

Mission Control Network Intrusion Detection System

How can I protect the assets of my company by identifying attacks before they damage and disrupt business operations?

To efficiently protect your confidential data, business infrastructure and your good reputation you need to know who is the internal or external enemy.

The five key criteria

To detect and prevent global intrusions and security breaches a Network Intrusion Detection System must fulfill the following five key criteria:

- 1 Comprehensive: Capture the risk-relevant data of all locations and activities.**
- 2 Anytime: Scan the network continuously for intrusions and extrusions – 24x7, 365 days a year.**
- 3 Significant: Use multi-level analysis and inspection methods, including human expert rating provided by security engineers.**
- 4 Integrated: Activate appropriate escalation process to prevent dangerous attacks.**
- 5 Auditable: Document the relevant events in a transparent and reportable way.**

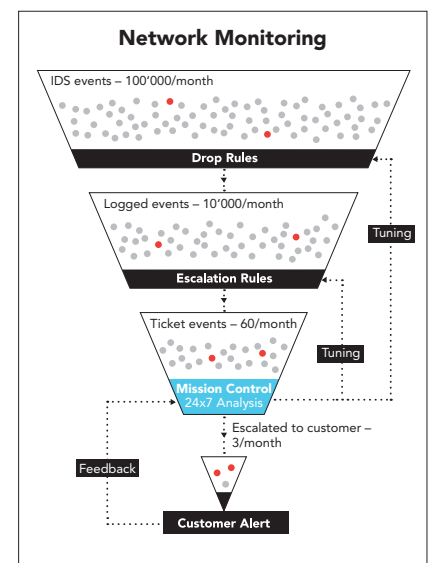
Maximum significance and improved security

You already developed and implemented a security policy. Despite your investments in a reliable defense infrastructure, you do not feel completely in control of identifying intrusions and extrusions in your global network before they damage and disrupt your business operations.

Network Intrusion Detection Systems (NIDS) represent an important building block of any robust defense infrastructure. Unfortunately, all too often Intrusion Detection Systems belie their expectations: to alert key personnel if there is a security breach. The reason lies in the huge number of false alarms, which prevent operations from extracting the essential events.

So the question is: What does it take to make a Network Intrusion Detection System more efficient and effective in protecting the assets of your company?

Mission Control Network Intrusion Detection System meets the five NIDS key criteria and improves the precision of alarms by using multi-level analysis and inspection methods, including human expert rating provided by security engineers as well as a feedback loop implemented in the detection and notification framework.



Due to this unique multilayer event processing including prompt human expert ratings and feedback mechanisms, alerts generated with Mission Control Network Intrusion Detection System have maximum significance, guaranteeing improved security with reduced management and operation overhead. Around the clock. 365 days a year. Worldwide.



mission control™
security services

Now is the time to get serious about IT security.



Renowned financial institutions, multinational industrial companies and internationally respected NGOs rely on Mission Control Security Services from Open Systems AG to secure their ICT infrastructure and protect their assets. In over 175 countries worldwide. Around the clock. 365 days a year.

Open Systems AG
Räffelstrasse 29
8045 Zurich
t +41 58 100 10 10
f +41 58 100 10 11
www.open.ch