

# A SOC in the NOC: A Vision for Security Operations Management

Track: Security in NMCI

Information and network security has become a *pain*. At first it was painful to our users due to the roadblocks that security placed in the path of productivity. Security was more concerned about preventing behavior rather than enabling productivity in a manner appropriate to the enterprise. It was common to rely on gates, guns and guards types of technologies to provide a “prevent and monitor” network security.

We’ve learned that architected and engineered properly, information and network security can enable our users to work in a safe environment. But security is still a pain. Identity management, access management, and threat management tools all combine to provide a user with appropriate rights to perform for an enterprise while preventing much of the undesirable behavior that can damage it. The trade off between blocking and monitoring technologies and enabling technologies has become the administration workload that an enterprise assumes.

In general, security tools were developed to perform specific functions and were rarely integrated. The enterprise needs a range of skill sets and bandwidth to manage the devices, hardware and software that comprise their security solution. Each product that we place in our enterprise adds to the amount of data that has to be processed and understood to analyze a security event. The real pain in security is in integrating our various security tasks so that we maintain real time or near real time situational awareness of the health of the network security.

## Wha’ Happen???: Situational Awareness

Very simply, it is easy to lose the bubble during a security event (or incident). There are tools in our security toolbox, such as intrusion detection systems, that are to alert us to a security incident. It is supposed to determine the method of attack, provide some automated response and help with information to counter the attack. The problem is that it is a single point of failure with its own strengths and weaknesses. Quite often, it isn’t until long after an event until information from various sources can be analyzed into a somewhat coherent picture. This does not provide us with a good picture of what is happening NOW in our enterprise. It doesn’t contribute to situational awareness and therefore doesn’t enable a real time or near real time proportionate or effective response to an incident. The lack of situational awareness also represents an opportunity for an attacker to create diversions to press home the true attack. The information is available; it just isn’t correlated, analyzed and reported in a manner meaningful to an operator.

## Sneaky stuff: Taxonomy of a security event

A security event isn’t just seen at a security monitoring device. It is seen across many devices, including routers, firewalls, switches, servers, etc. Situational awareness can be gained by being able to collect from all the sources of information, normalize the data being collected, correlate the normalized data with data from other sources, analyze the correlated

data to gain information and finally report the findings in a manner useful to an operator. Although malicious or inappropriate activity can be seen on a network, real situational awareness does not begin until the disparate sources of information can be melded together in real time or near real time to allow an appropriate response.

### **It Doesn't Need to be so Hard: Elements of a Security Management system**

One answer to the problem of situational awareness in the security context is to provide a management interface that can be used in a Security Operations Center (SOC) or even better, a Network Operations Center (NOC). Locating a SOC in a NOC proves beneficial due to the ability to gain assistance from other networking professionals that deal with equipment and software that is not security related and could be used to respond to an attack. Within this SOC, the interface would have to be distributable, so that operators have at their fingertips only the information they need and the remediation tools within their skill set. The solution should be extensible and open to take advantage of published standards and to allow connection with virtually any security or network device. The solution should be easily customizable via a web interface to allow the generation of graphics and tables that have meaning to an operator and that allow the operator to gain a quick grasp of the situation. The interface should have a high degree of usability to allow operators to switch between screens and perform tasks efficiently. Lastly, the system should be flexible in its alarming so that operators do not have to be tied to a fixed geographic location.

In battle, just as in any complex undertaking, the person with firm situational awareness has the best chance in winning. A well designed SOC in a NOC could help.