JNDMS Task Authorization 2 Report

Prepared By:
MDA Systems Ltd.
Suite 60, 1000 Windmill Road
Dartmouth NS B3B 1L7
MDA Reference # DN1010, Issue 1/1
Contract Project Manager: Brett Trask, 902-481-3511
PWGSC Contract Number: W7714-040875/001/SV
CSA: Marc Gregoire, JNDMS Project Manager, 613-998-2113

Contract Report
DRDC-RDDC-2014-C63
October 2013

Principal Author

Original signed by Scott McDonald

Scott McDonald

Project Engineer, JNDMS

Approved by

[Approved By Name]

[Approved By Position/Title]

Approved for release by

[Released By Name]

[Released By Position/Title]

Abstract

This report covers the activities and results for Task Authorization #2 as part of the Joint Network Defence and Management System (JNDMS) Technology Demonstrator.

Résumé

Le présent rapport traite des activités et des résultats touchant l'autorisation des travaux Nº 2, dans le cadre du démonstrateur de technologies du Système interarmées de défense et de gestion des réseaux (SIDGR).

Executive summary

JNDMS Task Authorization 2 Report

; DRDC Ottawa CR ; Defence R&D Canada – Ottawa; October 2013.

Introduction or background: The Joint Network Defence and Management System (JNDMS) Technology Demonstration project evaluated how custom and off the shelf tools could be used to provide enhanced Situational Awareness for networks. This document provides a report on the second Task Authorization as part of this Technology Demonstrator. The aim of this task authorization was to deploy JNDMS on the DREnet.

Results: The JNDMS was deployed on the DREnet and the resulting system was demonstrated.

Significance: A risk throughout the project was how much effort it would take to deploy on a real network and to evaluate the tools in a more realistic situation.

Future plans: A transition report is part of the TD and will identify future possibilities for this technology.

Sommaire

JNDMS Task Authorization 2 Report

; DRDC Ottawa CR ; R & D pour la défense Canada – Ottawa; October 2013.

Introduction ou contexte : Le projet de démonstrateur de technologies du Système interarmées de défense et de gestion des réseaux (SIDGR) a évalué comment utiliser des outils personnalisés ou disponibles commercialement afin d'améliorer la connaissance de la situation en réseau. Le présent document constitue le rapport sur la deuxième autorisation des travaux, dans le cadre de ce démonstrateur de technologies, qui a eu pour but de déployer le SIDGR sur le réseau DREnet.

Résultats : Le SIDGR a été déployé sur DREnet, et le système en découlant a fait l'objet d'une démonstration.

Importance : Pendant tout le projet, les efforts nécessaires pour déployer ce système sur un réseau opérationnel et pour évaluer les outils dans un contexte plus réaliste ont constitué un risque non négligeable.

Perspectives : Un rapport de transition au milieu opérationnel fait partie du DT; il décrira les diverses possibilités de cette technologie.

Table of contents

List of figures

1 Introduction

1.1 Overview

The purpose of this document is to report on the findings and activity for Task Authorization #2 of the Joint Network Defence and Management System (JNDMS) Technology Demonstrator Project. This document specifies DID SD-006 and covers CDRLs 31, 32, 33, 34, and 35.

2 Task Activity and Findings

This section discusses the findings derived from the five activities identified in the TA2 Statement of Work (SOW).

2.1 Project Management

This task included the planning, tracking and management of this Task Authorization. The effort to perform these tasks as well as technical reviews, monthly progress reports and this final report were part of this task.

2.2 NIO SOC Activities

The activities as part of this task included the setup of the JNDMS lab at DRDC-Ottawa for testing and demonstration purposes. This section identifies the components and efforts to secure appropriate permissions from the required stake holders.

2.2.1 DREnet

The DREnet is a special purpose R&D network that enables the Defence Research and Development Canada (DRDC) agency to undertake collaborative research on Department of National Defence (DND) research programs. Since its inception in 1985, the DREnet has achieved numerous milestones in the use of wide area network technology in support of collaborative defence research. The present day DREnet provides a flexible and rich network environment of interconnected network zones that facilitate collaboration between DRDC research centres, allied research centres, universities and defence contractors.

The DREnet is operated by the DREnet Management Contractor under the direction of the Directorate Research Development Knowledge and Information Management (DRDKIM) of DRDC. NRNS Incorporated, a JNDMS project team member, currently serves as the DREnet Management Contractor. Each DRDC research centre nominates a member of its Information Technology (IT) staff to serve as the Technical Point of Contact (TPOC) for the DREnet. The DREnet Management Contractor works closely with the TPOC membership to coordinate capability deployments and upgrades, problem resolutions and incident responses.

While the DREnet is an excellent candidate network for the deployment and "performance tuning" of the JNDMS TD, planning took place to ensure that there was minimal impact on the "production" functions of the network and that the JNDMS TD does not jeopardize the performance or security of the network.

The DREnet was the target network for the NIO SOC to monitor.

2.2.2 DRDC NIO SOC

The JNDMS takes inputs from key network management technologies and security products such as IT topology data, software asset inventory, IDS alarms, and asset vulnerability data to provide an SA "picture" to network stakeholders. The SA picture is primarily intended for Network Operators and best resides in an Operation Centre. However, due to the critical work performed by these stakeholders in a production network such as the DREnet, the deployment of JNDMS was setup to avoid putting operational DREnet management at risk by standing up a "Shadow Network Operations Center" or rather a "Network Information Operations Security Operations Center". This approach served a number of benefits, chief among which is the ability to test, experiment and develop CND technologies with minimum impact of current DREnet management operations.

Some benefits identified prior to the standing up the NIO SOC were:

- Seize the opportunity of demonstrating world-leading CND integration capabilities on life-size dynamic network.
- Capture system integration and deployment requirements such as technology interfaces requirements, deployment costs and level of efforts, users and system administrators' acceptance, etc, in the context of a "live" network. Lessons learned thereby collected would feed DND capital project to reduce risk.
- Investigate some of the process reengineering requirements associated with performing network performance and security management in the JNDMS paradigm.
- Provide a standard-based integration platform for CND SA related research, technology testing, validation, demonstration and transition, as well as a foundation for potential collaborative R&D projects with other GoC departments and allies.

2.2.3 Physical and Logical Location

The NIO lab located in Building 94 at the Shirleys Bay DRDC campus was the location chosen for the NIO SOC. Part of the equipment was physically located in Building 94 either on lab benches or racked in the server room.

A logical network was setup within the NIO SOC, identified as niosoc.drenet.dnd.ca. This setup required additional support infrastructure to be managed directly by DREnet management in Building 75. The integration components housed in Building 75 provided the branching off point between the JNDMS shadow SOC (NIO SOC) and the rest of DREnet.

2.2.4 Network Diagram

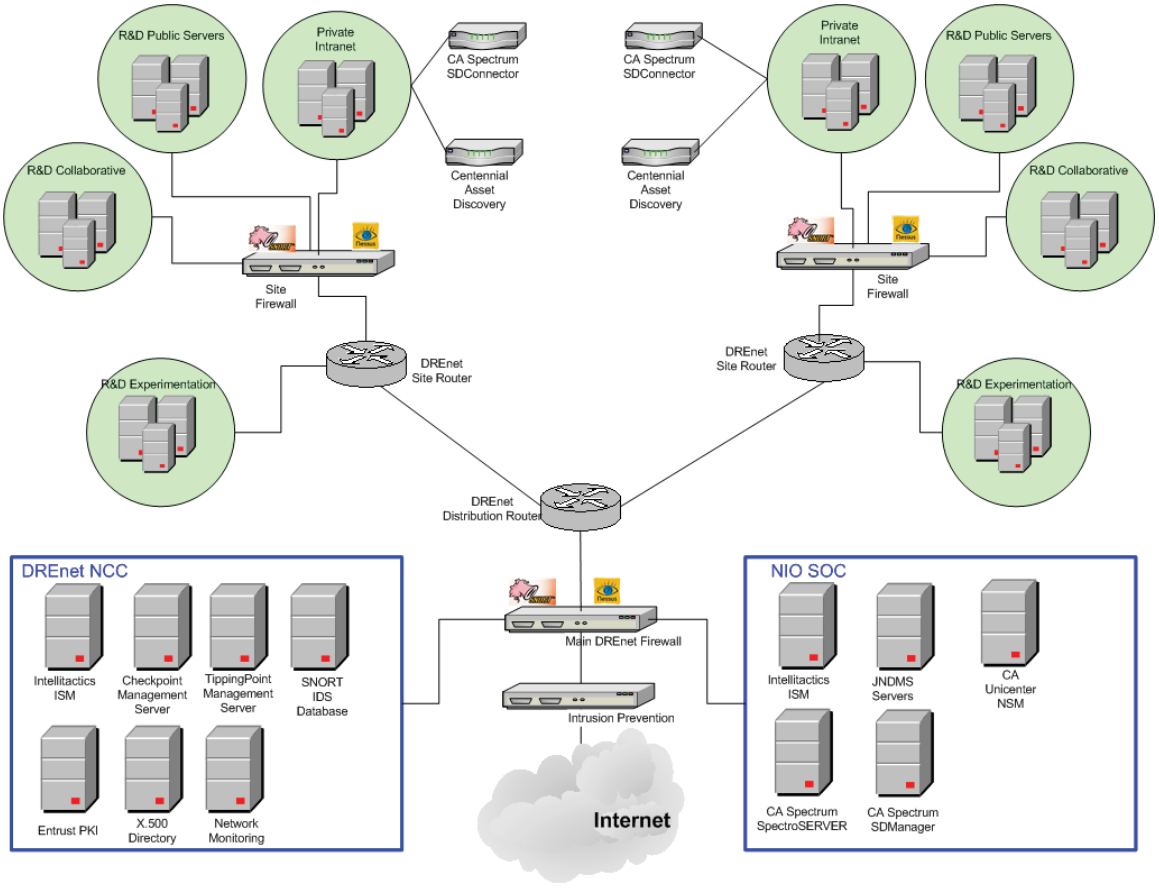

Figure 1: Network Diagram

Figure 1 illustrates the DREnet network architecture, but only shows two of the eight DRDC sites. The DREnet Network Coordination Centre is housed in a dedicated network segment connected to the main DREnet firewall. The NIO SOC is shown in its own dedicated network segment connected to the same main DREnet firewall. Each DRDC site included a deployed firewall with some intrusion detection and vulnerability scanning capability.

All DREnet firewalls were managed and maintained by the NRNS DREnet Management team.

2.2.5 DREnet Data Sources

DREnet data was mandated to remain in the NIO SOC at all times. Any DRDKIM approved data extracts or samples removed from the NIO SOC were to be subjected to a data sanitization processes. During the execution of TA2 no data was extracted from the NIO SOC.

Data types used in the JNDMS DREnet deployment are as follows:

- IT Topology data: Network discovery tools (such as CA Spectrum) are used to scan the network to discover all systems, routers, and switches and the linkages between them. The resulting data is a picture of the entire network as it is currently configured and operating. Spectrum was used to provide this data.
- Vulnerability Assessment (VA) data: Network Vulnerability Scanners are used to probe computers for security vulnerabilities, and to produce output listing potential security holes in those systems. nCircle IP360 provided this data.
- Network Intrusion Detection System (IDS) alarms: IDS' (such as Snort) are used to monitor network traffic for evidence of exploit attempts, security breaches, and network reconnaissance. When an IDS detects suspicious traffic, it raises an alarm. IDS components were part of the firewalls deployed and reported through Intellitactics.
- Firewall Policies: The firewall rules on the main and site firewalls determine what systems and services can transmit across these security perimeters. Taken as a whole this is the "blueprint" of the security perimeter of the network. The firewall rules were provided by a manual extract using a tool called CPRules.
- Firewall logs: The firewall logs show the successful and failed connection attempts across the security perimeter of the network.
- Availability monitoring data: Enterprise Infrastructure Management (EIM) tools such (such as CA Spectrum) are used to monitor the current "up/down" status of key assets on the network.
- Hardware and Software Inventory: Asset Management software (such as Centennial Discovery) is used to provide detailed inventories of monitored systems including the exact hardware and software configurations. Ideally this would include all DREnet workstations.
- Military Operations data: This is (fictional, not collected from the DREnet) data which defines the dependence of military operations on IT services and assets.
- Services data (client server relationships): This is (fictional, not collected from the DREnet) data which defines the relationships between clients and servers.

2.2.6 Permissions and Security Precautions

As part of the NIO SOC activities there were a number of stakeholders that had to be apprised of our intentions and their permission would be required for any deployment activities. NRNS were instrumental in providing appropriate interfaces to the DREnet management group and to DRDKIM. These groups had to assess JNDMS and ensure that the deployment activities would not compromise security or the operations of the network.

To manage this, the details of the DREnet deployment efforts and the JNDMS were provided to them and their comments or concerns were addressed as part of these activities.

This section identifies the permissions and security precautions that were employed as part of the deployment efforts.

2.2.6.1 Security of Data in Motion and Data at Rest

All DREnet data was to be safeguarded by appropriate technology and operating procedures both while in-transit (on the network) and at rest (stored on systems in the NIO SOC). Access to the JNDMS system was to be authenticated with Entrust certificates issued by the DREnet Public Key Infrastructure (PKI) server. Remote access to the data was secured using SSL/TLS over HTTPS (TCP/443). While at rest, the data was be secured on the systems using disk encryption on JNDMS servers, and the servers were physically secured inside locked racks inside the Building 94 lab. Access to these servers was restricted to DRDC personnel and their DREnet management team.

2.2.6.2 Physical Security

Entry to the NIO lab, and adjoining server room are controlled by access cards, as is Building 94 itself. NIO section personnel have card access to the lab and server room. Access to Building 94 is also limited, but includes a number of private companies who maintain offices within the building. Additionally the NIO SOC server equipment was contained within a locked rack in the server room.

2.2.6.3 Cyber Security

The level of network security would be equivalent to the current DREnet NCC servers in their "parallel" security zone off the DREnet firewall. The DREnet firewall managed by NRNS DREnet Management team controlled network access to the NIO SOC.

Systems deployed in the NIO SOC were subjected to a number of security constraints:

- Systems hardened according DREnet NCC standard practices, such as:
  - Automatic patching enabled;
  - Turn off unnecessary services;
  - Disabling unused accounts; and
  - Tightening File Permissions.

- Anti-Virus with automatic .dat file updates (Windows); and
- Vulnerability Scanned prior to deployment.

Additionally the JNDMS Web Portal, which gives access to the Network Management and Security data was restricted to HTTPS (TCP/443) authenticated access. Any additionally personnel wishing to access the NIO SOC must have the approval of DRDKIM and the NIO.

2.2.6.4 Data Sanitization

Any data extracts or samples removed from the NIO SOC must be approved by DRDKIM and be subjected to a DRDKIM approved data sanitization process. The JNDMS team was responsible for providing a suitable data sanitization process for DRDKIM approval. Data sanitization was to include at minimum alteration of IP addresses using a "data transformer" process. The purpose of extraction is to deliver realistic data to the JNDMS development lab.

- IT Topology data (i.e. network discovery scan data): An extract of a network discovery could be sanitized and extracted.
- Vulnerability Assessment (VA) data: Not to leave the NIO SOC environment. This data can be synthesized by scanning "real" hosts in the JNDMS development lab environment and cloning the results to create numerous instances of vulnerable hosts.
- IDS alarms: Samples of alarm logs, with IP addresses transformed could be extracted. The payload of the packet that triggered the IDS alarm must not leave the NIO SOC as it may contain sensitive information such as usernames and passwords.
- Firewall Policy data: Not to leave the NIO SOC. This data can be synthesized in the JNDMS development lab at MDA Halifax and NRNS Ottawa.
- Firewall logs: Samples of firewall logs, with IP addresses transformed could be extracted.
- Availability monitoring data (Spectrum): It is more practical to synthesize this data in the JNDMS development lab than to extract it.
- Hardware/ Software Inventory: Potentially a subset of DREnet assets could be inventoried, the resulting inventory data sanitized and extracted.
- Military Operations data: These scenarios would be created in the JNDMS lab (and brought into the NIO SOC).
- Services data (client server relationships): These would be created in the JNDMS lab (and brought into the NIO SOC).

A data sanitization tool was developed and the results were discussed with DRDKIM. During the execution of TA2, however, no data was extracted from the NIO SOC. This tool could potentially be used in the future if there is a requirement to extract portions of the collected data.

2.2.7 JNDMS Deployed Components

This section identifies the core components deployed as part of or to support JNDMS. These are broken down in to the DREnet furnished components, the JNDMS Furnished components and the NIO furnished components. The list of components was used as part of the planning and in discussions with stake holders.

2.2.7.1 DREnet Furnished Components

- Intellitactics Security Manager
- Snort/ Snort DB
- Checkpoint FW-1
- Centennial Discovery software and hardware inventory management
- nCircle IP360 licenses
- Server hardware

2.2.7.2 JNDMS Furnished Components

The following was deployed as part of the core of JNDMS:

- Intellitactics Security Manager. An ISM is deployed as part of JNDMS, in addition to the existing ISM installations so that custom rules can be deployed without impacting the operation of the DREnet.
- CA Spectrum: Network discovery and availability monitoring tool used by JNDMS TD
- nCircle IP360: (vulnerability scanner chosen by CF for the DWAN). Note that the appliance was supplied by JNDMS, however the licenses were part of the DREnet furnished components
- JNDMS hardware
  - 6 rack mount servers comparable to HP ProLiant DL380
- JNDMS software
  - Windows Server and Redhat Enterprise Linux operating systems
  - DRDC developed JNDMS software
  - Apache Tomcat
  - Oracle RDBMS
  - Liferay Portal (deployed but not part of demonstrated system)

2.2.7.3 NIO Section Furnished Components

- Rack space, power, physical access control
- Network connectivity (fiber from Building 75 to 94)

2.3 System Preparation

The system preparation task was to install the JNDMS support lab as well as provide updates to the system to address integration or scalability issues.

2.3.1 JNDMS Development Lab

The main JNDMS Development lab is located on MDA premises in Halifax and a secondary lab currently exists in the NRNS offices near Shirleys Bay. A VPN was setup so that the development personnel could gain access to a Microsoft Terminal Server as part of the NIO SOC. This access was setup to ensure that data could be sent to the NIO SOC, but not removed.

Updates to the system in the NIO SOC was performed by code updates being pushed into the NIO SOC from the Halifax lab and a development environment within the NIO SOC was used to build and deploy the components. Any updates to components housed in Building 75 were manually inspected and installed by DREnet management.

2.3.2 System updates

The system was updated to address new integration points as well as concerns noted on scalability and stability.

The significant updates included the following:

- Integration of IP360. This was identified as the primary vulnerability assessment tool.
- Integration of Centennial. This was a new tool used for the collection of software inventory.
- Updates to the integration of Spectrum. There were a number of issues with the integration of Spectrum, including possible issues in the deployment of Unicenter NSM. Spectrum had been identified as a tool that DREnet management would want to continue to evaluate and support in the future, however the role of NSM was not so clear. Part of the updates was to ensure that JNDMS could run without NSM. This update also simplified the integration of Spectrum.
- Updates to the integration of Intellitactics. The integration with ISM was updated to better handle correlated events, to export asset valuation back to ISM and to update the escalation rules to JNDMS. (See Annex A for reference notes on ISM escalation used for TA2).
- The ability to ‘fork’ the flow of security event data from a live ISM install into the JNDMS NIO SOC was deployed and tested.
- Updates to the various client programs to support the split deployment between Building 94 and Building 75.

- During the final stages of preparation of the demonstration there were still a number of issues relating to the user interface (portal), including some performance issues. A review was held at this point to determine the best way to update the portal. A new technology, the Google Web Toolkit, was evaluated and it was found to provide significant improvements over the current tool set. It was, however, identified as a risk to make such a change this late in the project. The possible alternatives were reviewed with DRDC Ottawa and it was decided that the improvements to the look and feel as well as the user interaction warranted the risk to migrate the portal to this new technology. The new portal was written and was the version demonstrated at the end of TA2.
- A 3D map view was added using the Google Earth Plugin.

2.4 System Deployment

The system was rolled out over several months and the results were examined to evaluate how the new portal behaved. The portions of DREnet that were part of the network monitoring included sites across Canada (see Figure 2).

Figure 2: DREnet Sites

The portion of DREnet that was part of JNDMS for the final demonstrations included:

- 3264 hosts (desktops and servers)
- 473 network devices
- 27 routers
- 10 firewalls
- 126K software assets (2 sites)

The demonstrations were held on 25 and 30 June 2009 and consisted of a short presentation followed by a live demonstration of the system on the DREnet and an opportunity for questions and answers.

The updated portal that was demonstrated used the Google Web Toolkit and consisted of the basic flow and concepts developed with the previous portal. The portal (see Figure 3) consisted of a side panel, and primary view, a secondary view and a global status area.

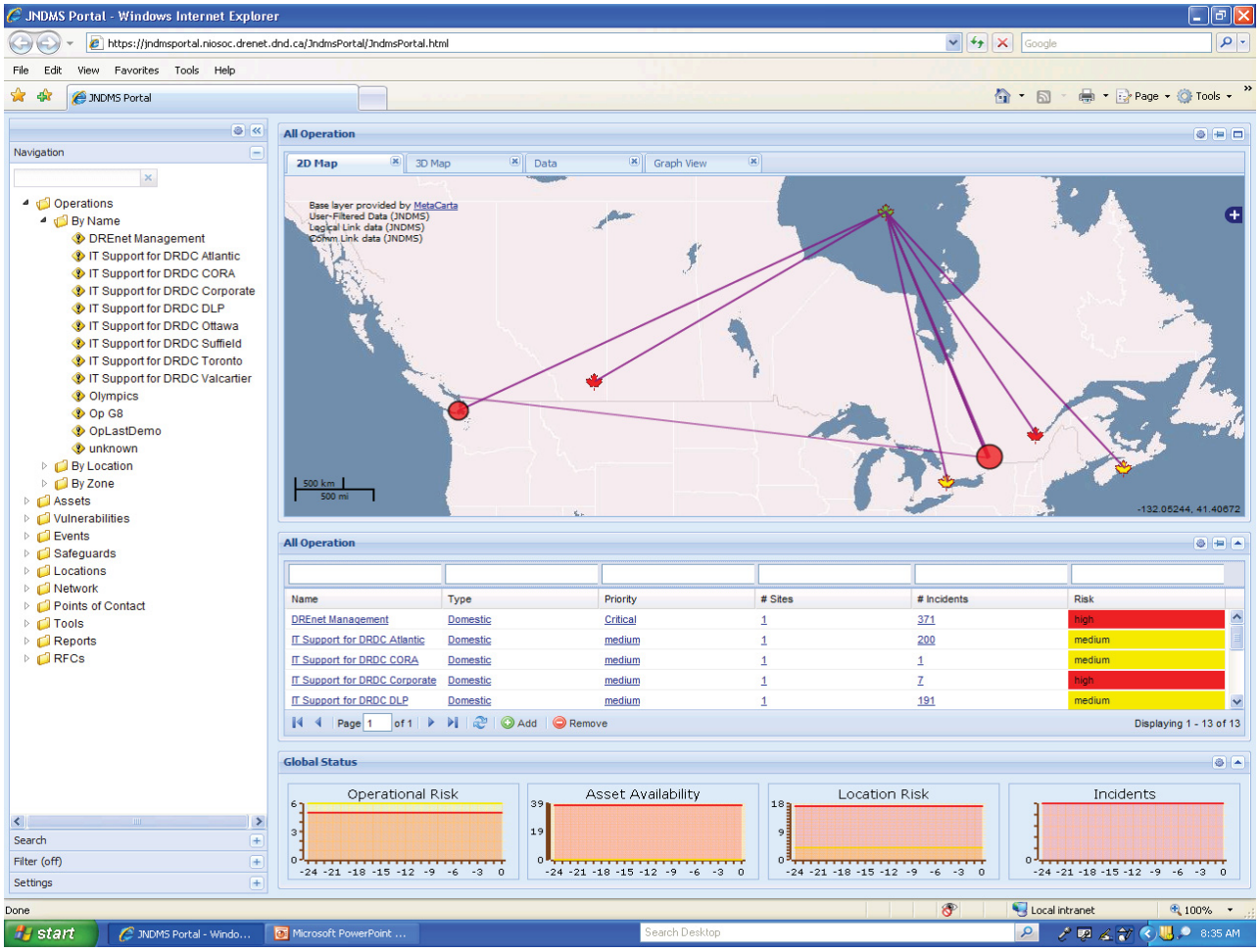

Figure 3: JNDMS Portal Overview

The hyperlinks provided within the portal would allow detailed information to be shown in the secondary view while the primary view was used for summary information (see Figure 4). The primary display could show text or data views (see Figure 4), maps or visualization.

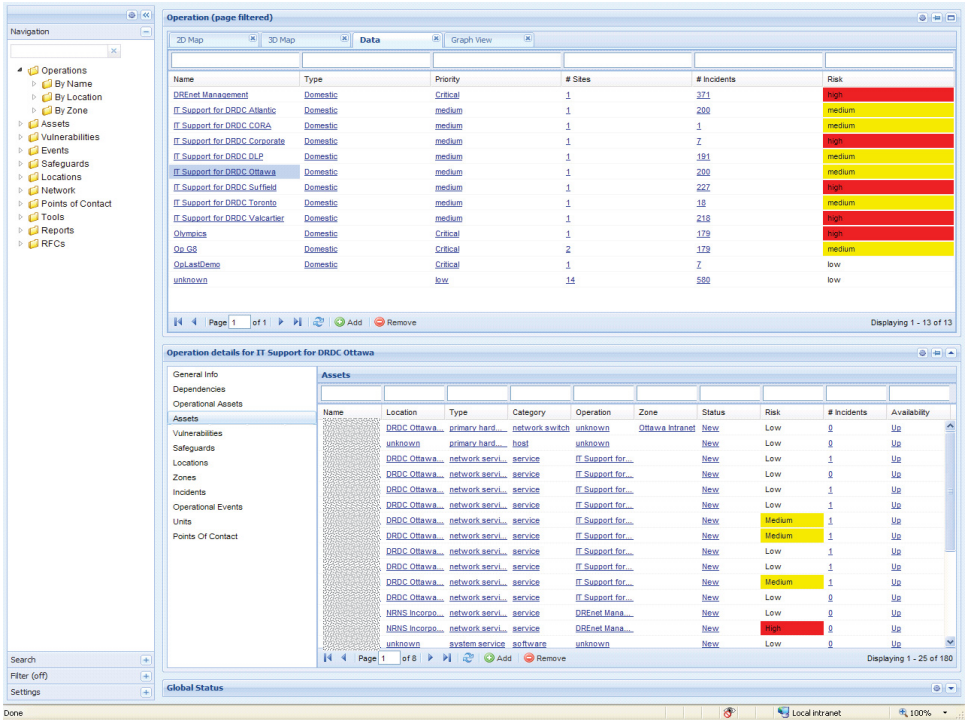

Figure 4: Portal Data Views

The visualization view (see Figure 5) could be used to explore relationships between items within JNDMS in a graphical manner.

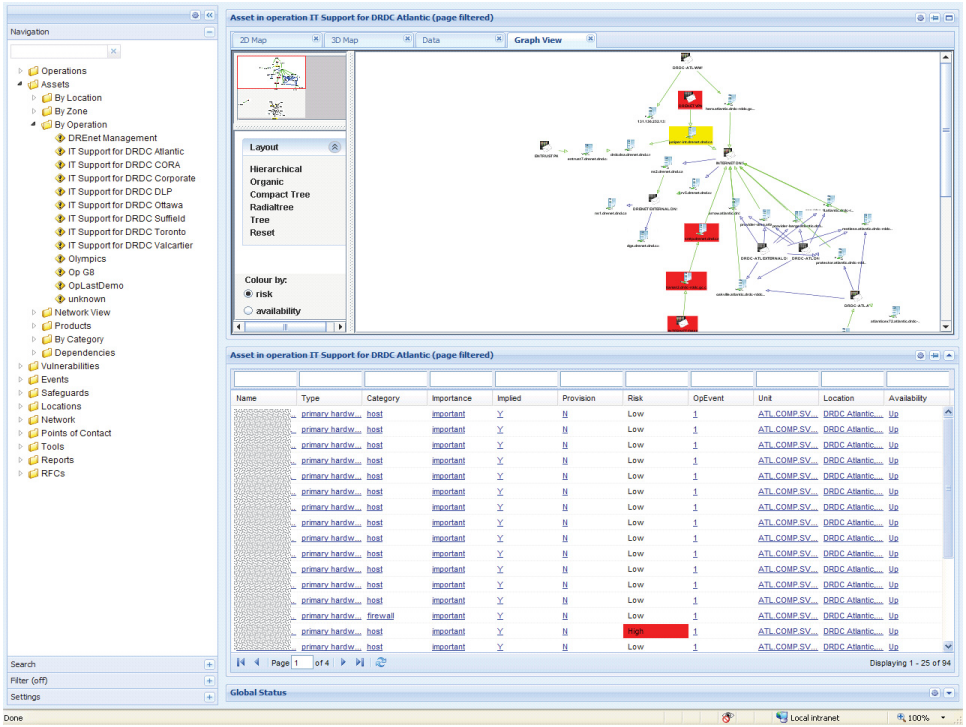

Figure 5: Portal Visualization View

As part of the demonstration a 3D map view was added to explore alternate GIS presentations (see Figure 6). The 3D map was provided using the Google Earth Plugin and prototype code on loan from another MDA project.

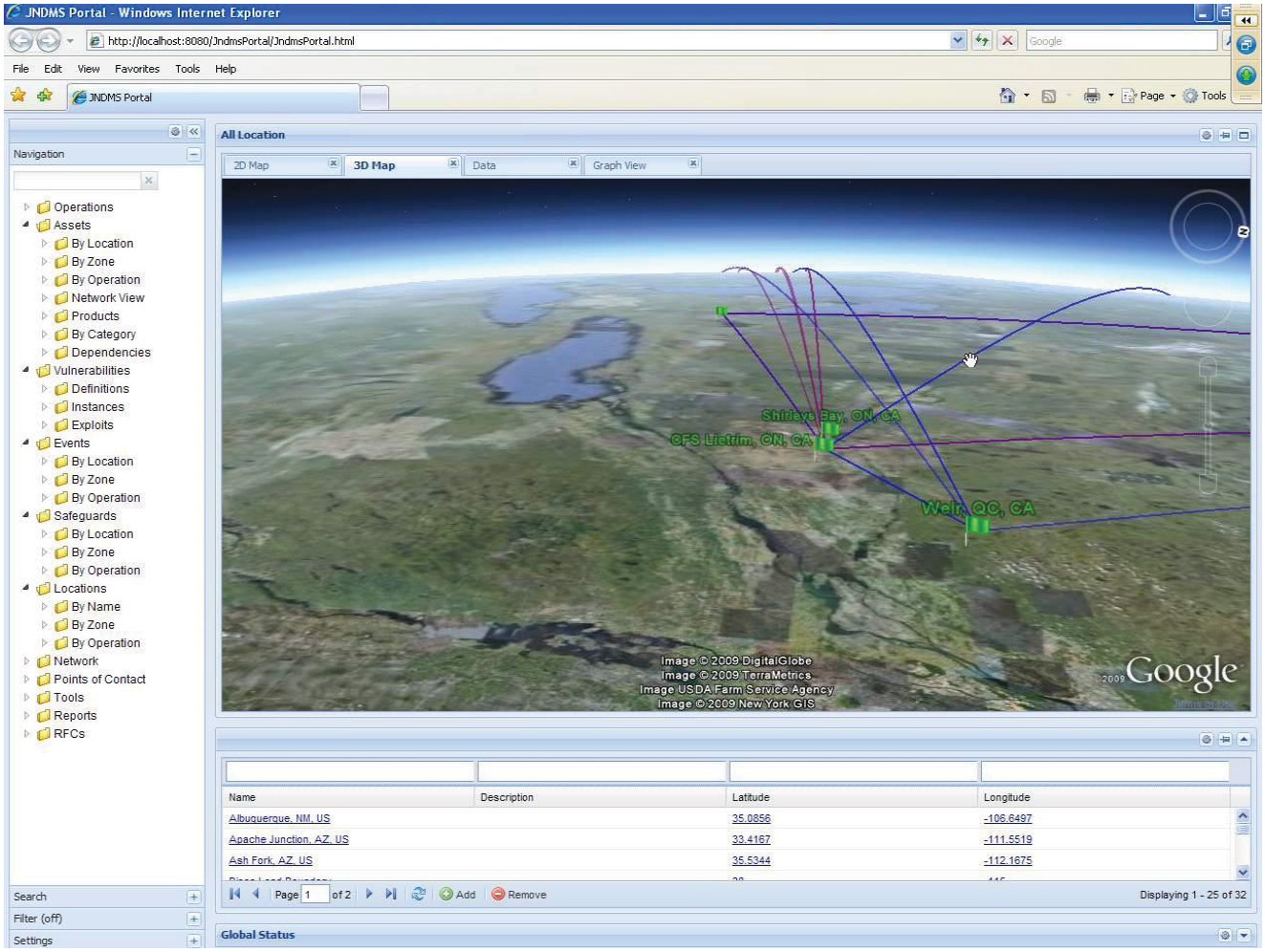

Figure 6: Portal 3D Map View

More detailed information on the new portal and how to use it can be found in either the Design Document [1] or the User's guide [2].

2.5 System Support

The system support task was to ensure that the system remains running during the time frame of this task authorization. This task included support to DRDC on the running of the system and also included an outline of support activities that would be performed.

2.6 In-Service Support Activities

The support structure will include a mix of NIO permanent scientific and support staff, as well as Contractor support. The NIO section will report to the DRDKIM all significant JNDMS configuration and support structure changes during the in-service support period.

The following in-service support activities will be undertaken by NIO:

1. Server OS and baseline: The JNDMS servers will be configured with DRDC baseline anti-virus, and periodic vulnerability/patch updates requirements analysis will be done. These tasks will be performed by NIO support staff with the help of DRDC Ottawa IT staff.

2. The JNDMS system will be scanned daily and automatically for vulnerabilities using either Nessus or IP360. The results of these scans will be reviewed by NIO staff and sent to DREnet managers along with other DREnet vulnerabilities scans. Patch/updates will be assessed jointly by NIO and DREnet management. Limiting JNDMS exposure to external threats will be the preferred course of action to avoid JNDMS configuration impact and DREnet risk.

3. Licences: JNDMS uses a mix of COTS and Open Source software. The Open Source components will only be updated in the case of vulnerabilities, or to provide additional functionalities required for research initiatives. The COTS licences will be transferred to the NIO section after JNDMS contract completion. Some COTS licences may be transferred to DRDKIM DREnet management team, such as CA Spectrum. The NIO section will assume license maintenance/support fees on an "as-needed" basis.

   The following COTS licenses will be deployed and maintained within JNDMS:

   a. Server OS: DRDC Corporate license will be used:

      i. MS 2003 server;

   b. Oracle 10i: Development license;

   c. Intellitactics: Research license;

   d. CA Unicentre;

   e. ESRI server;

   f. Operating systems (Redhat, Fedora) supplied with servers.

4. Data management: The JNDMS data will be stored and archived in the NIO lab, by NIO staff. Research activities requiring access to stored data will be conducted exclusively on the JNDMS DREnet subnet zone. Otherwise, request will be staffed to DRDKIM on a case by case basis, and data-sanitization will be used as required.

5. Network Connectivity: The JNDMS will be set-up in a new DREnet zone with restricted external access for data (AV .dat files, NIST CVE feeds, etc) updates. This zone will allow JNDMS to retrieve sensor data from the DREnet NOC and access JNDMS specific sensors such as Spectrum and IP360. To maintain this connectivity, DREnet management staff should keep NIO staff informed of significant network configuration changes which may affect JNDMS components.

6. Performance and availability: The JNDMS will remain a research platform and as such, shall never be used for operational reasons, unless clearly identified as part of an experiment (ex: operational research, situational awareness and/or process analysis study). Therefore, it is understood that JNDMS quality of service requirements will come second to operational priorities.

7. Security Officer: The DRDC Ottawa ISSO shall serve as the security officer for the NIO SOC. All security events (malware, virus, compromise, vulnerabilities, etc) will be reported to this person who will be responsible to DRDKIM DREnet management for proper mitigations implementation throughout the life of the JNDMS.

8. Contract Management: The NIO section will manage all contractual vehicles required for the in-service-support and development of the JNDMS, and will inform the DREnet management of all contract requirements prior to contract award.

Annex A ISM Escalation Reference

The objective of this document is to describe the mechanisms by which network security events are repressed or escalated to JNDMS as Incidents. There are several places where the JNDMS/ security administrator can make adjustments to the default settings to change various thresholds and filters to this escalation process. Understanding the escalation process and the ways it can be modified will allow the JNDMS administrator to tailor it to their environment and needs. The escalation process described uses the example of the JNDMS deployment on the DREnet as the context.

Overview

The stages a security event goes through in becoming an Incident in JNDMS are as follows:

1. Malicious or anomalous traffic is detected on the network by a Network Intrusion Detection System (NIDS) sensor, raising an alarm.

2. The alarm is sent from the sensor to the NIDS database.

3. The Security Information Management (SIM) data acquisition (DA) server periodically polls the NIDS database for new alarms.

4. The SIM rules and correlation servers take alarms from the DA and prioritize them using a "Risk Scoring" algorithm.

5. The SIM Security Operations Center (SOC) server takes the prioritized set of alarms and slots them into buckets (such as "Correlated Alerts", "Primary Alerts", "Secondary Alerts", and so on) based on user-defined thresholds.

6. The JNDMS alarm escalation process periodically takes the alarms (and their associated events) from the highest priority buckets (Primary and Correlated Alerts) and sends them to the JSS/DSS (Decision Support System).

7. The DSS uses a set of user-defined criteria to determine which types of alarms should become JNDMS Incidents and which become JNDMS "events."

8. The DSS compares the new alarms with the current set of Incidents and represses duplicates.

Each of these steps is described in greater detail below, along with if and how the escalation process can be modified by the user.

A.1 NIDS Sensor Detection

The Network Intrusion Detection System (NIDS) in this deployment is the open source tool Snort. Each Snort sensor monitors the flow of network traffic at the perimeter of the various security zones on the DREnet.

Each sensor raises alarms based on a set of pattern matching rules called signatures. Signatures are automatically updated on a daily basis to keep up to date with the latest threats.

User configurable parameters

A user can control which alarms are generated at this level by modifying the signatures running on the sensors.

- Signatures can be added or removed as required. Signatures that generate a large number of false positives on a given sensor are typically removed. This can vary depending on environmental factors of the monitored network.
- Signatures that are generally useful, but have a known false trigger can be modified to ignore that specific trigger, for example a given host that does network vulnerability scans might be explicitly ignored by a sensor so as not to generate thousands of false attack alarms when it runs.

This signature modifications are normally performed by the IDS managers on an as needed basis; in this case the DREnet Management contractor on behalf of DRDKIM.

A.2 NIDS Database

The DREnet Snort infrastructure uses Barnyard to store alarms from all DREnet Snort sensors in a MySQL database. Barnyard is an open source tool designed to work with Snort to take alarms from multiple sensors and store both the alarm (and in many cases the payload of the packet that triggered the alarm) into a database in an efficient manner.

This step in the data chain between sensor and JNDMS has no user configurable parameters.

A.3 SIM Data Acquisition

The DREnet corporate SIM (Intellitactics Security Manager – ISM) uses a “Data Acquisition” server (DA) to periodically poll the DREnet Snort database for new alarms and pull them into the rules system for processing. A custom rule has been written on the DREnet ISM to create two copies of those alarms. A cron job running on the DREnet corporate ISM moves the copy of the harvested alarm data over to the JNDMS integration server on the DREnet management LAN. A service on the JNDMS integration server sends the alarms to the “inbox” of the ISM DA on the NIO SOC LAN. Another cron job ensures that if data delivery is not possible, files older than a certain threshold are deleted, so that if the ISM DA is unavailable for a long time, it does not fill the drive on the JNDMS integration server, or overwhelm the DA once it comes back online.

User configurable parameters

The user of the DREnet corporate ISM can control the polling interval of the DA to the Barnyard DB, which affects alarm latency and performance of the servers.

The user can control how long alarms are cached on the JNDMS integration server before they are discarded, by modifying the data delivery cron job.

A.4 SIM Rules and Risk Scoring

The ISM "Threat Detector" (TD) and "Threat Evaluator" (TE) use a system of correlation, aggregation, escalation rules, and filters to group and prioritize alarms.

One of the factors used to prioritize alarms in ISM is the operational value of the assets involved. This asset value, called "Operational Risk" in the ISM context is expressed as a number between 0 and 5. In the JNDMS deployment all assets known to the JNDMS system (e.g. through Spectrum discovery) have a value greater than 0. These values are generated by JNDMS and pushed into the SIM to product an Operation Risk value of 1-5 for all assets.

User configurable parameters

There are a number of user configurable parameters for this step.

Correlation Rules

ISM has a number of user modifiable correlation rules which come with the product, and others can be created at the user's discretion. These rules can be enabled/ disabled, or modified from within the ISM Administration Console. While there are a number of steps in the data flow within ISM which precede the correlation rules, the first place relevant to alarm escalation to JNDMS is in the "Threat Detector" (TD) subsystem. The correlation rules are applied to security events as they pass through the TD, weighing each event against such criteria as environmental data, source and target history, vulnerability status, similar events which have occurred in a specified time period, and so on. Many of the correlation rules generate a new alarm of a "correlated" type rather than passing the original event on through the escalation path; a good example of this is when many events are taken together to represent a single correlated alarm.

To view and modify the default correlation rules, log in to ISM using the Administration Console and navigate to the TD in the "Domain Navigation" panel. A set of nested folders under this subsystem (shown following as the niotd) contain bookmarks to various key settings and configuration panels in ISM.

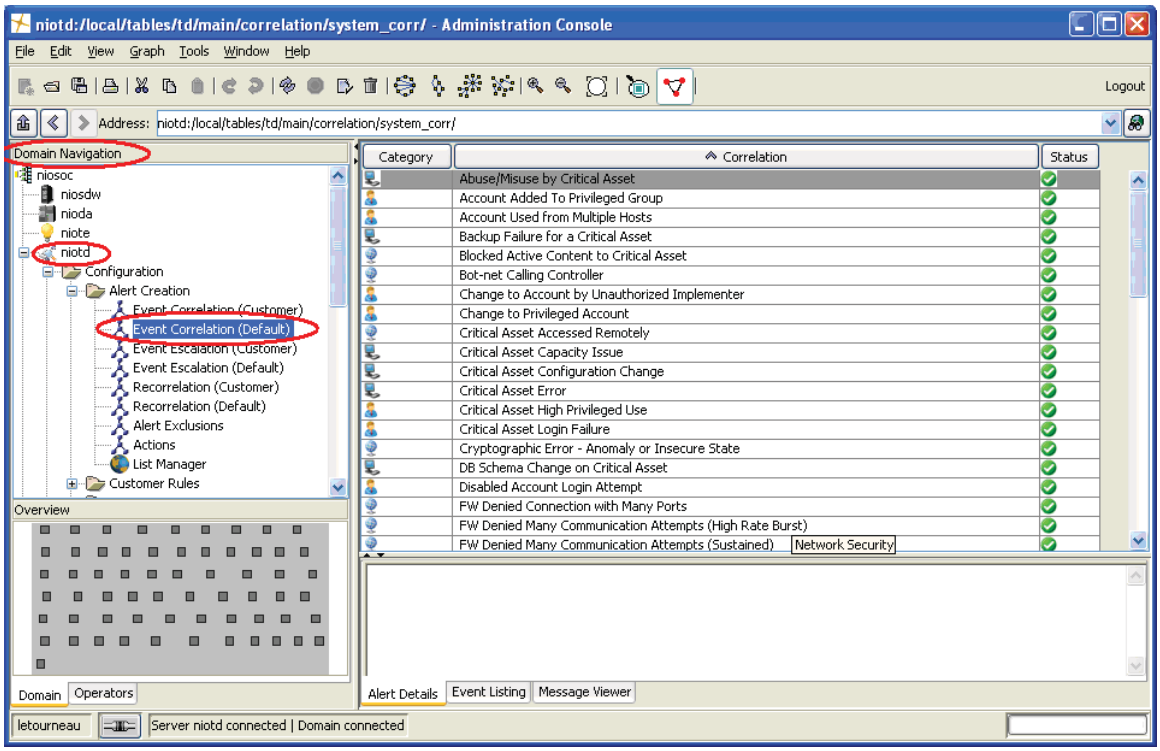

Figure 7: Modifying Correlation Rules

Modifying Correlation Rules

Each of the correlation rules in the TD have one or more user modifiable parameters, which are accessed by opening the "meta panel" specific to the rule. A meta panel is an ISM dialog box with user editable controls specific to the system element being modified and is typically accessed by double clicking on an item (such as a rule) or using a bookmark in the Domain Navigation panel. An explanation of the correlation rule, along with the modifiable fields is found in the meta panel.

This example shows a rule detecting "Abuse/ Misuse by a Critical Asset" and allows the user to define what "operational risk" (asset value) is used as the threshold of "critical". Changing the operational risk threshold (say from the default of 2 up to 4) will limit the events that this rule will consider to those originating from assets with an asset value of 4 or greater (instead of > 2).

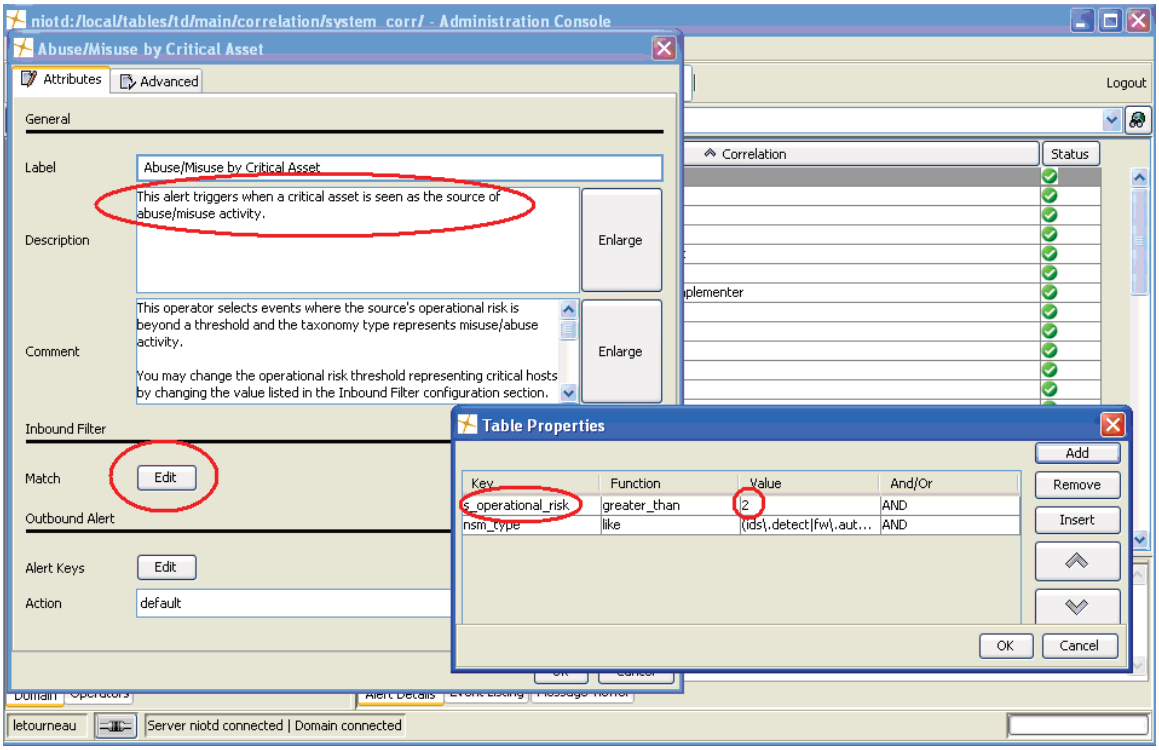

Figure 8: Escalation Rules

Escalation Rules

After an event is processed through the ISM correlation rules, the TD also has a set of "escalation rules" which allow events to be assessed against a set of criteria which determines if they are significant enough to escalate for further processing as a high priority alarm.

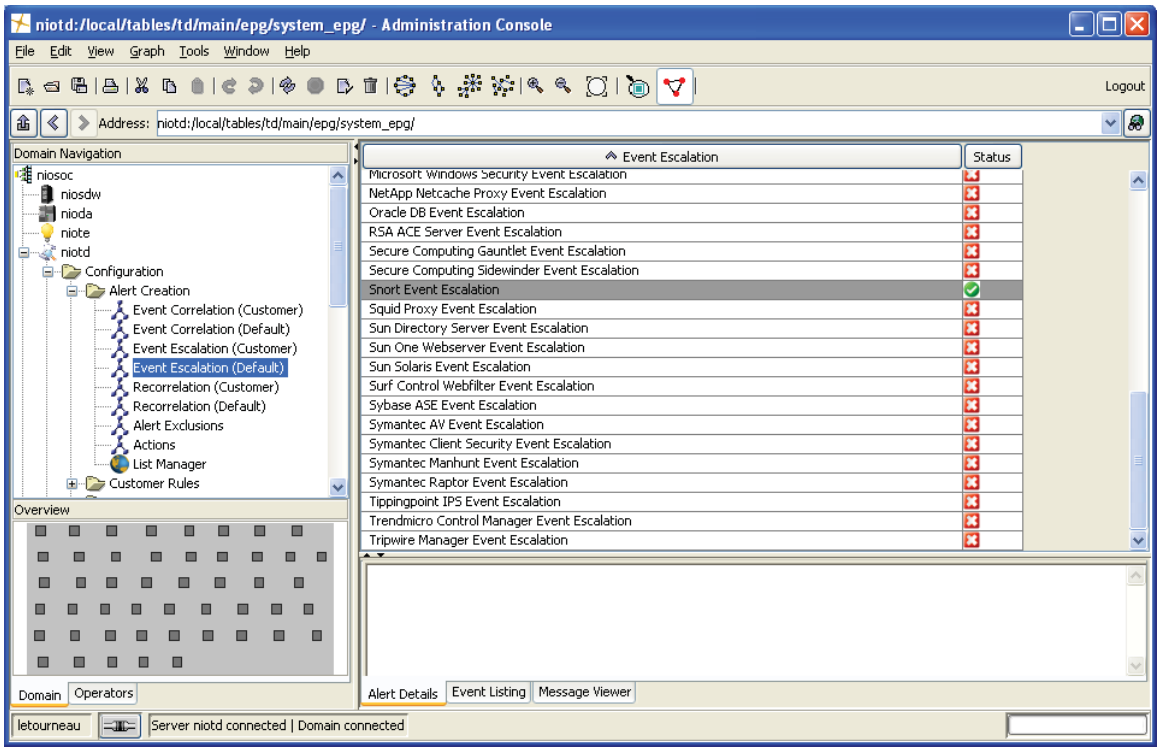

Figure 9: Escalation Threshold for Snort Alarm Priority

These escalations are also modifiable via a meta panel in a fashion similar to the correlation rules. This example shows that the user can modify the escalation threshold for Snort alarm priority.

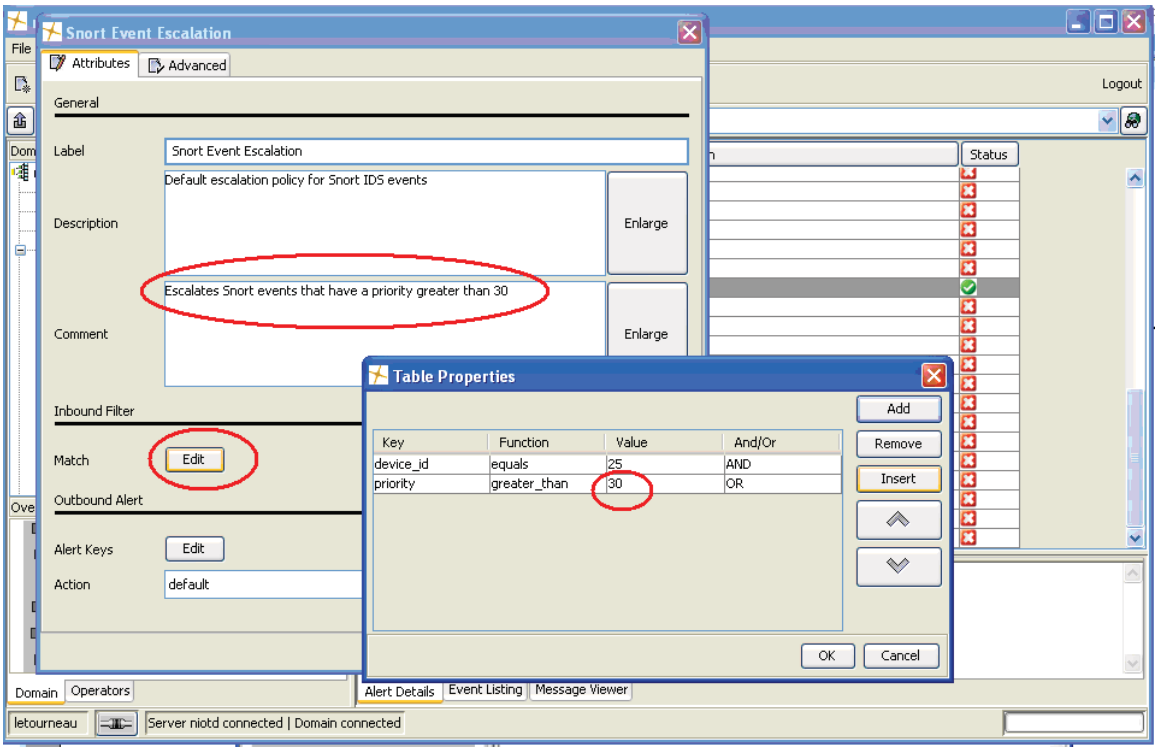

Figure 10: Recorrelation Rules

Recorrelation Rules

The ISM TD is also responsible for finding patterns (correlations) amongst the other high priority alarms (escalations) and correlated alarms previously seen by the system. Each correlated alarm is fed through "recorrelation rules" which weigh them in the context of the other alarms to determine if there is a larger pattern of malicious behaviour at work, such as a worm outbreak.

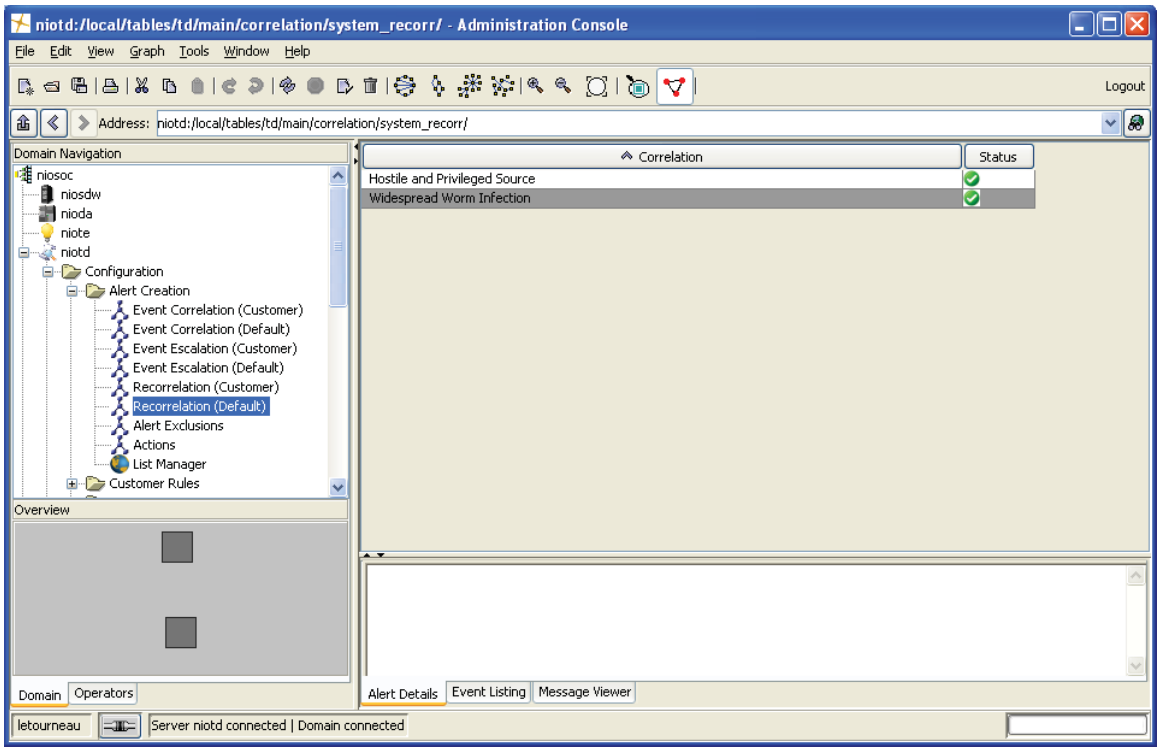

Figure 11: Meta Panel

The recorrelation rules are modifiable in the same fashion as other TD rules by using the meta panel. This example shows the rule used to detect worm-like behaviour and how the user can modify such parameters as the number of events, time window, and the priority of the generated correlated alarm.

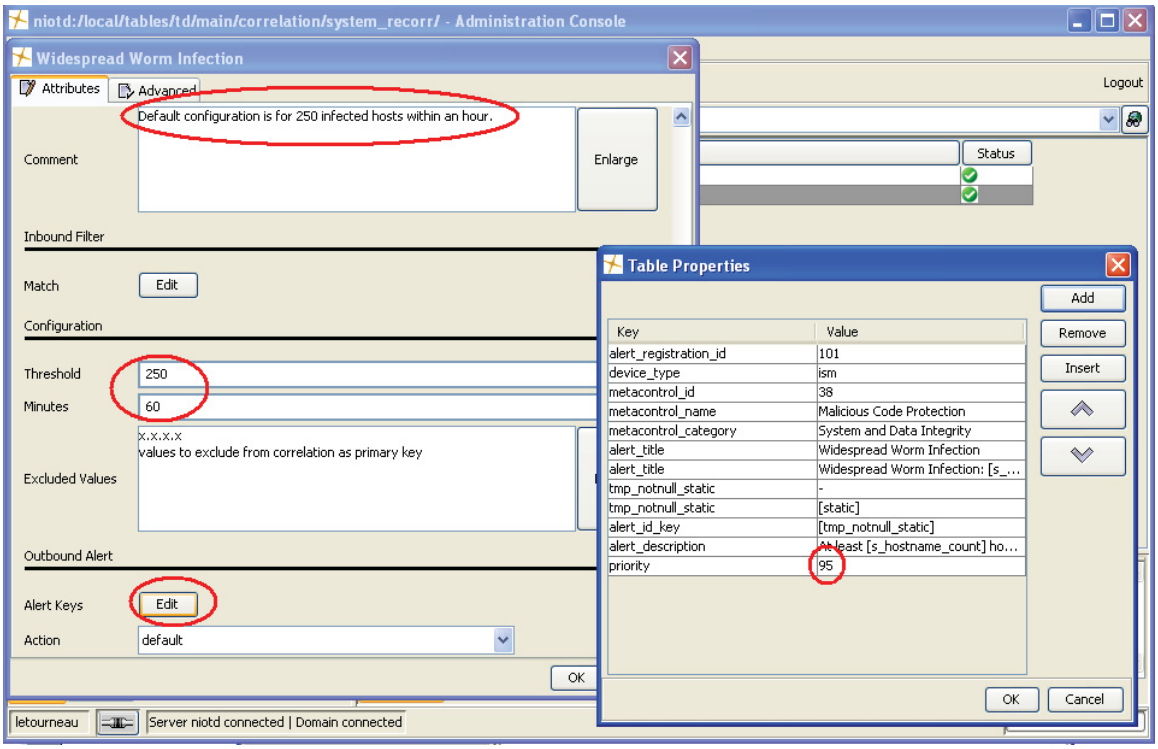

Figure 12: Risk Score

Risk Score

A key part of the ISM rules system is a "risk scoring" algorithm for each alert (correlated or individual). This risk score takes into account a number of historical and environmental factors in making the determination as to how important it is to the ISM user. In the ISM "Security Operations Center" (SOC) subsystem, the user can select any alarm and view the factors and their score contribution which determine the ISM risk score.

These factors are:

- Alert priority: a measure of how important this alarm type is relative only to other alarm types.
- Source and Target vulnerability: determined by using the quantity and severity of vulnerabilities on the source and target of the event (if known).
- Source and Target history: determined by assessing the history of events (known to the SIM) on both the source and target.
- Source and Target Compliance: a measure of how important the source and target systems are from a regulatory compliance perspective.
- Source and Target Operational value: a measure of how important the source and target systems are in terms of operational value (asset value).

The risk score is normalized to produce a value between 1 and 1000.

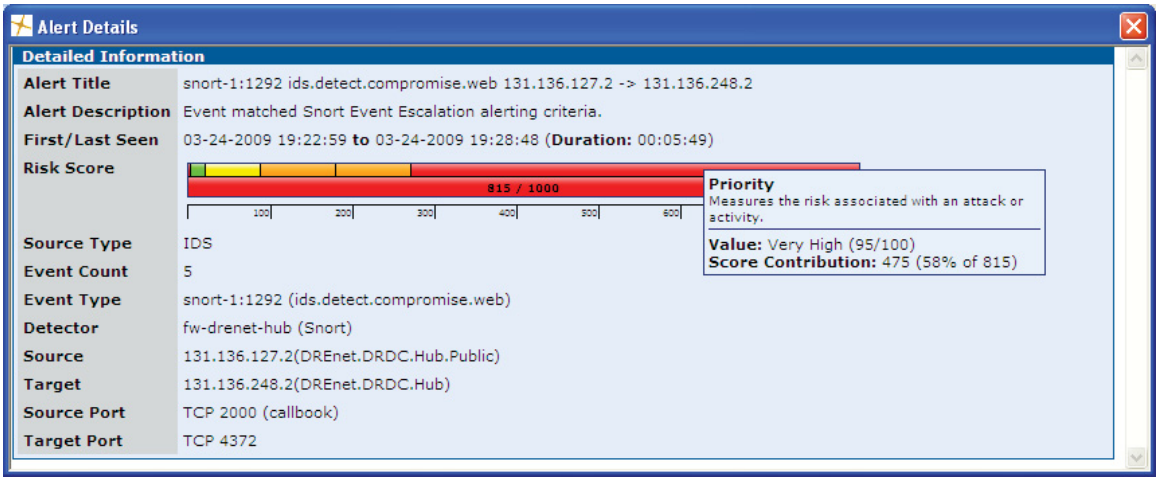

Figure 13: Alert Details

Users can modify the weight each of these factors has in the Risk Scoring formula; the meta panel is accessible through the "Risk Weights" bookmark on the ISM "Threat Evaluator" (TE) subsystem.

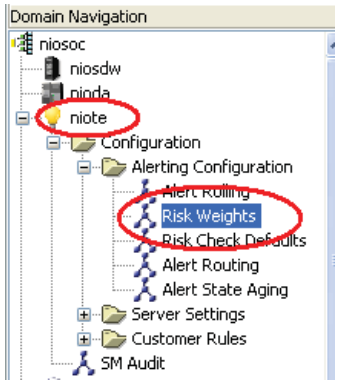

Figure 14: Access to Risk Weights

Each factor that contributes to the overall risk score can be assigned a weight value of between 0 and 10, which allows the user to bias the risk score toward those factors they consider most important in their environment. Each "weight" number becomes a multiplier for that factor in the overall risk score, which is then normalized to always produce a value between 0 and 1000.

This example in the DREnet context the assets have not been assigned a "regulatory compliance value", so these factors have been turned off in the Risk Scoring formula.

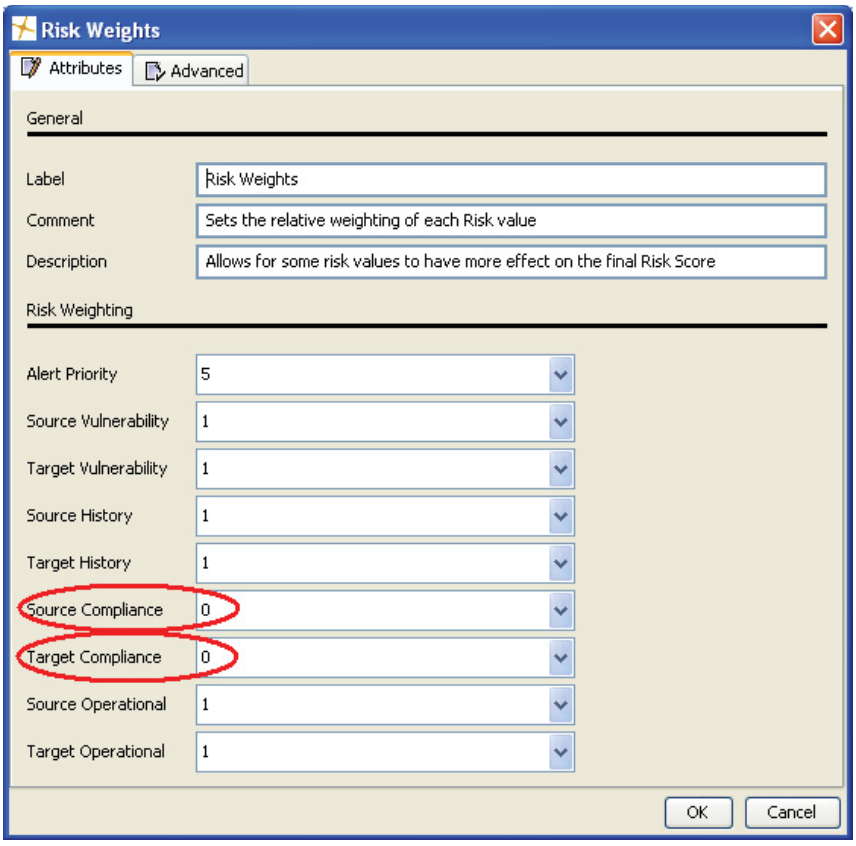

Figure 15: Risk Weights

A.5 SIM Presentation Layer

At the level of the ISM SOC, alarms that have a risk score exceeding a user defined threshold are presented to the user in the "Primary Alerts" view. These include correlated, escalated, or recorrelated alerts.

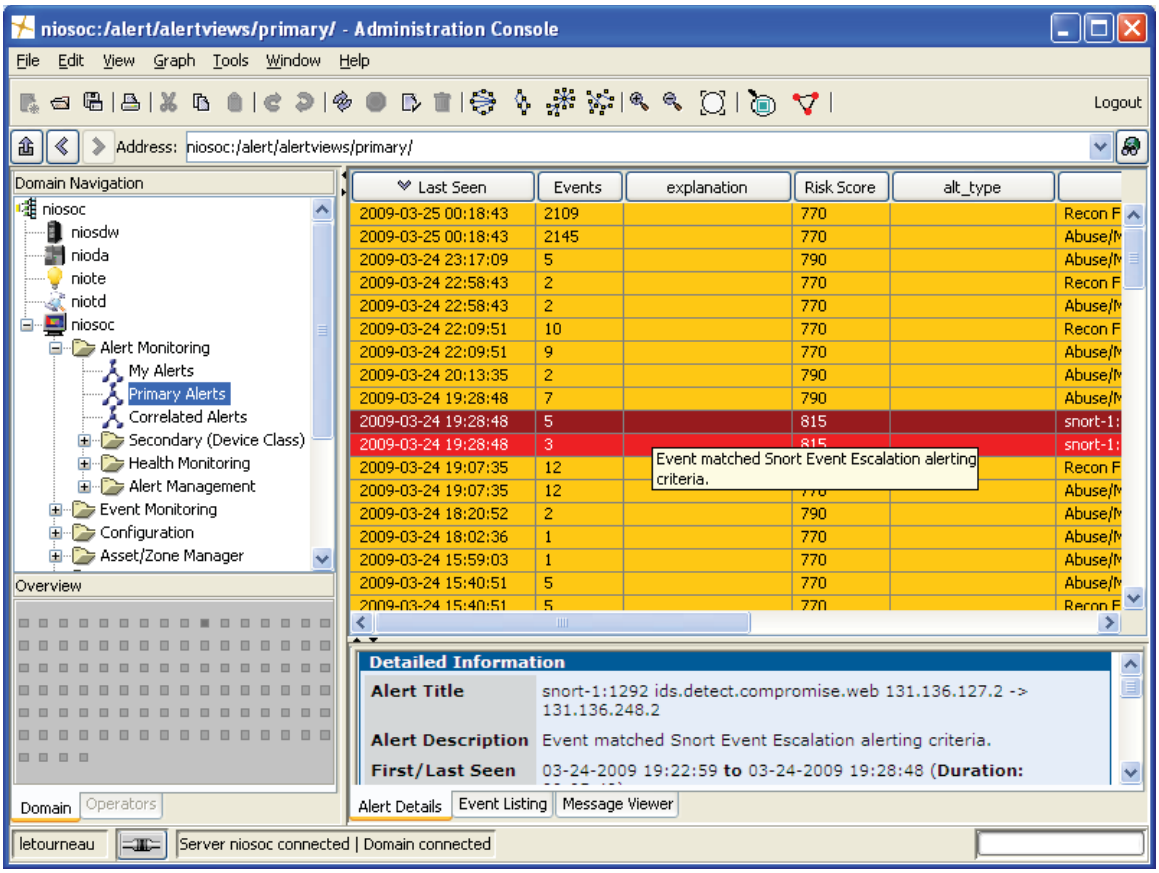

Figure 16: Primary Alerts View

User configurable parameters

The user can control what Risk Score threshold is used as the cut-off for inclusion in the Primary Alerts view. This also determines which alarms are escalated to JNDMS in the context of the DREnet deployment.

In this example we see that on the TE, the user can change the Primary Alerts threshold in a meta panel, accessed through the “Alert Routing” bookmark.

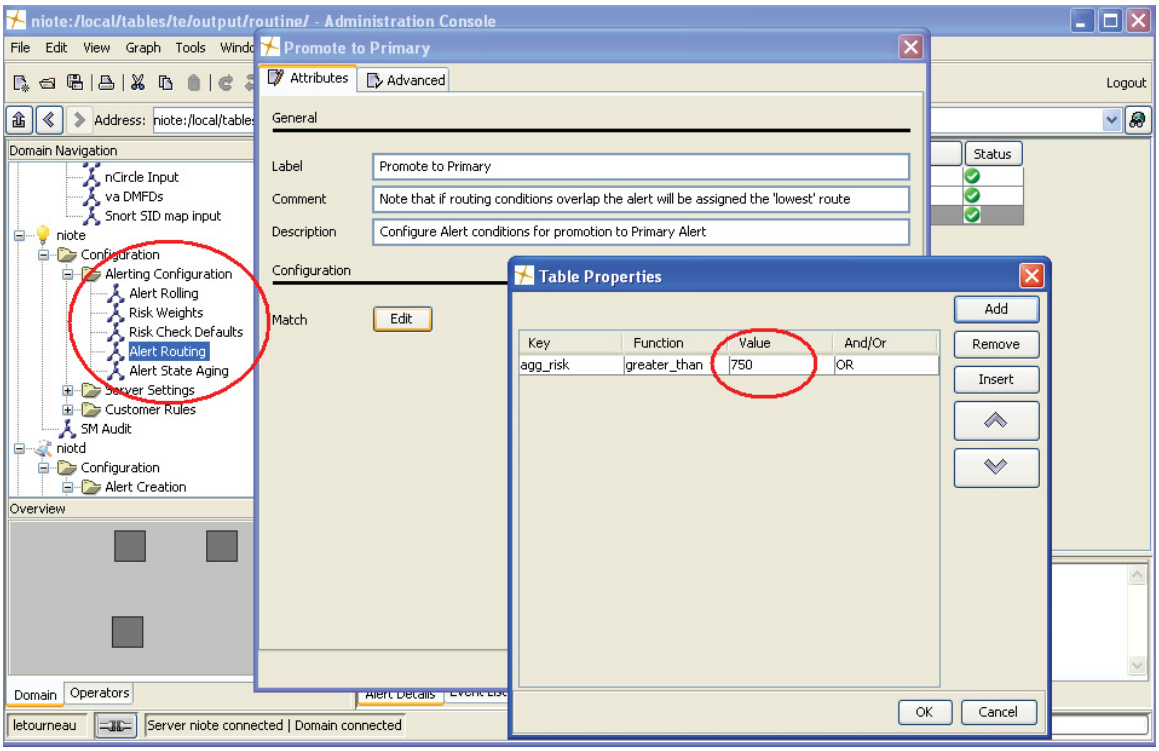

Figure 17: Control of Alarms

Additionally, the user can control how many alarms are held in the Primary Alerts view. This is accessed from the ISM SOC under the Primary Alerts view by right clicking on any alarm in the view and selecting “Preferences”.

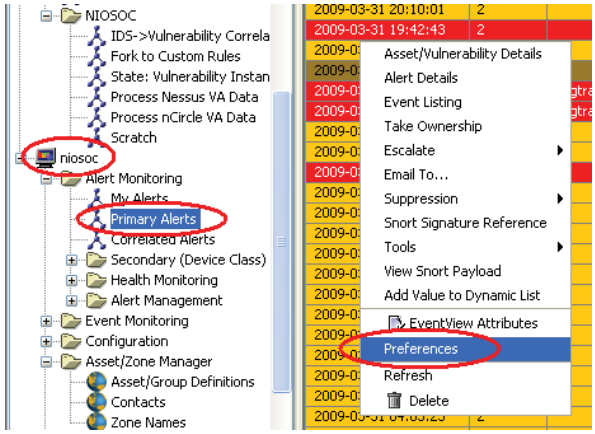

Figure 18: Preferences

The current setting in the JNDMS ISM retains up to 100 Primary Alerts at a given time. As the hundred and first event comes it, it will overwrite the oldest alert in the view, and so on.

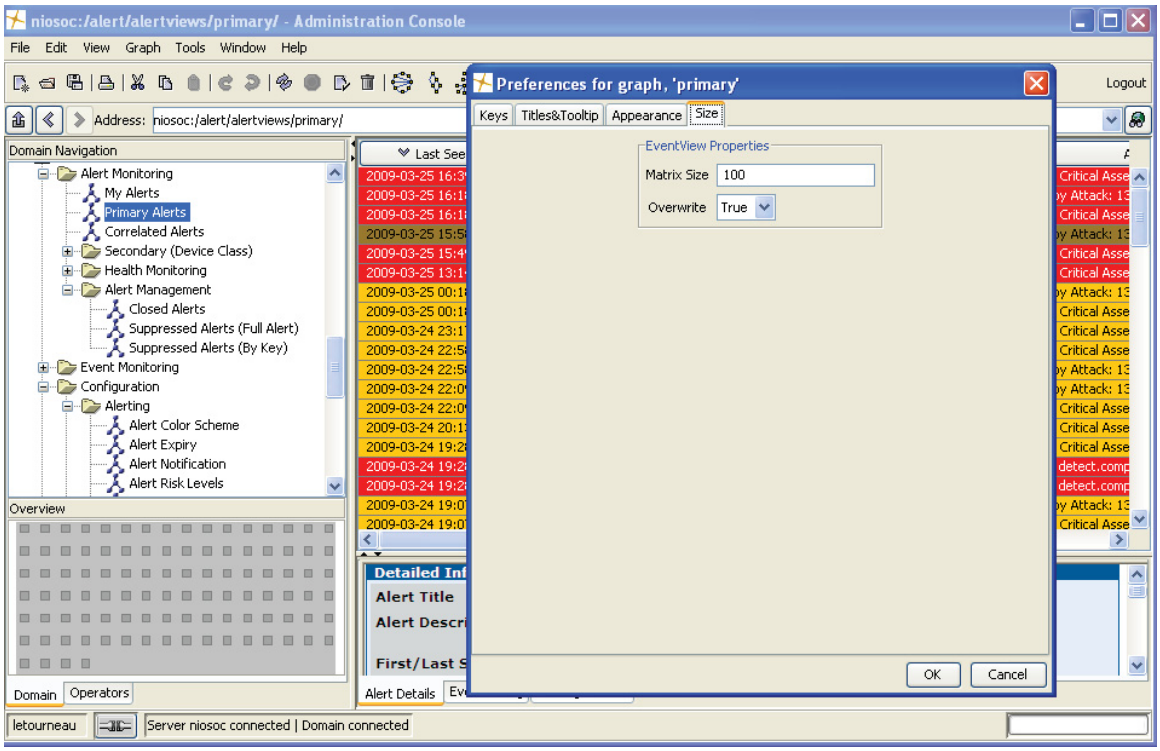

Figure 19: Preferences for Graph, 'primary'

A.6 Escalate SIM alarms to JNDMS

A timer process on the ISM SOC server iterates through the alarms in the “Primary Alerts” graph every 30 seconds and writes a copy of the alarms to a temporary directory.

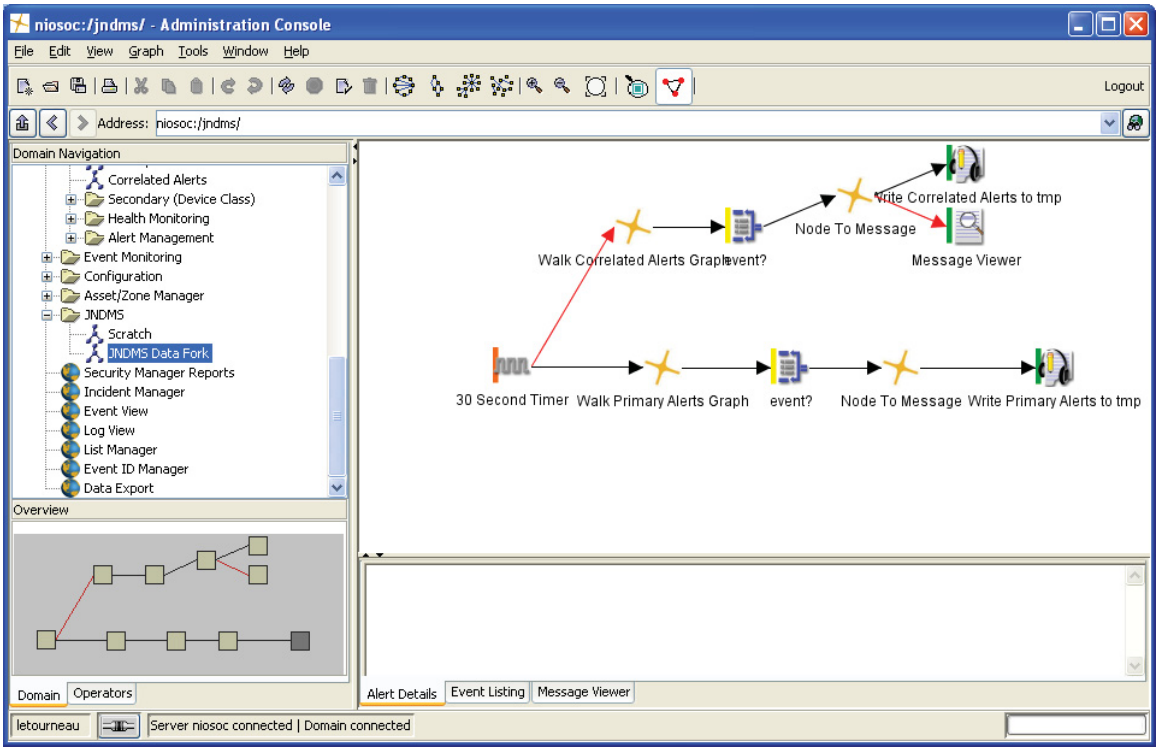

Figure 20: Primary Alerts Graph

A system daemon (/etc/init.d/jndms_sendalerts) watches the temporary directory and sends the alarms to the JSS. A data cleanup cron job periodically runs to clean out the temporary directory of all files older than 1 hour (to ensure that there is never an overwhelming backlog of events waiting for escalation to the JSS if it is offline for some time).

User configurable parameters

The data retention period and frequency of the data cleanup script can be modified as required.

A.7 Categorize alarms as Incidents or Events

The DSS map the SIM correlated alert and alarm types to JNDMS Incident Type using a pair user-definable properties files. These type mappings determine the JNDMS Incident type, and whether or not the alarm in question is an "event" (INCIDENT.INCIDENT=N) or an incident (INCIDENT.INCIDENT=Y) which is presented in the JNDMS portal.

User configurable parameters

There are two files that are user configurable at this step. The files are found in JSS\WebContent\WEB-INF and specify the mappings for correlated or single (high priority) alarms respectively. It is also worth noting that the JNDMS Incident Types themselves could potentially be modified, but this would require more research to understand the impact that those changes might have on the system.

The following file is used to map ISM "correlated alert" types (e.g. "Possible DDOS Target") to JNDMS Incident types (e.g. "Denial of service"). It is also used to specify if the alert type is considered an "Incident" in JNDMS terms or not (set by the true/false field). If a new ISM correlated alert type is passed to JNDMS for which a mapping does not exist, it is noted in the JSS log file on the JNDMS Portal system. If the file is modified, the JSS must be restarted for the changes to take effect.

correlation-properties.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="IDS Many Alerts Targeting Critical Asset">Malicious logic - worm,
true, TARGET, 1.0, 0.05, 0.2</entry>
<entry key="Possible DDOS Target">Denial of service, true, TARGET, 1.0, 0.05,
0.2</entry>
<entry key="Recon Followed by Attack">Reconnaissance, true, SOURCE, 1.0, 0.2,
0.05</entry>
<entry key="Restricted Source Port">Reconnaissance, false, NONE, 0.1, 0.1,
0.0</entry>
<entry key="Restricted Target">Reconnaissance, false, TARGET, 0.1, 0.3,
0.1</entry>
<entry key="Restricted Target Port">Reconnaissance, false, NONE, 0.1, 0.3,
0.1</entry>
<entry key="Abuse/Misuse by Critical Asset">Reconnaissance, true, SOURCE, 1.0,
0.2, 0.1</entry>
<entry key="Critical Asset Accessed Remotely">Reconnaissance, true, TARGET, 1.0,
0.1, 0.3</entry>
<entry key="IDS Alert to Vulnerability Match">Compromise, true, SOURCE, 1.0,
0.8, 0.8</entry>
<!--  Remove the following when corrected -->
<entry key="snort-1">Policy violation - other, true, NONE, 1.0, 0.8, 0.8</entry>

</properties>
```

The following file is used to map the ISM individual alarm "taxonomy types" to JNDMS Incident types. To accommodate the thousands of taxonomy types, the first three levels of the (hierarchical) taxonomy name for the alarm are used to match many related alarm types to the appropriate JNDMS Incident type (e.g. everything in the "ids.detect.exploit.*" hierarchy is mapped to "Malicious logic – other"). If the file is modified, the JSS must be restarted for the changes to take effect.

nsm-properties.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>NSM TYPE</comment>
<entry key="ids.detect.agent">Malicious logic - trojan horse</entry>
<entry key="ids.detect.anomaly">Malicious logic - other</entry>
<entry key="ids.detect.auth">Reconnaissance</entry>
<entry key="ids.detect.compromise">Compromise</entry>
<entry key="ids.detect.conf">Denial of service</entry>
<entry key="ids.detect.corrupt">Denial of service</entry>
<entry key="ids.detect.deliver">Malicious logic - worm</entry>
<entry key="ids.detect.disclose">Reconnaissance</entry>
<entry key="ids.detect.dos">Denial of service</entry>
<entry key="ids.detect.error">Policy violation - misconfiguration</entry>
<entry key="ids.detect.evade">Reconnaissance</entry>
<entry key="ids.detect.exploit">Malicious logic - other</entry>
<entry key="ids.detect.fw">Reconnaissance</entry>
<entry key="ids.detect.insecure">Policy violation - misconfiguration</entry>
<entry key="ids.detect.misuse">Policy violation - unauthorized use</entry>
<entry key="ids.detect.nocompromise">Reconnaissance</entry>
<entry key="ids.detect.recon">Reconnaissance</entry>
<entry key="ids.detect.request">Reconnaissance</entry>
<entry key="ids.detect.spoof">Reconnaissance</entry>
<entry key="ids.detect.svc">Reconnaissance</entry>
<entry key="ids.detect.throttle">Reconnaissance</entry>
</properties>
```

A.8 Repress Duplicate Incidents

The event count of how many security events a JNDMS Incident represents is available in the ISM Primary Alerts view, however this information is not held within JNDMS. After categorization the DSS refers to the Incident table; any alarm which represents an additional alarm with the same attributes and values as one that already exists in the Incident table is discarded, rather than creating a duplicate entry. For example to avoid multiple duplicate Incidents corresponding to a given correlated "port scan" alarm, each subsequent event belonging to the same port scan Incident is discarded by JNDMS (but still available in ISM).

There are no user configurable settings for this step.

References

[1] JNDMS Design Document, MDA Reference # DN0678 dated March 2006

[2] JNDMS User's Guide, MDA Reference # DN1009 dated September 2009

List of symbols/abbreviations/acronyms/initialisms

ACL	Access Control List
AJAX	Asynchronous JavaScript and XML
AM	Asset Management
API	Application Program Interface
BID	Bugtraq ID. This tracks vulnerabilities reported through the Bugtraq mailing list.
BPS	Boundary Protection System
BRE	Business Rules Expert
C2	Command and Control
C2IEDM	Command and Control Information Exchange Data Model
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CA	Computer Associates
CANUS	Canadian and US
CAP	Common Alerting Protocol
CAPI	Cryptographic Application Programming Interface
CDRL	Contract Data Requirements List
CFNOC	Canadian Forces Network Operations Centre
CIA	Confidentiality, Integrity and Availability
CIK	Crypto Ignition Key

CIRT	Computer Incident Response Team
CMDB	Configuration Management Database
CME	Common Malware Enumeration
CND	Computer Network Defense
CNES	Canadian Network Encryption System
CO	Commanding Officer
CONOPS	Concept of Operations
CoS	Class of Service
COTS	Commercial Off The Shelf
CSE	Communications Security Establishment
CVE	Common Vulnerability Exposures
CVSS	Common Vulnerability Scoring System
DHCP	Dynamic Host Configuration Protocol
DID	Data Item Description
DMF	Device Modeling Framework
DMFD	Device Modeling Framework Definition
DND	Department of National Defence
DRDC	Defence Research & Development Canada
DRDKIM	Director Research and Development Knowledge and Information Management

DREnet	Defence Research Establishment Network
DSS	Decision Support System. Part of JNDMS
DVPNI	Defence Virtual Privet Network Infrastructure
EAL	Evaluation Assurance Level. These levels are defined by the Common Criteria guidelines.
EIM	Enterprise Information Management. Part of JNDMS
ETL	Extract, Transform, Load
GIS	Geographic Information System
GUI	Graphical User Interface
GWT	Google Web Toolkit
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
I&A	Identification and Authentication
IAT	Impact Assessment Tool
IATF	Information Assurance Technical Framework
ICMP	Internet Control Message Protocol
IDE	Integrated Development Environment
IDS	Intrusion Detection Systems

INE	In-line Network Encryptor
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM	Intellitactics Security Manager
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
IT	Information Technology
ITI	Information Technology Infrastructure
J2EE	Java 2 Enterprise Edition
JAR	Java Archive. This is an archive file format defined by Java standards.
JDBC	Java Database Connectivity
JDW	JNDMS Data Warehouse
JNDMS	Joint Network and Defence Management System
JNDMS	Joint Network Defence and Management System
JSR	Java Specification Request
JSS	JNDMS System Services
JUI	JNDMS User Interface
KMI	Key Management Infrastructure
KML	Keyhole Markup Language - A GIS format defined by Google

LMP	Link Management Protocol
MARLANT	Maritime Forces Atlantic
MARPAC	Maritime Forces Pacific
MCOIN	Maritime Command Operation Information Network
MDB	Management Database. This refers to the datastore used by the CA products.
MTTRS	Mean Time To Restore Service
MUX	Multiplexer
NATO	North Atlantic Treaty Organization
NCC	Network Coordination Centre
NDHQ	National Defence Headquarters
NIAC	National Infrastructure Advisory Council
NIC	Network Interface Card
NIO	Network Information Operations
NIST	National Institute of Standards and Technology
NOC	Network Operations Centre
NSM	Network Systems Management. This is part of the Unicenter product line.
NTSM	National Telecommunication Management System
NVD	National Vulnerability Database
ODB	Operations Database

ODBC	Open Database Connectivity
OOB	Out Of Band
OODA	Observe, Orient, Decide, Act
OpenGIS	Open Geodata Interoperability Specification
OSVDB	Open Source Vulnerability Database
PKI	Public Key Infrastructure
POC	Point of Contact
PWGSC	Public Works and Government Service Canada
QoS	Quality of Service
R&D	Research & Development
RDBMS	Relational Database Management System
RDEP	Remote Data Exchange Protocol
RFC	Request For Comments (Internet Standards documents)
RFC	Request For Change. A formal request for change on a network within DND.
RSS	Real Simple Syndication
SA	Situational Awareness
SCC	Security Command Centre
SCEM	Secure Common Email
SCI	Special Compartmented Information

SCP	Secure CoPy
SDA	Service Delivery Area
SDNS	Secure Data Network System
SDP	Service Delivery Point
SDW	Security Data Warehouse
SIM	Security Information Management. Part of JNDMS
SIP	Service Interface Point
SML	Strength of Mechanisms Level
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SNI	Secure Network Infrastructure
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOC	Security Operations Centre
SOP	Standard Operating Procedure
SOW	Statement Of Work
SRA	Secure Remote Access
SSH	Secure Socket Shell
SSL	Secure Sockets Layer

TBD	To Be Determined
TCP	Transmission Control Protocol
TD	Technology Demonstrator
TDP	Technology Demonstration Project
TPOC	Technical Point Of Contact
TTP	Trusted Third Party
UDP	User Datagram Protocol
UPS	Uninterrupted Power Supply
VA	Vulnerability Assessment
VPN	Virtual Private Network
WAN	Wide Area Network
WAR	Web application Archive. A format defined by Java standards for deploying web applications.
WGS 84	World Geodetic System 1984
WSDP	Web Services Developer Pack
XML	eXtensible Markup Language
XSLT	extensible Stylesheet Language Transformations

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

MDA Systems Ltd.
Suite 60, 1000 Windmill Road
Dartmouth NS B3B 1L7

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON_CONTROLLED GOODS)
DMC A
REVIEW: GCEC JUNE 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

JNDMS Task Authorization 2 Report

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

MacDonald, S.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
October 2013	54	2

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
15BJ	W7714-040875/001/SV

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
	MDA Reference # DN1010, Issue 1/1

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This report covers the activities and results for Task Authorization #2 as part of the Joint Network Defence and Management System (JNDMS) Technology Demonstrator.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Computer Network Defence // Cyber Situational Awareness