

11.3.4 Details on the Security Services Proposed Solution

Enterprise Security Operations Center (eSOC)

What is the Enterprise Security Operations Center?

The eSOC is a team of highly skilled security professionals who are responsible for a diverse set of security tasks in order to achieve the security goals of the Commonwealth. The eSOC is not a collection of level one and level two security analysts who monitor security events on a console. Rather, the eSOC takes the information from level one and level two SOC operators as one of many data inputs needed for preventing, detecting, and responding to attacks in the Commonwealth's IT environment.

What is the structure of the eSOC?

The eSOC has the following four roles:

1. The **Security Manager** has overall responsibility for the eSOC and the security services.
2. The **Information Security Advisor(s)** is the highest level role in the eSOC. This individual has ultimate responsibility for the Security Controls Policy Document (GSD331). The advisor creates, approves, and regularly updates the Security Controls Policy Document.

In addition, as the highest level role, this individual is responsible for education and training and offers executive-level presentations on security posture and/or current activities. The Information Security Advisor manages a security risk management process to assist the Commonwealth in fixing current vulnerabilities or accepting the security risk that is posed.

3. The **Security Intelligence Analyst(s)** has a broad range of technical responsibilities. The Security Intelligence Analyst is responsible for day to day activity for Network Intrusion Detection, Host Intrusion Detection, Network Intrusion Prevention, and Vulnerability Scanning. This individual has responsibility for verifying that these services achieve the goals of the Commonwealth. The Security Intelligence Analyst will work closely with the IBM SOC to verify that processes and procedures exist for handling security touch points.

The Analyst(s) conduct the data mining, data analytics, and data visualization in order to find low-and-slow attacks and other non-obvious trends in the attack data. Additional responsibilities are tuning the sensors and maintaining the appropriate profiles for vulnerability scanning, based on the Security Controls Policy Document.

The Security Intelligence Analyst is responsible for monthly conference calls for Intrusion Detection/Prevention and Vulnerability Scanning in order to provide analysis and status.

4. The **Vulnerability Assessment Analyst(s)** is the most sophisticated and most technical role in the eSOC. The Vulnerability Assessment Analyst is responsible for conducting vulnerability assessment on components of the Commonwealth's IT infrastructure. This consists of scanning a target system or network device for security vulnerabilities, and attacking these vulnerabilities in an effort to gain unauthorized access. The purpose of the service is to identify specific security weaknesses on the target systems, and to recommend techniques or improvements to strengthen the security of the target system. This service is provided for all platforms (UNIX, Linux, Windows, etc.). This individual provides assessments on operating systems, common packages, and custom applications.

How do the Commonwealth's eSOC and the IBM SOC interact?

The following is a sample situation of interaction:

1. IBM SOC is monitoring IDS sensors and determines that an event or series of events necessitates a callout.
2. IBM SOC calls the eSOC and provides the necessary information.
3. eSOC analyzes the information and determines the proper response plan.
4. eSOC works with the other IT groups in the event that more information or data is needed in order to determine the propagation and likelihood of success.
5. eSOC determines the proper response.
6. eSOC works with the other IT towers as needed to implement the response.
7. eSOC provides all communication to management and escalation as needed.
8. eSOC owns documentation, process, and procedures for response.

eSOC is responsible for KPIs and security metrics for security incidents.

Intrusion Detection and Prevention Solutions

The Commonwealth Partners are proud to offer an intrusion detection and prevention solution that addresses the detection and prevention of attacks in the Commonwealth. This solution provides fully redundant and scalable 24x7x365 monitoring of intrusion detection and prevention devices.

Intrusion detection services (IDS) and intrusion prevention services (IPS) provide monitoring of the Commonwealth's network, using a combination of hardware and software that is called an intrusion detection/prevention sensor. (Redacted)

Our Key Differentiators

IBM will provide the Commonwealth with a Security Portal which contains a variety of standard and custom reports. Attacks are tracked, reported, and trended on IBM's Security Portal in a number of different ways. The Security Portal produces an 'Executive Summary' report and tracks attacks in a number of various charts and tables.

IBM supports multiple vendors in network intrusion detection, host intrusion detection, and wireless intrusion detection. IBM's infrastructure currently supports over 1,000 network intrusion detection sensors and over 1,000 host intrusion detection sensors. These sensors are deployed in thirty different countries, providing the Commonwealth with global visibility and perspective from attacks around the globe.

IBM provides filtering and tuning best practices along with the capability to create custom signatures (IBM supports filtering and tuning of signatures on intrusion detection/prevention devices to the degree that the intrusion detection/prevention software allows).

Events are sent over encrypted channels.

The Commonwealth's eSOC Security Intelligence Analyst will coordinate analysis and response and provide monthly status calls, as well as additional data mining and data visualization.

IBM has a suite of tools from Security Intelligence to reduce false-positives and false negatives. The Commonwealth's eSOC Security Intelligence Analyst will make recommendations for reducing false-positives and false-negatives.

Deliverables

We will provide the following deliverables:

- 24x7 Security Operations support with callout for critical events
- Security portal with reports made available to security leads
- Security Intelligence and Analysis via the eSOC
- Monthly Conference Call via the eSOC
- IDS engineering (filtering, tuning, etc) via the eSOC

Vulnerability Management

The Commonwealth Partners provide both breadth and depth in assisting customers with managing vulnerabilities in their enterprise. Vulnerability scanning services consist of testing a target system, based on the “Best Practices” Security Policy for known vulnerabilities and configuration weaknesses, and then reporting on problems found. Vulnerability scanning is optimized to create minimal impact on well-configured systems. Targets can be identified as specific IP addresses or network ranges where the scanning tool will determine active systems for testing. The scanning report will be configured (filtered) according to the security controls for the Commonwealth and will only flag problems that are in violation of the security controls. The basic report will also include a risk assessment with aging, and a reference describing the problem. The output from the vulnerability scans is reviewed by the eSOC to verify that the test ran successfully. A summary report will be created and provided to the Commonwealth and to the service providers for the appropriate and corrective action to be taken. All scanning services involve execution of the type of scan selected, a basic report of findings, and security exposure notification. In addition to the base scanning services and extranet scanning, additional finding analysis and customer conference calls are available as Subscription Services.

Redacted

Our Key Differentiators

Our solution includes a Security Portal that contains a variety of standard and custom reports. Vulnerabilities are tracked, reported, and trended on the Security Portal in a number of different ways. The Security Portal produces a summary report, along with tracking vulnerabilities by delinquency date, severity, OS, and status, as well as a variety of other charts and tables.

Correlation of the Commonwealth’s vulnerability scanning data with IDS/IPS data will occur in real-time.

The eSOC Security Intelligence Analyst will become very familiar with the Commonwealth’s environment and can be a partner in maintaining a high level of security. **Redacted**

Deliverables

We will provide the following deliverables:

- Security portal with reports made available to security leads
- Vulnerability scan performed at specified intervals
- Enhanced finding analysis and investigation with recommendations
- Weekly service audit
- Monthly Conference call

Solution Architecture

IBM’s vulnerability management solution is illustrated below:

Redacted

Figure 11.3.4-1 - Vulnerability Management Solution