



Project Remedies Inc.



The SARMM Solution: Situational Awareness, Risk Management and Mitigation System

An End-to-End Solution

**A White Paper from
Project Remedies Inc.
and ProInfo Inc.**

August 27, 2010

The SARMM Solution Situational Awareness, Risk Management and Mitigation System (SARMM)

The Problems in Managing Cyber Security and Operations

Opportunities for intrusion have expanded greatly. Networks have experienced tremendous growth and they continue to expand. Wireless usage continues to increase. Operating systems and applications are becoming ever more sophisticated and more complex, thus more vulnerable to attack. Those who would do us harm are ever more empowered and have new technologies available to them. As a result, thousands of events, including emergent vulnerabilities, cyber recon, and intrusions, occur on our networks hourly.

These events are becoming more numerous and complex, and the remediation is becoming harder to manage. The “white noise” needs to be eliminated in order to focus on the most serious issues. Often, the speed of the response is too slow, the quality of the response is insufficient, and the resources required to work the remediation efforts are sparse, geographically dispersed, and busy working on other things. Few tools for managing mitigation and remediation efforts are available. Cyber security is almost always reactive and not proactive, and thus more expensive than it should be.

Several systemic issues further obscure the picture:

- Typically no real-time Common Operating Picture (COP) is available for either a) the operational status of the network(s) or b) remediation efforts, either in progress or under consideration.
- No real-time COP is available that updates the operational status of the network with indications of the remediation efforts in progress or recently completed.

Cyber Risk and Remediation Management

One of the key challenges in Cyber Security Management is determining both specific and overall risk. This often lags behind other efforts because the required risk profiles have not been done or formalized.

Managing risk mitigation and remediation efforts is difficult. There are multiple types of concurrent efforts, and they are not managed together or centrally. Understanding the risk, the scope of probability, and the impact of an event or vulnerability needs to be balanced against the cost of response and the availability of resources. Real-time project and resource status visibility is needed to achieve this, but resource management, i.e., knowing what each person is working on, is not managed well. Data is spread over multiple monitoring systems, applications, organizations, and locations, and data used for planning is often out of date.

Resource availability is a key issue. If people are taken off their current projects and tasks and put on something new, what is the impact of that change in direction?

The Two-COP Model

Let's start with a definition. A common operating picture is not simply a list of problems or a punch list of things to be done or being done. A common operating picture is a single, consistent display of the relevant status information of an organization or a specific environment. For example, if you were the President of a large corporation with numerous business units, a profit and loss statement for each business unit would provide you with consistent information for determining the health of each organization within the corporation. A common operating picture promotes coordinated planning and helps to achieve situational awareness.

In the area of Cyber Security Operations, a Common Operating Picture (COP) shows the status, relationships, and direction of threats and remediation efforts under way. Two COPs are needed to achieve optimum situational awareness:

- The *Operations and Vulnerabilities Common Operating Picture (OV-COP)* gives you a consistent way to view the status of each network or organization and its relative current and potential vulnerabilities.
- The *Remediation Common Operating Picture (R-COP)* gives the status of all work currently underway to mitigate or remediate problems: active projects, projects going through a proposed-project stage-gate approval process, and maintenance tasks.

The separation of the data in two COPs makes the management of risk, risk mitigation, and remediation easier and more complete, thereby preventing data overload. Each provides visibility into one side of "situational awareness." Together they provide the real-time picture required for an effective response.

SARMM is the Cyber Security Management Solution: One System / Two Views

SARMM, the Situational Awareness, Risk Management and Mitigation System, synergistically combines technologies from two companies, making the sum greater than the parts. It is a game-changer.

Cauldron™ from ProInfo Inc. allows the aggregation of risk and system data from different network monitoring tools and applications, aggregates and then correlates the data, and provides a better visualization of the data so that you can better calibrate a response. This better visualization helps eliminate white noise and predict vulnerabilities in the network. Cauldron provides the Operational and Vulnerabilities Common Operating Picture (OV-COP).

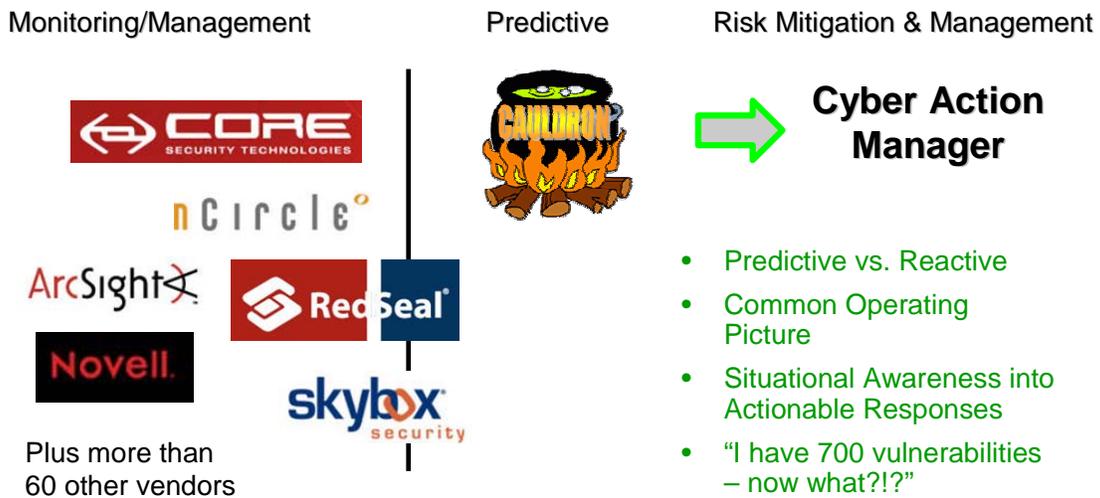
Cyber Action Manager™ (CAM) from Project Remedies Inc. is a BMC Remedy Action Request System-based application, which leverages your investment in Remedy. CAM takes risk and system data feeds from Cauldron and from other sources including monitoring tools such as HBSS and ArcSight, maintenance requirements and tasks, and incident reports. The CAM workflow functionality plus the robust CAM project template functionality automatically enables real-time generation, categorization, and weighting of importance for active projects, proposed projects, and maintenance tasks. People working the projects can be notified automatically. Resource availability and conflicts can be quickly checked and resolved. Asset information in the BMC Remedy Asset Management System can be updated automatically.

Data on incidents, vulnerabilities, and projects from the fused Cauldron and CAM tools can all be integrated into CAM. Then, using CAM's project portfolio view, management can see the current status of ALL mitigation and remediation efforts in real-time: active projects, proposed projects, and cyber events, all in one place. This is the Remediation Common Operating Picture (R-COP).

The Three Tiers To Cyber Security

Network Monitoring and Management make up the 1st tier of cyber security and the bulk of current approaches. Cauldron takes data from up to 60 different Network Monitoring capabilities and integrates their data into a Common Operating Picture (COP). Cauldron also adds a predictive component and creates a 2nd tier of cyber security. The SARMM approach adds the 3rd tier of integrated risk mitigation and remediation, providing proactive and rapid reaction remediation of system vulnerabilities.

Three Tiers to Cyber Security



Where Decisions Meet Budget and Resource Constraints

The Command Cyber Readiness Inspection

When the inspectors visit a Command for a Command Cyber Readiness Inspection, one area of questions they have involves vulnerabilities. Cauldron provides them with a better understanding of the issues in the environments being inspected. Cauldron takes feeds from multiple systems, correlates and aggregates the data, and prepares a better way for the network administrator and his / her management to see their environment. With this better view, they can calibrate their picture and see potential vulnerabilities that they had not seen before. Similarly, this gives management at a higher level

organization a consistent way to better understand each environment. Figure 1 is an example of this Operational and Vulnerabilities Common Operating Picture (OV-COP). From this picture, we can see from an entry point (the green icon) to the destination (the red icon) all of the combined vulnerabilities which are bi-directional yet displayed on a node to node basis. Every single vulnerability can be remediated. Using Cauldron, you can understand vulnerabilities in context.

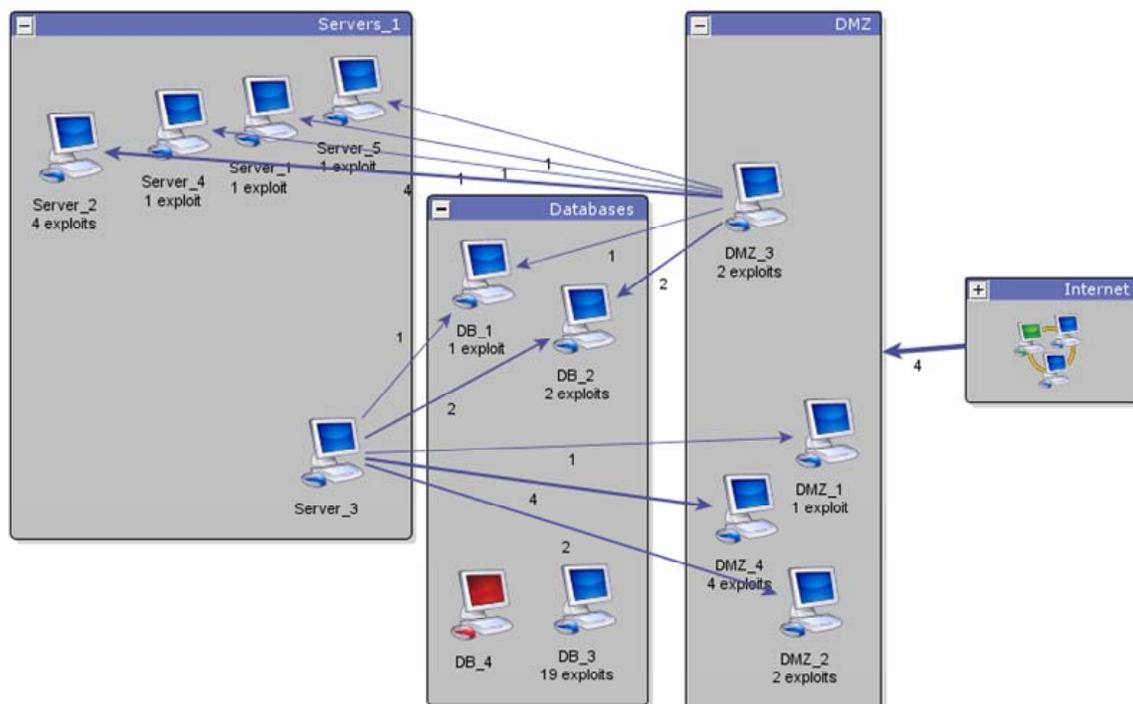


Figure 1 – Operations / Vulnerabilities Common Operating Picture

The New Daily Briefing

This Remediation Common Operating Picture (RCOP) can also be used for a Command Cyber Readiness Inspection as well as for your daily briefing. It gives you real-time access to all of this information, allowing you to better respond to requests from senior leadership. In fact, senior leadership will be able to look for themselves at the status of each effort any time they choose.

Each project and task is current up to the last entry. This means that the 7:30AM daily briefing can be done with a workstation and a projector looking at the real data. The need for the preparation of PowerPoint slides is eliminated. This also means that the data is more current. If someone comes in at 4:30AM to prepare the PowerPoint slides for the 7:30AM meeting, the events that occur during that 3 hours are not included in the slides. By 7:30AM, the data is up to 3 hours old, and in the world of cyber security, that is simply not acceptable.

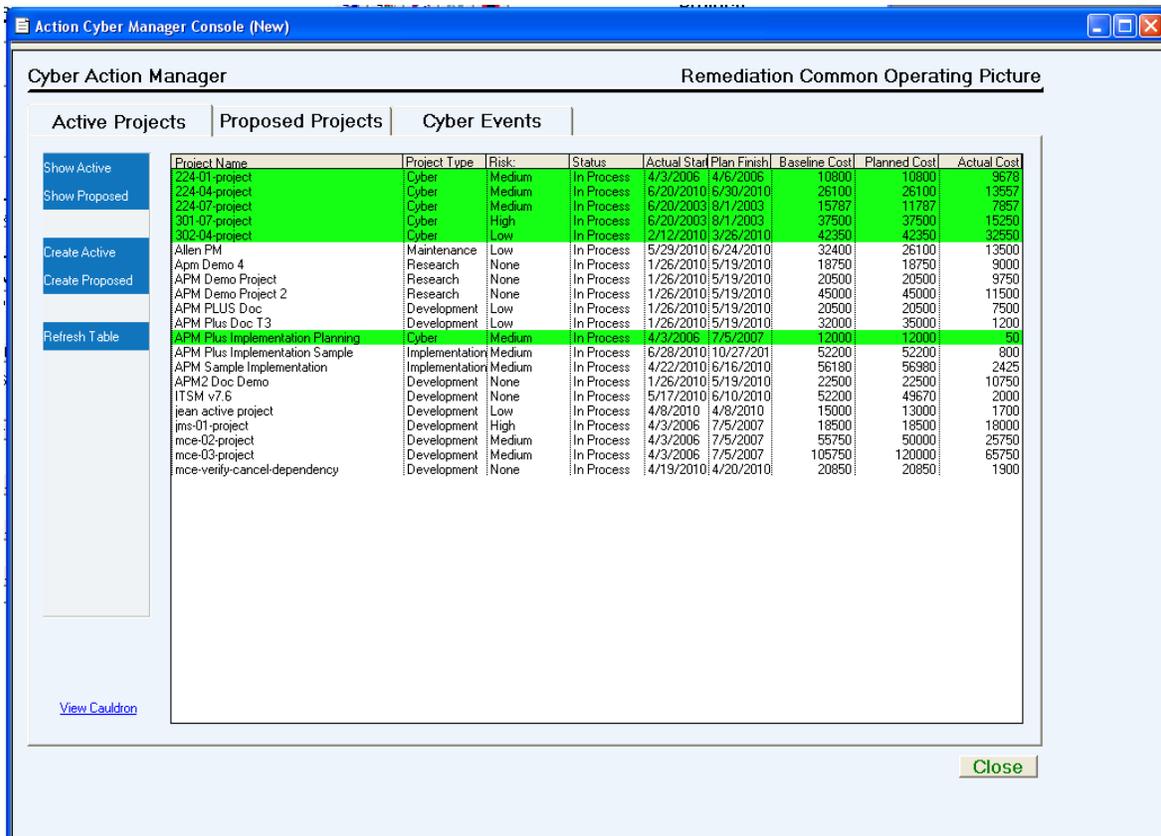


Figure 2 - CAM Remediation Common Operating Picture

Using the CAM Remediation Common Operating Picture shows you all projects, including cyber projects, in play. Double-clicking on a project opens the project record. Two more clicks bring you to the task detail. Click on the Gantt chart button to see a Gantt chart for the project. Click on another button and see a “Pool” Gantt Chart (Figure 3). A “pool” is a group of projects.

Coordination changes can be made on the fly, literally during briefings, making the briefing more useful, providing accurate and up to date situational awareness to Senior Leadership. Notifications and policy changes can go out directly from the briefing to remote staff and the help desk.

When thinking about a Command Cyber Readiness Inspection, another area that the inspectors will ask about is “how are you managing your remediation efforts?” Would it not be great if the team being inspected could pull up the CAM Remediation Common Operating Picture and say: “We are managing our remediation efforts like this. Click on this tab and you see each project in process. Double click on a highlighted project and it brings up the project record. Click on the Gantt chart button to see a Gantt chart of the project. Two more clicks and you can see the task detail, and the data is all current up to the last entry. Click on the next tab for Proposed Projects and the third tab for Cyber Events. That’s the way we are managing our remediation efforts.”

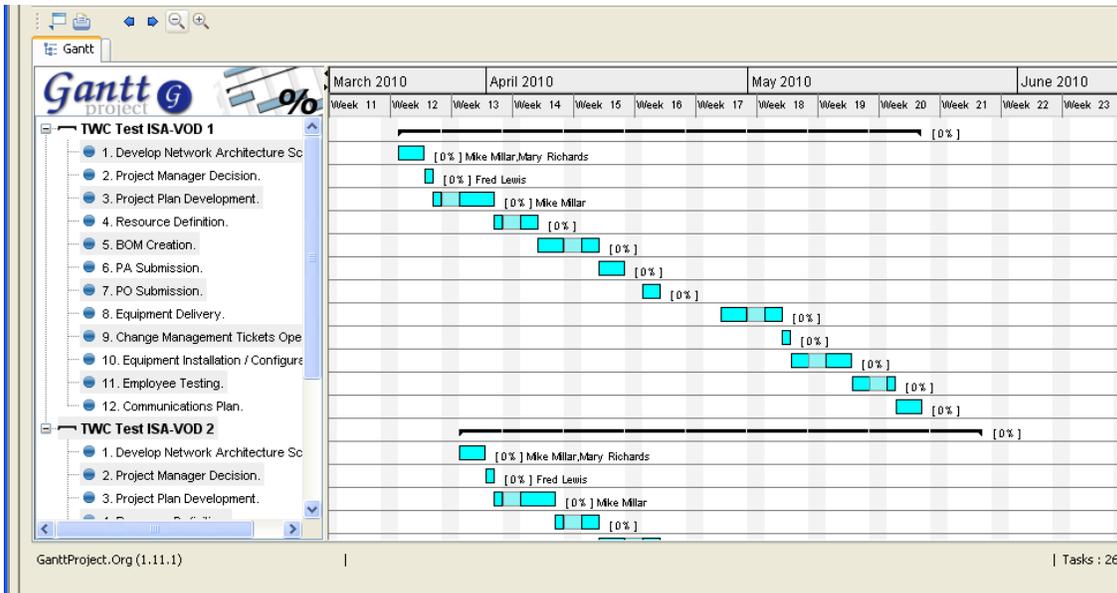


Figure 3 – CAM Pool Gantt Chart

CAM Helps Use Limited Resources More Effectively

Cyber Action Manager includes robust resource management functionality. Our Resource Management Chart (see figure 4) shows how busy people are, and to what projects and tasks they are committed to, up to the last entry. In the world of cyber security, having this information available at your fingertips is critical and ensures the proper resource response at the proper time.

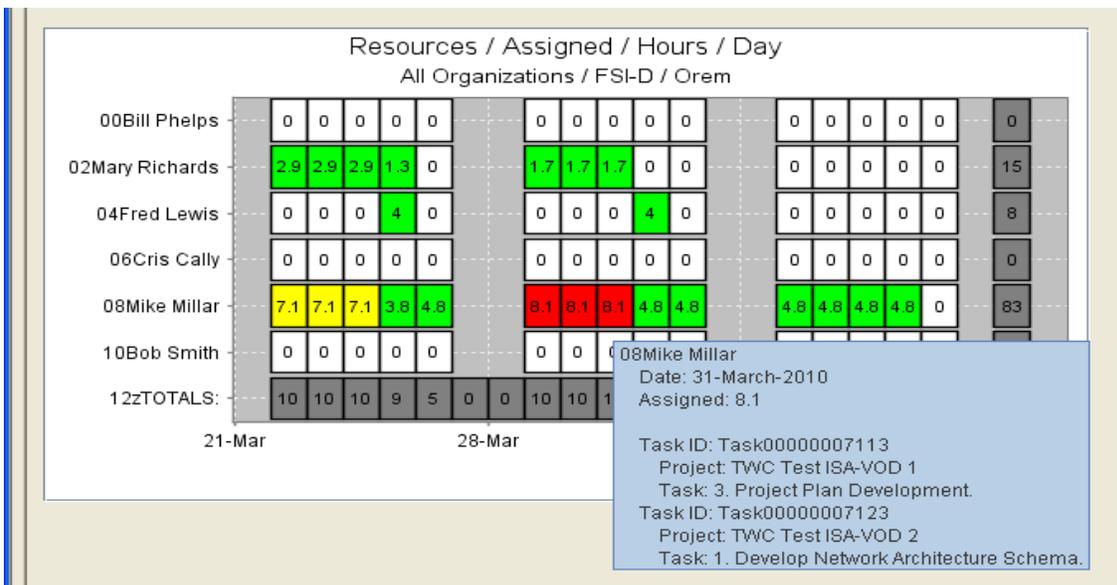


Figure 4 - CAM Resource Inventory Detail

The Unique and Critical Extra Step

Additional synergy is created when mitigation or remediation efforts are underway, because there is a link back from Cyber Action Manager to Cauldron and its OV-COP,

providing visibility into remediation efforts already in process and their current status. The OV-COP then has situational awareness regarding the remediation.

The Game Changer: From Reactive to Proactive

The operational tempo in cyber security is close to that of daily combat. Knowing where your adversaries are going to strike changes the battle rhythm. Similarly, the SARMM-fused toolset opens the opportunity for rapid response and preventive mitigation vs. responding after the fact to the latest crisis. What changes everything is Cauldron's ability to identify vulnerabilities, weight them, and integrate "proactive mitigation" into the R-COP before the vulnerabilities can be used by adversaries for intrusion.

R-COP increases the speed of mitigation and remediation by cueing and weighting all events, including high impact events and predicted vulnerabilities, into a flexible portfolio. Again, the game-changer is moving cyber security operations from resource intensive remediation after an intrusion, to the more cost-effective security shield and mitigation to prevent intrusion.

Whether the response is the mitigation of a vulnerability or the remediation of an intrusion, Cyber Action Manager (CAM) uses adaptive project templates that can accommodate either very simple assignments or very complex, multi-phase, multi-member projects. CAM can be set to notify staff automatically of assignments and follow up if the work does not start on time. It provides a way for the remediation staff to update the status of their projects in the R-COP and thus the OV-COP, providing near real-time situational awareness of mitigation and remediation efforts.

The SARMM Risk Mitigation End-to-End Life Cycle.

This is an end-to-end, enterprise-wide solution. As described in the diagram in Figure 5 below, Cauldron takes events from network management systems and other systems and does several things with them. An Operational and Vulnerabilities Common Operating Picture is developed and the events are categorized. With this information, the "white noise" is eliminated and management can focus on the events that need remediation.

Cauldron will aggregate and normalize varied data inputs for different aspects of the security structure (i.e., scan files and firewall configuration files), normalize the data, and correlate the data against known vulnerabilities. Cauldron then allows for "what if" modeling so the analyst can make decisions about remediation needs based upon situational awareness. By creating synergies between varied data sets, Cauldron will calculate the impact of a change before the change is made. The data synergies allow for all stakeholders in the security organization to understand the impact of change from a common point of view. Cauldron will then visualize the topology of the vulnerabilities, allowing for the views of only critical vulnerabilities if required, but overall providing for a flexible review/analysis of the overall security profile from a variety of perspectives.

The SARMM Risk Mitigation Life Cycle

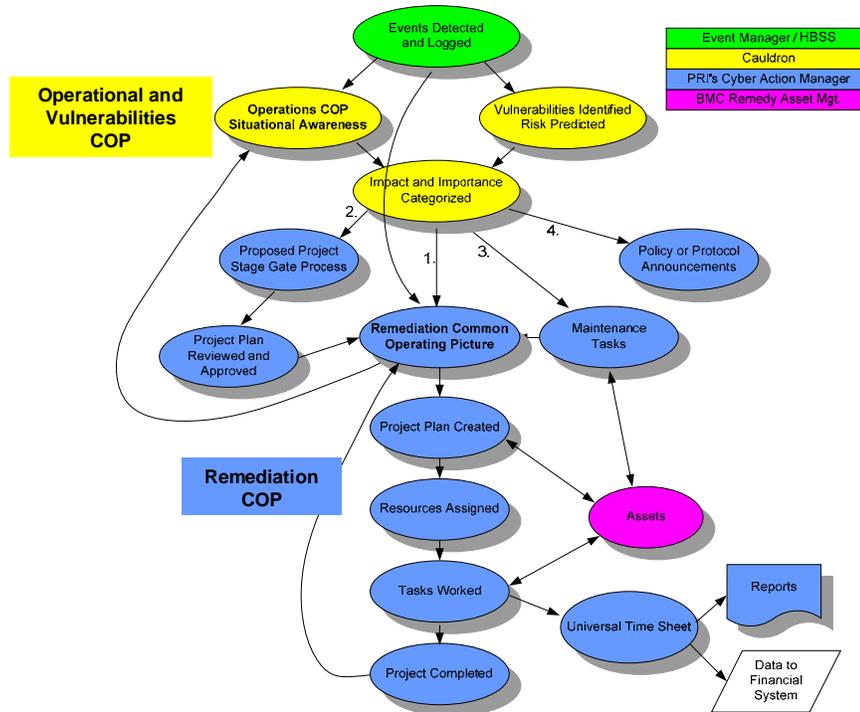


Figure 5 - The SARMM Risk Mitigation Life Cycle

Cyber Action Manager allows you to launch, track, and manage various remediation efforts, depending on the categorization of the event.

- If the event is absolutely critical and remediation response obvious, a project is launched automatically (using Remedy Action Request System workflow functionality) from HBSS or an Event Management System at network speed. The person managing the project and the people working the tasks are notified immediately, in real time.
- If the event is less critical and you want to evaluate the impact and the risks involved with responding or not responding and balance this against the cost and availability of resources to respond, the network administrator using Cauldron can click on a button and Cyber Action Manager will automatically create a proposed project. This takes you through several steps (which are managed with templates) to describe the event, the risks and issues involved, the resources needed, the cost of responding, and the priority of this particular project. It then goes through a stage-gate approval process, and provides the decision-making board with all of the information needed to determine whether or not a response should be made.
- If management wants to create a project, that's the third way to do it.
- With events that require a simpler response, maintenance tasks can be automatically or manually generated.
- Events that require policy or protocol announcements also generate tasks, and the people responsible are automatically notified.

When projects and tasks are launched in Cyber Action Manager, the project status data is linked back to the Operations and Vulnerabilities Common Operating Picture in Cauldron. This means that when you are looking at the O-V COP in Cauldron, you can see which assets have remediation efforts already in process. This is a major capability that makes managing your networks and other assets much easier to do.

SARMM: The Holistic and Strategic Cyber Solution

SARMM helps with the development of cyber strategy, resource planning, and budgeting. The archived data provides detailed data about past threats, and also the patterns of emerging threats, chronic areas of vulnerability, and likely levels of future threat. This allows for data-driven technical and architectural threat analysis and planning. This allows Cyber Strategy Planning to identify the kinds of technologies needed to keep the system secure and the architectural modifications needed to evolve cyber security ahead of evolving adversaries.

Staff Resource Planning can be performed more realistically with real data on actual mitigation and remediation performance and time frames, actual resource utilization, and actual costs for mitigation and remediation. SARMM answers the questions: Are new hires needed, or can we better use the current staff? Are there chronic vulnerabilities in our architecture? What if we made this or that change, what is the impact?

When it comes to managing the scale and complexity of the cyber response, the Situational Awareness, Risk Management and Mitigation System (SARMM) provides a holistic cyber solution suite to meet and mitigate the proliferation of cyber threats, vulnerabilities, and intrusions.

For more information about SARMM, please contact:

Stan Feinstein, President of Project Remedies Inc. at 310-230-1722 or stanf@projectremedies.com.

John Williams, President of ProInfo Inc. at 301-237-0007 or johnrw@proinfomd.com.