CONF-961092--5 SAND96-0468C
SAND--96-0468C

Operational Tips for Improving Intrusion Detection System Performance

Douglas G. Adams
Sandia National Laboratories
Security Technology Department
Albuquerque, NM 87185-0780

Abstract -- The installation of a new intrusion detection system (IDS) is, of course, expected to improve site security. However, depending upon the way the system is used, it can, over time, actually degrade security. Proper use, control, and maintenance of the IDS is critical if site security is to be maintained. This paper discusses several operational issues that should be addressed in order to use an IDS effectively. Several anecdotes from the author's experience are given to illustrate proper and improper use of an IDS. Improper operational use of an IDS can render it ineffective. Applying these tips can help keep the IDS operating at peak performance.

Background

Over the last ten years the Security Technology Department at Sandia National Laboratories has been involved in the design, installation and evaluation of intrusion detection systems. These systems, often called "annunciators", are used to display and control exterior and interior intrusion detection sensors.
In many instances we have observed operational practices which make the annunciator ineffective, and sometimes useless. This paper is organized as a set of tips, with anecdotes describing how to, and how not to operate an annunciator.

You paid good money for that system, Use it!

Don't ignore alarms.

The purpose of an IDS is to detect and communicate intrusion events to an operator. It is important not to ignore the alarm information which is communicated. This may seem like common sense, but complacent operators have been known to ignore alarms because "they were busy doing something else." Many times a poorly maintained system has a high nuisance alarm rate. These false alarms tend to reduce operator confidence in any alarm; therefore, alarms get ignored.

At one site, it was noticed that the IDS indicated an event (by beeping) for every alarm and for successful processing through an entry control portal. Of course, the entry control information was unimportant since it was a successful entry. The operators started to ignore the alarm signals. Worse, they started deleting system alarms without looking at the display. Intrusion alarms were deleted along with the rest of the events. A knowledgeable intruder could use such information to penetrate the site. Moral: Don't ignore alarms.

Don't abuse sensor access.

One way to reduce false alarms from authorized entries is to place sensors into access. Access means the system ignores alarm information from a sensor. This concept is useful in interior applications. Many times a room is occupied during the

day, but is vacated at night. Intrusion sensors are on-line at night but accessed during working hours. This reduces false alarms during the day.

Watch out. Don't abuse sensor access. Having the system ignore an alarm is as bad as the operator ignoring it. Operators can, and do, access entire buildings, perimeters, and sites. Accessing a sensor reduces the false alarm rate to zero; it also reduces the detection probability to zero.

Leave the system powered on.

On one training trip, we noticed the security system was turned off. The screens were dark. No alarms. Upon inquiring why the system was off, it was explained that the system was down until all operators had taken refresher training. Even though the system worked and site personnel could operate the equipment, the system was turned off. An annunciator cannot do its job, if it is turned off.

Security Officers should know and understand the system

Training must be continuous.

One of the secrets of maintaining an effective IDS is training. Continuous training must be a mandatory part of an IDS operator's job. Part of the training schedule should be testing exercises which simulate real world intrusions. Exercises help keep IDS operators alert and provide a mechanism for personnel performance.

Understand what the system does and how it works.

This tip is obvious. Operators are most effective when they understand what the system is telling them, and how that information is generated. Theory of operation should be included in any training course.

On-the-job training ain't enough.

On a visit to upgrade an IDS, a new security operator asked, "what does this yellow color, on the screen, mean?" No one had explained to the operator that yellow indicated an alarm was in access. Accessed sensors do not report alarms. Half of his perimeter was in access, and he was unaware of the condition. Training is imperative.

Security Officers should keep physical control of the system.

Limit access to authorized operators.

The only people that should operate the IDS are authorized operators. Visitor and other unauthorized personnel, most likely, are not trained to properly operate the system. More important, unauthorized personnel may be a security risk.

Casual visitors should not even see the system.

Lock that annunciator away. Casual visitors should never see the IDS console. Much can be learned about the physical security layout and guard force procedures by observing the IDS.

Two anecdotes illustrate these tips. One site had the IDS console located near a visitor waiting area. Glass walls separated the waiting room from the annunciator control room. All activity on the IDS and guard responses to alarm activity could be observed. Anyone could obtain access to the waiting area and could remain unchallenged for up to thirty minutes. Meanwhile details of site security could be observed and recorded.

At another site it was common for non-security site personnel to operate the system. A physical plant technician was observed accessing over half the perimeter security sensors. We determined that he was going to work on some equipment in one area of the perimeter, and accessed the extra sensors "just in case" he needed to move someplace else. System operators were unaware of his actions. A better procedure would have been to request one perimeter zone be accessed, security officers posted at that sector, and then work begun. Subsequent zones could have been turned off (upon request) as needed. Non-security personnel must not have access to the system.

Maintenance personnel must be trusted and have the proper security clearances.

Maintenance of an annunciator is necessary but risky. Maintenance technicians have complete access to the IDS. The greatest risk is that configuration files could be changed without security approval. Such changes could render the IDS ineffective, creating security "holes" in the sensor system. Maintenance personnel must have clearances equivalent to those of the IDS operators. In addition, all physical access to the annunciator must be supervised by security officers. Maintenance technicians must not make unauthorized changes to the annunciator.

Keep system running at peak performance.

Maintenance personnel should also get refresher training.

Most maintenance problems are not caused by malicious intent. Problems are created by technician inexperience or mistakes. IDS service personnel must be adequately trained in system maintenance. It is also imperative that refresher training be continuous for repair persons. It is helpful to put repair technicians through the same IDS training provided security officers. Additional training on maintenance procedures can be added as necessary.

Run a regular schedule of preventive maintenance.

It is better to be proactive rather than reactive. Preventive maintenance helps eliminate system down-time by avoiding common faults. On a repair trip to a site, we observed extremely harsh conditions on the perimeter. High temperatures, blowing dust, and excessive temperature swings from day to night constantly stressed perimeter security electronics. It was common to see a fine coating of conductive dust covering every surface, including those surfaces inside sealed (supposedly) enclosures.

In this case, the maintenance team was prepared. A regular program of preventive maintenance was in place. All IDS equipment was inspected and vacuumed once a month. The IDS electronics were in excellent condition. Equipment enclosures were spotlessly clean. The repair team was proactive in keeping their site operational.

Conclusions

In this paper we presented several tips for improving annunciator performance. In summary, here are the tips:

⇒ Don't ignore alarms.

⇒ Don't abuse sensor access.

⇒ Leave the system on.

⇒ Perform continuous training.

⇒ Run tests (exercises).

⇒ Understand what the system does.

⇒ Understand how to operate the IDS.

⇒ On-the-job training ain't enough.

⇒ Limit access to authorized operators.

⇒ Casual visitors should not see the system.

⇒ Maintenance personnel must be trusted.

⇒ Maintenance personnel should also get refresher training.

⇒ Run a regular schedule of preventive maintenance.

Training, proper use, and restricted access are key to operating an IDS effectively. Care should be taken to weigh operational issues with the level of security you wish to achieve at a given site.

Acknowledgments

This work was sponsored by the US Department of Energy under contract DE-AC04-94AL85000.