Firewall Management
- VPN Management
- Remote Access Gateway Management
- Intrusion Prevention / Detection Management

Other infrastructure security services are described within our Services as well as the Security Service Line section of Capgemini Outsourcing portfolio. Particularly, in the "Operational Security" section of the Security catalogue. The Service Components that Capgemini provide as part of these Operational Security Services are as follow:

- Firewalls and Access Controls
- Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS)
- Content and URL Filtering (includes Anti-Spam Filtering)
- Malware Management
- Secure Configurations
- Media Handling, Classification & Disposal

All these Services are part of a complete and coherent set of Security Services that are provided as standalone offerings, or embedded within our global Outsourcing Services.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

As shown in the diagram below, Capgemini does cover the entire scope of Security Services, from Consulting & Governance to Operational Security Services and Desktop Security features, see *figure 1 Security Domains.* This is supported and delivered by the Capgemini Service Lines across all functional areas and in an integrated manner.

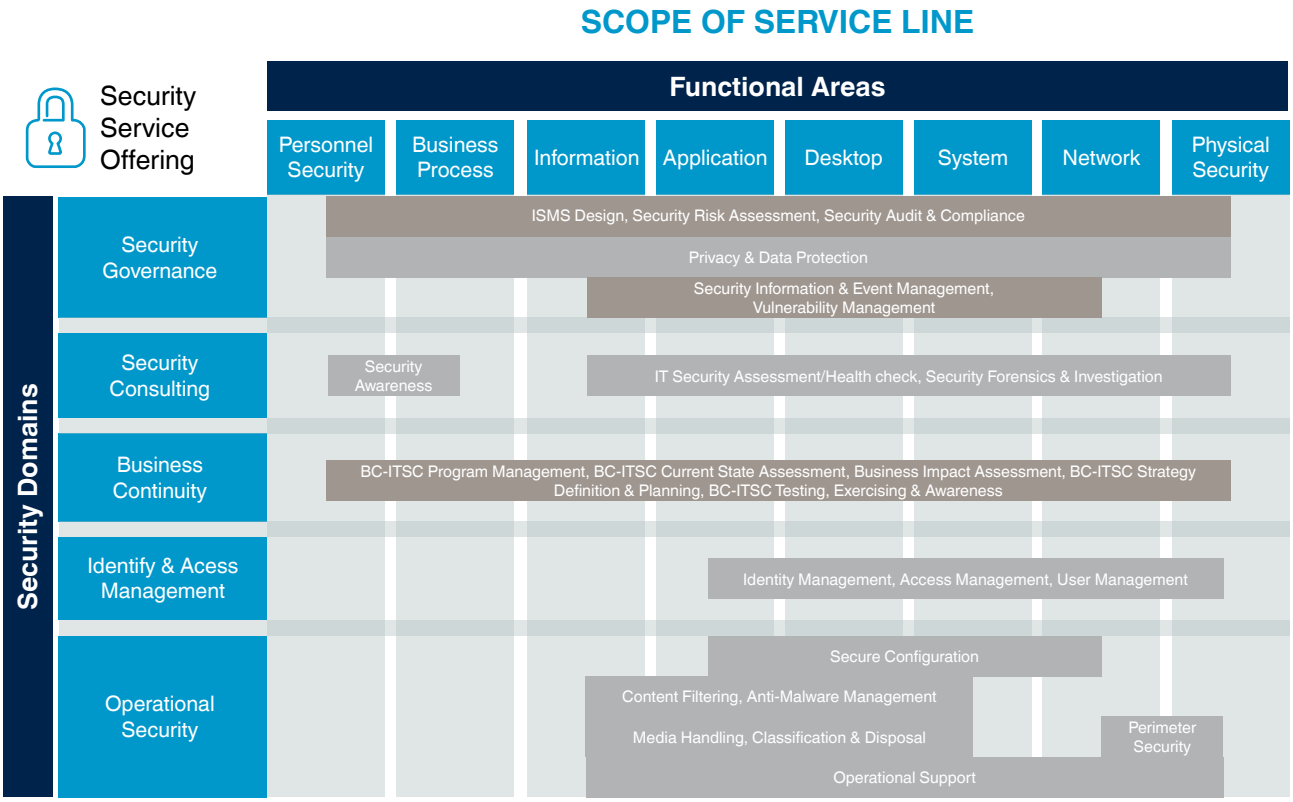


Fig. 1 - Security Domains in Capgemini

SCOPE

Managed Security Services include all people, processes and activities, tools and equipment resources necessary to manage all network security components under prevailing or appropriate governance.

Capgemini deliver Managed Security Services on both:

- Client infrastructures
- Capgemini infrastructure providing shared or client dedicated systems
- Infrastructures that are used for interconnection between Capgemini and its clients (e.g. used to deliver BPO services, DMZ to provide remote Infrastructure Outsourcing services but to name a few.)

Capgemini delivers 24x7 Operations with Offshore as well as on/near-shore (our RighShore methodology) capabilities and local partnerships for maintenance. As described in detail in the following sections, our services encompass Monitoring and Fault Management, major security incident & crisis management, problem/incident resolution and change implementation, consulting services, 3rd parties management and on site support to name a few.

Capgemini supports all key technologies and market available infrastructures for each Network Security Service.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

Capgemini Network Infrastructure Services addresses the data, network security, voice and unified communication requirements of its client's IT infrastructure, delivered and reported in an environmentally consciou manner.

VOICE SERVICES

- Telephony Management
- Contact Center Services (Hosted & Managed)
- Unified Communications Management
- Conferencing Management
- Mobile Phones & Mobility Management
- Voice Consulting Services

DATA NETWORK SERVICES

- Managed Router Service
- Managed LAN Service
- Internet Access Management
- Applications Networking Management
- Domain Name System Management
- Data Network Consulting Services

MANAGED FIREWALL SERVICE

- Firewall Management (fig. 2)
- VPN Management (fig. 3)
- Remote Access Gateway Management (fig. 4)

Other Security Services are available via our security services.

Fig. 2 - Managed Security Services
Fig. 3 - VPN Services
Fig. 4 - Remote Access Gateway Management

Fig. 2 For Firewall Management Services, the type of services embedded in the Capgemini service component are:

- Security Application on Server platform
- Appliance (physical or virtual)
- Application Security
- Cloud Security Services
- Optional Intrusion Detection or Prevention Services
- Optional High-available resources

Fig. 3 For VPN Management, the type of services embedded in the Capgemini service component are:

- Router
- Appliance (physical or virtual)
- Security and access control
- Client Software (VPN software)

Fig. 4 For Remote Access Gateway Management, the type of services embedded in the Capgemini service component are

- Remote Access Gateway Server & Application
- Appliance (physical or virtual)
- Application RAS

For each of the above, Capgemini deliver a number of value-added services such as:

- Implementation of security standards (systems hardening and similar), Application controls to name a few
- Security events reporting; auditing & analysis
- SSL VPN Application & Appliance management; IPSEC VPN Client administration
- Network Infrastructure Security Services compliance with regulatory requirements as imposed by international or national authorities or standards (such as FDA, PCI, NERC, ISO27001 and similar)

Managed Security Services provides:

- Security Management
- VPN Management
- Remote Access Gateway Management

Managed Security Services are part of a larger suite of Security services that various Capgemini Outsourcing Service Lines deliver.

Capgemini Security Services address the confidentiality, integrity and availability requirements of the client's business operations and IT infrastructure. This is achieved through a flexible combination of management, operational and technical controls, leveraging people, process and technology depending on the client's risk appetite

SECURITY GOVERNANCE

- Privacy & Data Protection
- Security Information and Event Monitoring
- Vulnerability Management

IDENTITY MANAGEMENT

- Identity Management
- Access Management
- User Administration

OPERATIONAL SECURITY

- Firewall Security Management
- Intrusion Detection/Prevention Systems
- Content Filtering
- Anti-Malware Management
- Secure Configurations
- Media Handling, Classification & Disposal

SECURITY CONSULTING

- ISMS Design
- Security Risk Assessment
- PCI Compliance
- Security Audit & Compliance
- IT Security Assessment/Health check
- Security Awareness
- Security Forensics & Investigation

BUSINESS CONTINUITY & IT SERVICE CONTINUITY

- BC-ITSC Program Management
- BC-ITSC Current State Assessment
- BC-ITSC Business Impact Assessment• Security Audit & Compliance
- BC-ITSC Strategy Definition and Planning
- BC-ITSC Testing, Exercising and Awareness

Fig. 5 - Operational Security Services

CAPGEMINI CAPABILITIES

The Capgemini Global Network Operations Centre (GNOC) is our central reporting and coordination point for all network incidents, problem and change requests. It provides all Level 1 and 2 support of the data network infrastructure. The Capgemini GNOC is staffed with a full time network operations team with comprehensive network skills to conduct 24x 7 incident problem and change management of the network. Incident managers own all incidents through to service restoration and resolution. Working with the operations team are Level 2 network analysts who provide escalation support for Incident and change management where required. They also provide the network documentation and performance and capacity reporting for the network. Skill levels for our Level 2 support team are typically CCNA, CCNP, MCP, MCSE, certified or equivalent technical certification for technologies that exist within the network.

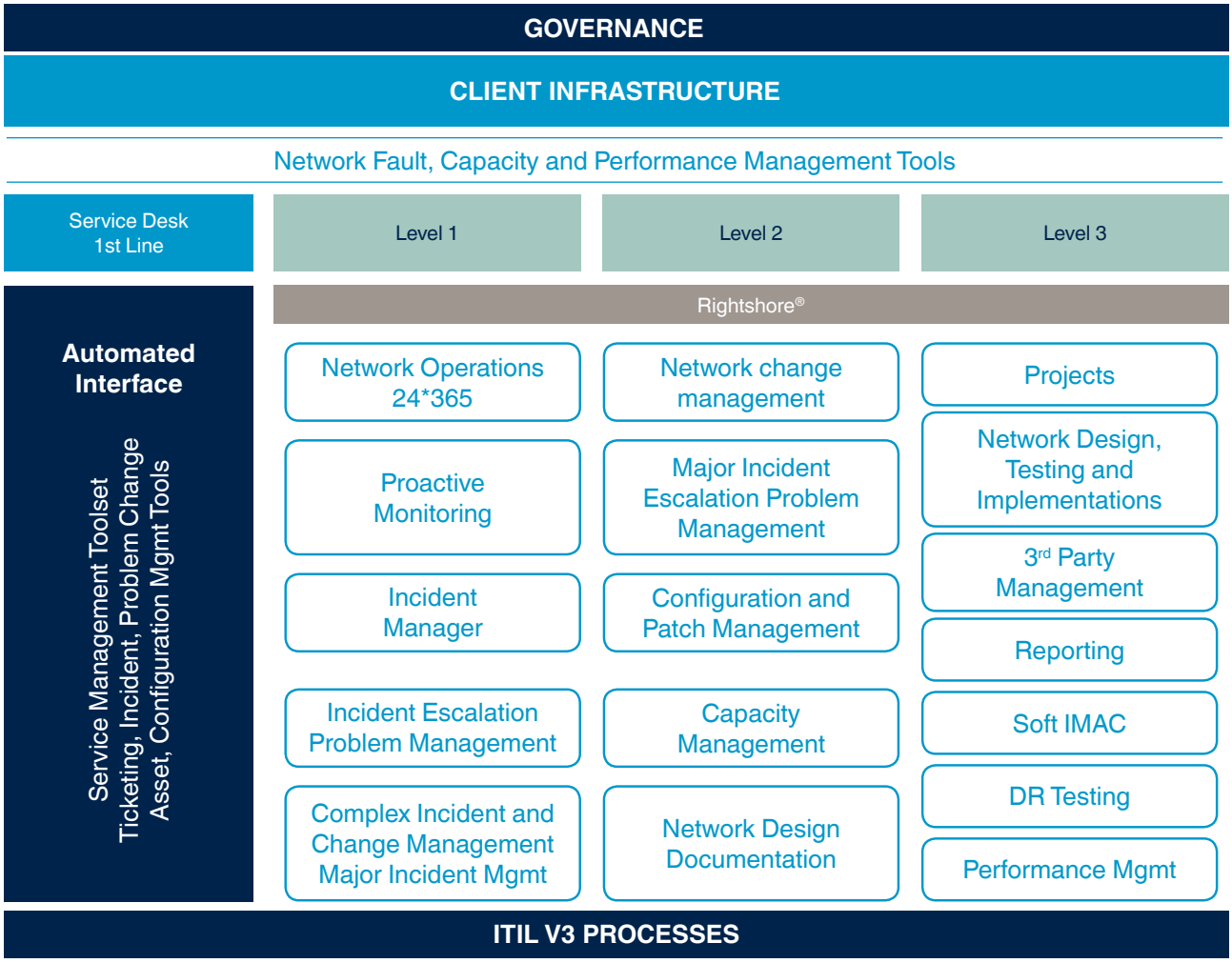


Fig. 6 - Capgemini GNOC services

A network engineering team will provide incident escalation for complex network issues and 3rd Level support functions. This team will also review and provide recommendations regarding the network state for capacity and performance requirements. They provide network design, implementations, asset refresh and project support for new initiatives as well as DR / failover testing. Skill levels for our network engineers vary from CCIE, CCDP, CCNP, CCNA certified or equivalent..

All moves, additions and changes including asset refresh will be coordinated by the Capgemini GNOC working with the offshore engineering teams managing configuration changes and documentation updates. The Capgemini GNOC, Level 2 Analysts and Network Engineering teams support the network through remote management. Network Services moves and changes that require onsite activities will be provided by our partner onsite teams through dispatch tickets or called out to our hardware maintenance providers. Again the Capgemini GNOC has central control and oversight for these teams through to completion and ticket closure.

The Capgemini GNOC works closely with the Capgemini IMOC™ (Infrastructure Management Operations Centre) to ensure incidents are identified, categorised and assigned to the appropriate resolving team. Common standards, processes and toolsets ensure a swift and consistent approach to incident resolution.

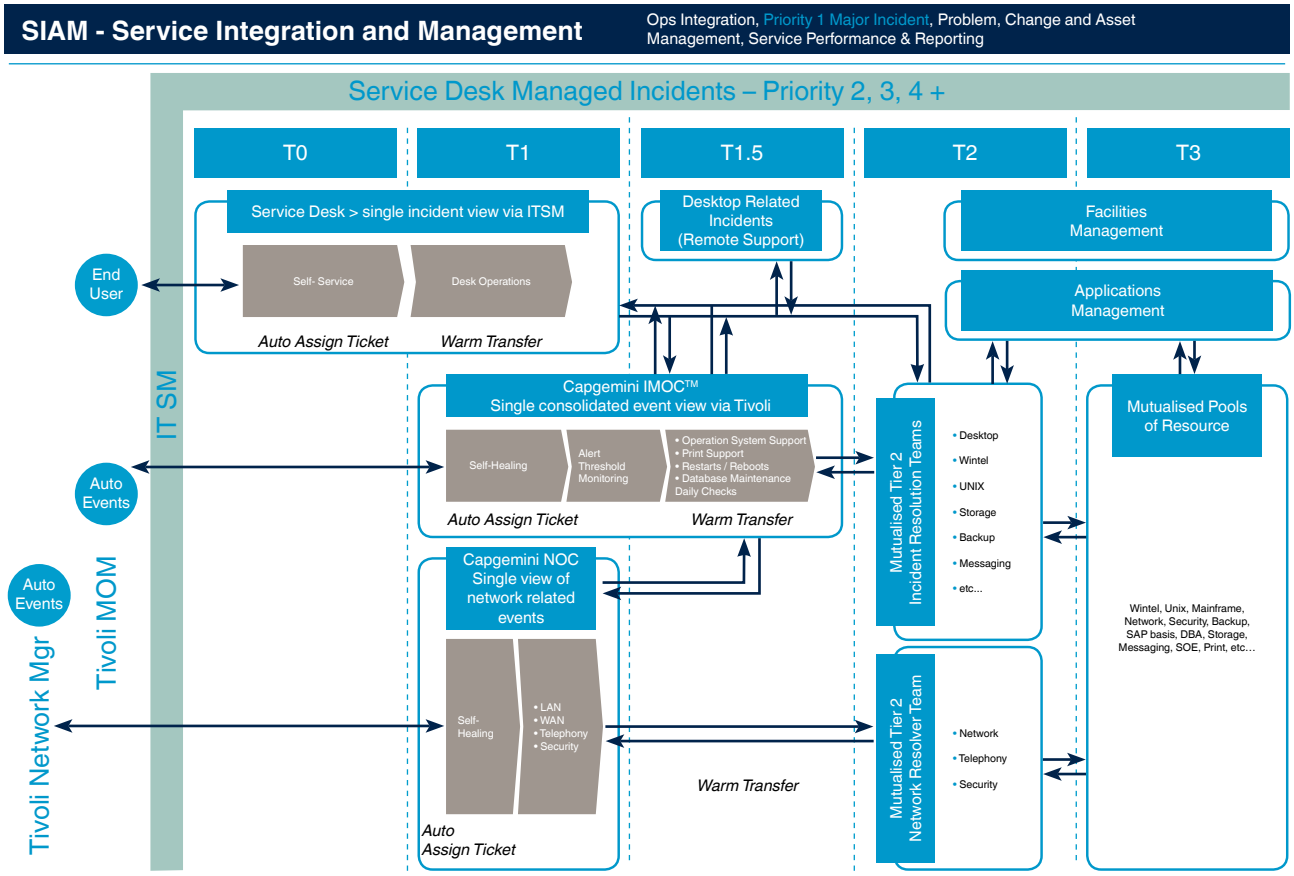


Fig. 7 - Capgemini IMOC™ and GNOC integration

Current Security Services delivered by Capgemini Outsourcing are as follow:

- 1,000,000+ Identities Managed
- Over 1.1 Million Malware Protection Agents Deployed and Managed
- In excess of 1000 Fault-tolerant Security pairs Managed

KEY ACTIVITIES & PROCESSES

Managed Security Services includes:

- Monitoring
- Incident & Problem Management
- Change Management
- Configuration Management
- Capacity & Performance Management
- Service Reporting

- Software Management & Upgrades
- Standard Security implementation, including Vulnerability alerts and fix/patch application
- Network Security Architecture & Expertise
- Application Control
- Management of relevant third parties
  - Telco & 3rd Party operational management:
  - Escalation, Fault & Problem Management
  - SLA Reporting
- Asset Management

This may vary for client dedicated network security infrastructure. An analysis and design are performed as early as possible, with information from RFP or during the due diligence phase. Options or customized service might have to be implemented to fit with the client's specific environment (hardware & software, tools used, features required, etc.) and constraints.

We describe in the section below some of the key activities that are specific and representative of Managed Security Services as delivered by Capgemini Outsourcing Services. This section does not outline all the activities undertaken but highlights important ones:

MONITORING

Capgemini employs a set of people, tools and processes to deliver a comprehensive 24x365 proactive monitoring capability for our Managed Security Services. This is most important to providing the highest service levels required by our clients. Our technical staff are knowledgeable and current in network technologies implemented in our datacenters and we maintain a number of network certifications (Capgemini IMOC™ staff are ITIL v3 certified and are Cisco trained and certified – associate, specialist, professional, expert - depending on their functions (level 1, 2 or 3)). Capgemini IMOC™ technicians are continually monitoring the tools and events on client networks. When a fault is detected by our IMOC and it is determined that it is a service affecting incident, our escalation process is triggered and the incident is managed end to end till resolution by our Incident Management team, in full coordination with the Capgemini IMOC™ (and at level 3 if/as necessary). Our Incident Management flow goes in a seamless process from first level of resources and if the incident cannot be handled by our first level technical staff within a pre-defined time, the second level engineers are engaged to review and determine the root cause, etc up to 3rd level support (or vendor) and if necessary, engagement of our partners & suppliers centres of expertise.

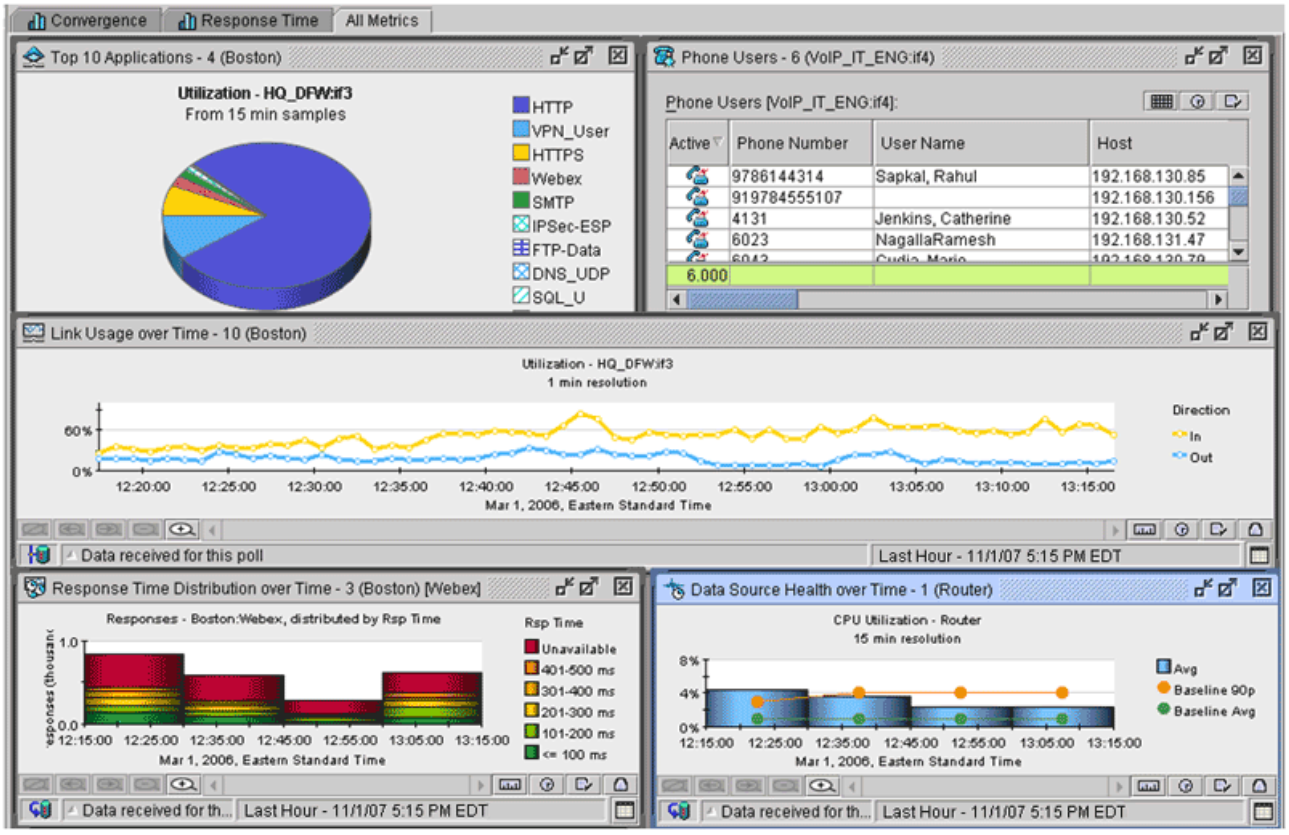
Proactive management of the infrastructure enables the remote identification and correction of incidents and is underpinned by the use of advanced management tools. Network Security devices are proactively monitored by using polling cycle to each managed device to detect the status of that device. These tools are an important part of our monitoring services. Capgemini uses a standard set of tools to provide monitoring and management.

Where we are managing a client owned security infrastructure, Capgemini has can leverage tools implemented by our customers which are separate but compatible with our standard set of tools. We do this when our client has implemented a capable set of tools that provide the same capability and function that our tool set employs and where using these tools provides a better value to our client. However, whether using Capgemini or client specific tools, we continue to provide and roll up all network events and corresponding information to our higher level management tool to provide comprehensive event correlation and perform automated ticket assignment and escalation to the right resources to restore service quickly.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

PERFORMANCE AND CAPACITY MANAGEMENT



Capgemini will provide a capacity planning and performance management service which verifies that the IT infrastructure is capable of delivering the right level of security, performance and capacity for your business. This caters to multiple platforms, locations and environments and is built on industry leading processes and integrated tools.

Performance and utilization data are collected via monitoring agents on each critical system. The proposed solution would keep performance and capacity data in the performance tool repository. The Capgemini GNO (and/or regional Cap network security teams depending on the exact Delivery organization) carries out proactive network analysis to find any potential performance issues and reports to engineering for proposed action. When necessary, capacity recommendations will be reported to you to avoid future issues in network security. The Capgemini GNOC (and/or regional network security teams depending on the exact Delivery organization) also provides a monthly analysis summary, detailing trends, potential problems and capacity planning recommendations.

Capacity Analysis is provided from standard reports built on reporting tools such as Computer Associates, Cisco Prime Management, NetHealth and accessible for you through the our portal or email delivered reports.. In regards to capacity management Capgemini will:

- Provide capacity analysis reports and analysis of network security capacity
- Identify issues in accordance with your network security performance
- Advise on appropriate monitoring regimes and taking timely and effective action to ensure

- That monitoring regimes remain fit for purpose
- Ensure appropriate improvement actions are identified and added to the service strategy recommendations.
- Producing and maintaining appropriate Operational documentation (e.g. “Quarterly Security Traffic Report”)
- Ensuring timely delivery of reports, including contributions to Service Performance Reports
- Incidents reports and Benchmarking reports

As part of the capacity management service, we will include an agenda item at the periodic service review meetings dedicated to capacity issues. During these meetings we will raise any issues identified under the performance and capacity service, along with recommendations for adding extra capacity to mitigate such items. This service can only be a success if it is fully collaborative between the client and Capgemini. We would expect the client to play an active role in forecasting capacity requirements by providing business knowledge and forecasts at these service review meetings.

By analysing this forecast data, Capgemini can make recommendations about future changes to the network security infrastructure to ensure that it runs at maximum efficiency.

CHANGE MANAGEMENT

The support teams will implement changes that are in the scope of service in accordance with the agreed change records. Change details will be recorded in the change management system.

REPORTING

Capgemini will utilize our standard tool for service reporting to our client. Our monitoring and management tools feed network management and service level information for monthly network reporting requirements. These reports can be viewed on line by our client’s designated Network Security points of contacts. In addition, we can update your web available portal that can be used today for real time management review. This real time network performance dashboard will provide you with specific data monitoring activity regarding the client’s Network Security. Specific reporting such as vulnerability assessments and security compliance are provided as per service scope defined with the client.

Several management, security and reporting tools can be used to deliver required reports.
Capgemini counts on a broad partnership ecosystem to deliver this item.

For each of these services, Capgemini has defined the detailed scope of standard activities it usually provides, the various type of technologies or services it can apply to, the assumptions it typically takes etc.

Activities are of three types as described below:

BASE ACTIVITIES

GENERAL ADMINISTRATION

- Management of client communication via the service manager
- Maintenance and update of technical documents used to deliver the services
- Quarterly review of client business objectives and infrastructure
- Bi-annual review of client hardware and software standards

MONITORING

- Proactive monitoring security devices for health and availability using the automated toolset
- Monitoring of industry standard thresholds for devices
- Automated trouble ticket generation for incidents

INCIDENT RESOLUTION

- Investigation be resolving team, diagnoses and restoration of affected services as notified by the ticket raised through the incident handling process, aligned to agreed service levels
- Details of incident and resolution will be recorded within the problem management system.

PROBLEM RESOLUTION

- According to the problem management process, the resolving teams will prevent a recurrence of incidents by identifying and eliminating the root cause
- Details of the problem management activities will be recorded within the problem management system

CHANGE IMPLEMENTATION

- The resolving team will implement changes to configuration items in accordance with the agreed change record
- Details of the change will be recorded in the change management system

CONFIGURATION MANAGEMENT

- Maintenance of up-to-date configuration information on in-scope Security devices for use in resolving incidents
- Moves, adds and changes of configuration incidences are registered
- Automatic backup of asset configurations to a central configuration management tool

PERFORMANCE MANAGEMENT

- Establish and maintaining a common set of performance metrics and then measuring and checking the level of performance in terms of latency, response time and availability
- Reporting on such measures against agreed Service Levels
- Monthly review and reporting based on pre-defined reporting templates, including measures to agreed performance matrices on in scope services

CAPACITY MANAGEMENT

- The analysis of data provided my monitoring, undertaking trend analysis and making sizing recommendations to the client regarding the necessary resource levels to provide the most efficient use of resources or to avoid service impact in the future
- Resource measures include utilisation (memory, processor and concurrent sessions) are monitored and analysed against pre-defined thresholds agreed with the client based on good industry practice
- The service is provided continually and reported to the client on a monthly basis using the standard report templates

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

STANDARD SECURITY IMPLEMENTATION (APPLICATION)

• Implementation of rules, policies, zones, VLAN's, VRFs, according to clients Security Officer requirements

REPORTING

• Reporting on availability, sessions, denies, provided on a monthly basis
• Reporting on common targets and recurrent attacks
• Reports provided by working day "X" (the value of "X" to be determine by mutual consent)
• Standard reporting suite automatically produced by the Service Management process
• Bespoke reporting available as a separate charged item

USER ADMINISTRATION

• User administration is restricted to OS administration accounts set up on in scope assets
• A rights and delegation model is in place which ensures that administration rights are used in the correct way
• Administration rights are restricted to Capgemini staff supporting the service components
• Administration rights are reviewed and updates as necessary in line with human resource changes
• Passwords are updated and distributed every 120 days

ASSET MANAGEMENT

• Maintenance and management of all assets in a global database

SECURITY ADMINISTRATION (HARDWARE)

• Hardware configuration (system configuration, network configuration, root logging and security)
• Distributed account management is restricted to Security systems administrative accounts
• A rights and delegation model is in place which ensures that administration rights are used on the correct way
• Provision of compliance information

SECURITY ADMINISTRATION (APPLICATION)

• Configuration for Security application
  - Rule base
  - Network configuration
  - Routing, Network Address Translation
  - IP addressing
  - DMZ plan
• Distributed account management is restricted to Security administration accounts
• A rights and delegation model is in place which ensures that administration rights and privileges are used in the correct way
• Provision of compliance information

ARCHITECTURE

• Maintenance of architecture blueprints
• Respond to queries related to changes and other service management activities
• For further technical solutions and project work a separate set of network Assessment, Design and Optimisation services are available enabling Capgemini to deliver the entire life cycle management

ASSET REFRESH

• Life cycle management
• Replacement through change control process of existing in-scope assets at end of useful life or support by manufacture
• For base service asset life is typically five years

APPLICATIONS CONTROL

• Implementation and management of applications control for systems or users traffic
• These provide granular policy based controls of Web-based applications such as:
  - IM
  - Multiplayer games
  - Unauthorised HTTP-tunnelling
  - Wikis
  - P2P
  - Public voice over IP (VoIP)
  - Blogs
  - Data sharing portals
  - Gateway level (TCP/IP) malicious code
  - Remote PC access
  - Web conferencing
  - Chat
  - SQL
  - Injection
  - Cookie poisoning
  - Parameter tampering
  - Directory traversal
  - Streaming media

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

OPTIONAL ACTIVITIES

OS MAINTENANCE AND SUPPORT – MAJOR RELEASES

- Included updates in OS for major releases – new or improved feature sets
- Project based implementation covering evaluation, testing and updating the OS through the change management process
- Major releases are first evaluated by Capgemini to determine if the release is required or necessary to implement
- Major releases as determined by manufacture rating

DYNAMIC ROUTING PROTOCOL MANAGEMENT

- Management of the dynamic routing protocol (BGP, OSPF, EIGRP) within the Security routing layer and for in scope service components

HIGH AVAILABILITY MANAGEMENT

- Management of the routing protocols between active and standby security elements within a service location
- Management of other high availability mechanisms required for proper operation of security environment
- Provided according to hours of support and other pre-agreed options of service.
- Provision of third party management if relevant and required

HIGH AVAILABILITY MANAGEMENT

- Management of the routing protocols between active and standby security elements within a service location
- Management of other high availability mechanisms required for proper operation of security environment
- Provided according to hours of support and other pre-agreed options of service.
- Provision of third party management if relevant and required

SPECIALIST ACTIVITIES

CONTRACT MANAGEMENT

- Management of third party contract on behalf of the client
- Tracking SLA
- Reporting
- Escalation management

PERFORMANCE TUNING

- Performance tuning focuses on optimising performance and consists of setting and configuring the operating system parameters to achieve an improved system response time and availability
- Re-active and pro-active measures including the investigation of performance issues and initiating / advising on appropriate actions
- Tuning may, for example, include traffic prioritisation techniques for Quality of Service and Class of Service configuration according to clients business needs

MOVES, ADDS AND CHANGES

- Changes to client's infrastructure associated with a service request as opposed to incident and problem resolution
- MAC's cater for changes in the clients business requirement

REPORTING – NON STANDARD

- Special, bespoke reporting not included in standard reporting set

TECHNOLOGY REFRESH

- Technology refresh enables major changes of technology that globally impact to existing asset base
- The service provides:
  - An audit of the existing Security infrastructure
  - Evaluation of new technologies, business case and approval
  - Design of target infrastructure
  - Physical implementation of new assets
  - Testing and implementation of new solution
  - Handover to live operation
  - Provision of documentation
  - Update architectural blue prints

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

ADVANCED LOG MANAGEMENT

- Post mortem analysis of the logs on the Security (events, rules, CPU, DMZ) to establish root cause of an incident

WEB URL FILTERING

- URL filtering is used to block websites which do not comply with the security policy
- Blocking and blacklisting URL's as per vendor URL database
- Updating blacklists for different categories

WEB CONTENT FILTERING

- Implementation and management of content filtering
- Detection and analysis of malicious codes such as:
  - Malware
  - Virus
  - Trojan
  - Spyware
  - Worm
  - Adware embedded objects
  - Zombies
  - Polymorphic viruses
  - Macros
  - Malicious scripts and file extensions

EXPERTISE

- Lead proposal stage
- Assist in vendor selection
- Create and lead action plans in case of Security specific issues
- Coordination of vendors and partners
- Run cost saving audits

SECURITY BEST PRACTICE REVIEW

- Review of Security infrastructure against industry best practice
- Produce recommendations document, costngs and project plan

USER BASED SECURITY POLICY

- Where next generation Security and Active Directory are integrated, implement and manage Security policy (rule base) based on users / user groups. client sites.

SOBRE A CAPGEMINI

Com 145 mil profissionais em mais de 40 países, a Capgemini é um dos principais provedores globais de serviços de consultoria, tecnologia e terceirização. Em 2014, o Grupo reportou uma receita global de 10.573 bilhões de euros. Em conjunto com seus clientes, a Capgemini cria e entrega soluções de negócios e tecnologia, que atendem às suas necessidades e alcançam os resultados desejados. Como uma empresa essencialmente multicultural, a Capgemini desenvolveu seu modo próprio de trabalhar, o Collaborative Business Experience™, com base no Rightshore®, seu modelo de entrega mundial.

Em 2010, o Grupo Capgemini adquiriu a CPM Braxis, que vem operando com sucesso no Brasil por mais de 30 anos. No final de 2012, a CPM Braxis Capgemini teve sua marca mudada para Capgemini. No País, a Capgemini emprega 8,5 mil pessoas e atende mais de 200 clientes, oferecendo quatro principais linhas de serviços: Applications Services, Infrastructure Technologies & Services, e Business Process Outsourcing (BPO).

Conecte-se à Capgemini no Brasil pelo Twitter, Facebook e LinkedIn.