



Comprehensive security shield

Mission Control Application Gateway, Mission Control Firewall, Mission Control Internet Proxy, Mission Control Security Gateway, Mission Control Passport, **Mission Control Intrusion Detection**, Mission Control Email Shield, Mission Control Virus Protection, Mission Control Client VPN, Mission Control Wireless Zone Protector



Mission Control Network Intrusion Detection Datasheet Description

Comprehensive protection of an organization's information network is a core requirement. Policy enforcement points at the perimeter of the infrastructure network mitigate the risk of known attacks. However, due to previously unknown breaches, the threat level increases constantly. Therefore, **Network Intrusion Detection Systems (NIDS)** represent an important building block of any sound defense infrastructure. Unfortunately, all too often these vital elements belie their expectations: to alert key personnel in case of a successful security breach. The reason lies in the huge number of false alarms preventing operations from extracting the essential events. Therefore, the challenge lies in being able to differentiate between an attempted and a successful attack.

Unique Event Processing

The Mission Control Network Intrusion Detection improves the precision by using a **combination of protocol, signature and anomaly based inspection** methods to analyze network traffic and prevent critical threats from affecting the network. Whether deployed at the perimeter, in the DMZ, or in critical network segments, it helps to protect business continuity, company assets, and brand reputation around the clock by identifying attacks before they damage and disrupt business operations.

Due to the unique multilayer event processing including classifications done on the centralized database as well as human expert rating provided by the Mission Control Operations Centers, generated alerts have maximum significance guaranteeing improved security with reduced management and operation overhead.

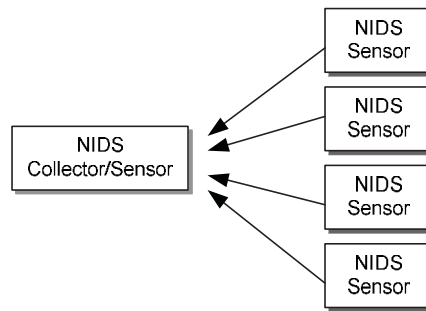
Operational facts

The Mission Control Network Intrusion Detection is running on **dedicated, industrial strength hardware** for reliable 7x24h operation. The **hardened operating system** assures that only essential tools and utilities are activated and therefore cannot lead to unexpected instability and compromised systems.

After extensive testing procedures, all required security updates and patches are installed, ensuring that the systems are always up-to-date. The device is capable of **booting multiple releases** which provides an efficient fallback and recovery process if required. Furthermore, all device and environment specific configurations are automatically generated, based on the **Mission Control configuration database**. This is an essential part of an **efficient disaster recovery** process since it allows for the instantiation of a replacement configuration in a very short time.

Architecture

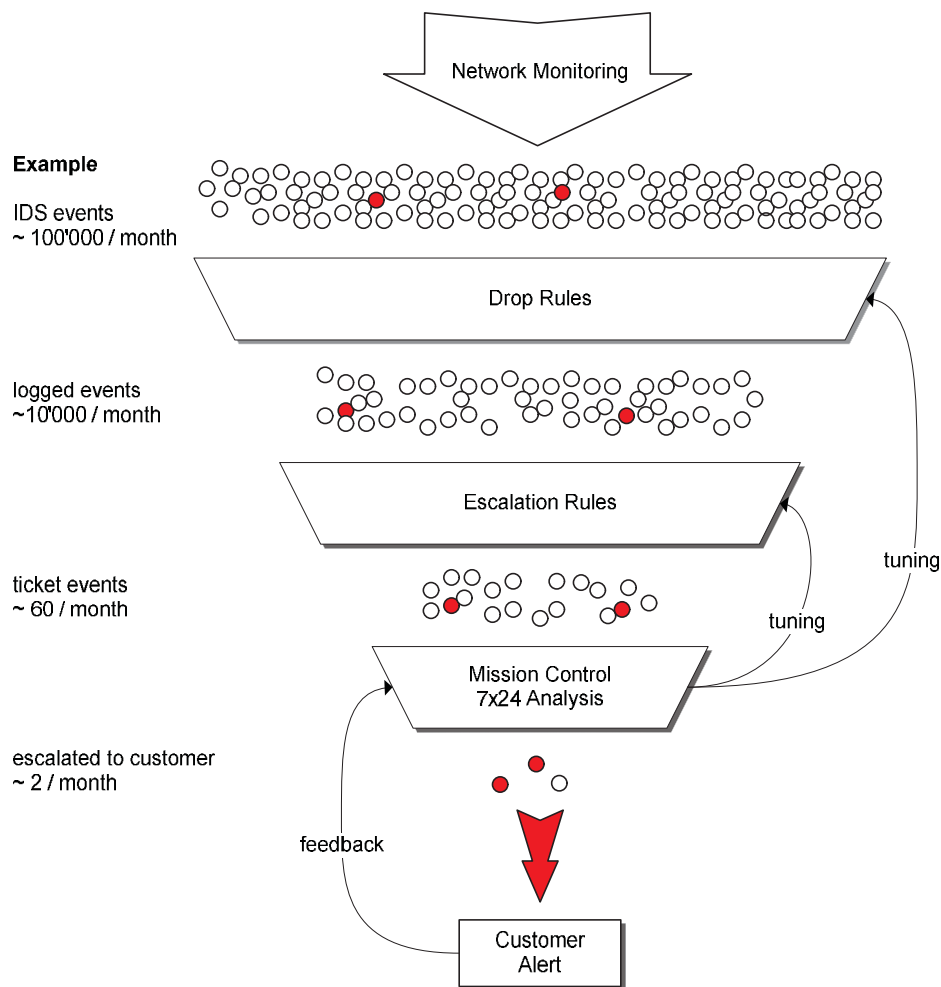
The Mission Control Network Intrusion Detection consists of three main components. The **Sensors** are directly attached to the protected networks, capture the entire traffic and generate sensor messages. The **Correlator** records all those messages in the database and applies an elaborate rule set in order to generate alerts. The alerts are finally sent to the **Mission Control experts** where they are again rated and attributed to the proper context. Such events are documented in the Mission Control ticketing system and followed by the escalation process if required. Mission Control also **correlates all alerts from all global locations** and is therefore able to identify global attacks and attack campaigns.



The sensors are **updated daily** based on **multiple signature sources** to be constantly up to date and to base the analysis on the knowledge of multiple signature sources as well as Mission Control. Besides the imported signatures, the Mission Control NIDS is extended by **customized detection patterns** which are extracted constantly from the Mission Control worldwide NIDS installation basis. This synergy effect allows Mission Control to further improve the detection rate and eradicate false alerts for every single system. Mission Control engineers analyze the pool of events generated by the engine and perform differentiation between imprecise, uninteresting, suspicious, and confirmed messages. Interesting cases are communicated to the customer for further classification.

The used escalation engine makes use of **Extrusion Detection** which is a mechanism to avoid false positives and unsuccessful attacks. By being able to differentiate the direction of traffic into incoming, outgoing, and internal, the generated signatures can be attributed a higher relevance. Extrusion Detection is the result of research work done in cooperation with the Swiss Federal Institute of Technology (ETH Zurich).

An important building block of the reliability and relevance of a Network Intrusion Detection System is the **feedback loop** consisting of customer feedback implemented in the detection and notification framework. The Mission Control NIDS is adjusted not only based on inputs generated by the Mission Control operations centers, but also based on direct input from the customer base. The Mission Control NIDS is therefore capable of representing individual infrastructure constellations.



High performance engine

A single Correlator can handle a number of Sensors distributed globally. These Sensors report only relevant information back to the Correlator where event storage and interaction with Mission Control is done. This saves a considerable amount of bandwidth as the intelligence to implement the global policy is distributed to all Sensors.

Through the use of **traffic partitioning**, customers may split the load to multiple Sensor instances (across multiple cores or even multiple machines). This unique technique makes the Mission Control Network Intrusion Detection System scalable and accept load which would exceed the limits of a single system.

Auditability with Mission Control

All relevant information including alerts, notifications, changes, reports, and monitoring is provided in a single, administrator and management friendly interface called the Mission Control Cockpit. The Mission Control Cockpit is a very powerful and feature-rich interface (available through HTTPS and strong authentication from all around the world) supporting different users associated to different roles (access levels) with all the information they require.

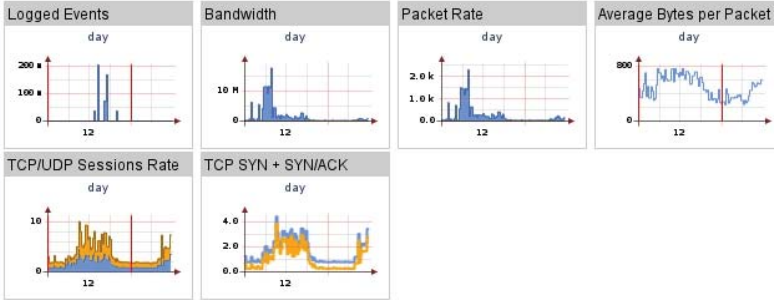
The Mission Control Cockpit provides **all operational facts and figures** of Mission Control Intrusion Detection including the number of logged events, bandwidth usage, packet rates, the number of TCP sessions, TCP/UDP session rates, and the difference between SYN and SYN/ACK packets. All these statistics are scalable for a day, month, and year period to get a very quick and precise overview of the current status.

Escalations and notifications are based on strictly defined processes including active notifications via SMS, Email or Fax.

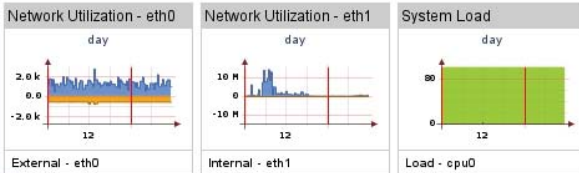
Services > Intrusion Detection NG nikita > Statistics

Status **Statistics** Configuration Tools

Network Intrusion Detection



System



[Connection Monitoring](#)

Host Information

 **nikita**

Network Interfaces

| | |
|----------|---------------------|
| eth0 (m) | 213.156.231.10 / 24 |
| eth1 | 0.0.0.0 / 0 |

[notifications >](#) [data sheet >](#)

Time Zones

| Mission Control | Zurich | Your Time |
|---|---|---|
|  |  |  |
| 11:51 (UTC+1) | 11:51 (UTC+1) | 11:52 (UTC+1) |

Location



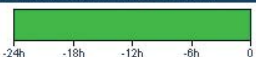
Address

Räffelstrasse 29
8045 Zurich Switzerland 

Geo Info

Lat. 47 ° 21 ' 45.03 N Long. 8 ° 30 ' 39.91 E

Connection Monitoring (last 24h)



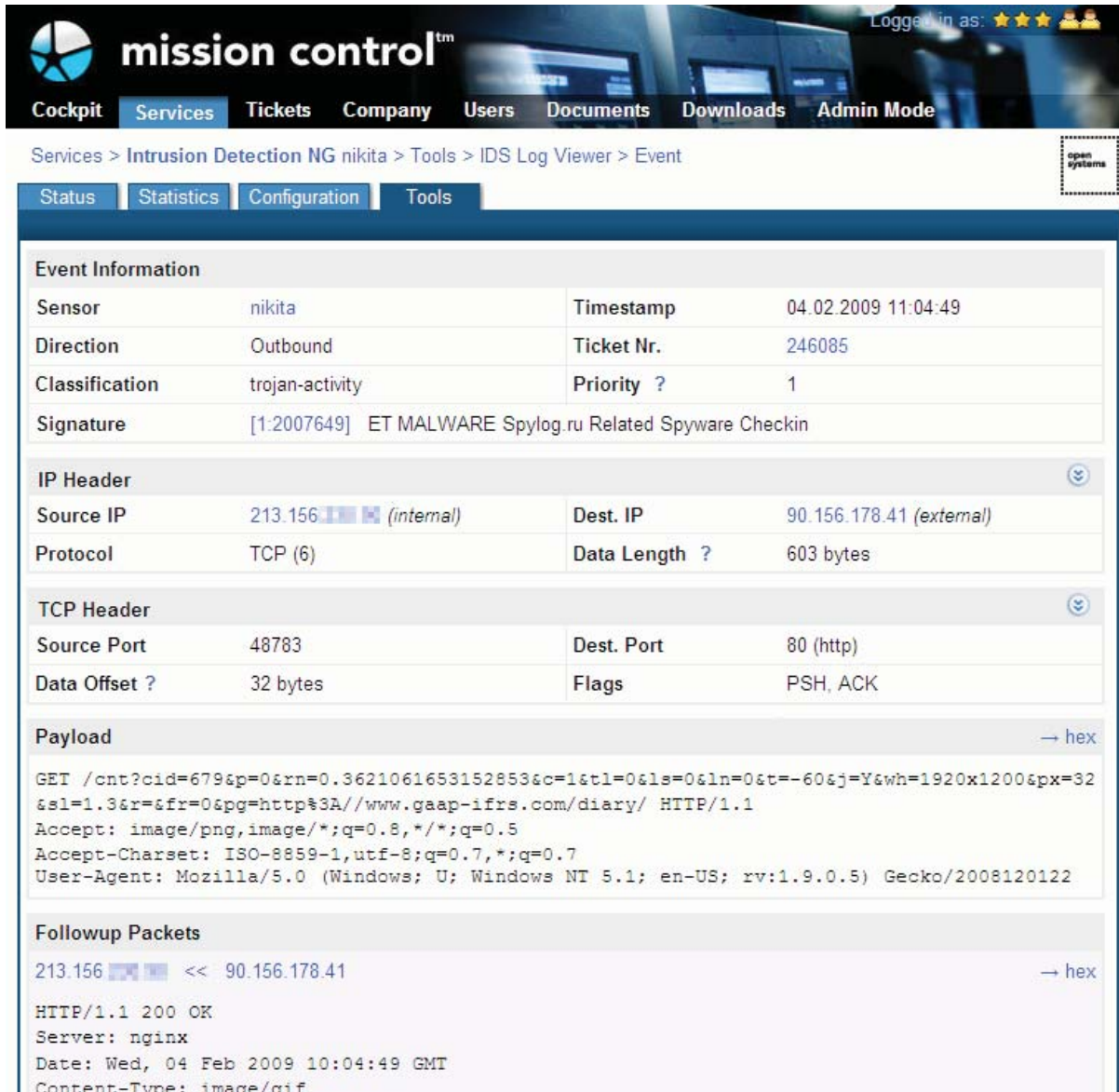
Last interrupt: 04.02.2009 17:10:44 [more >](#)

IDS Event Investigation

If the interest focuses on specific IDS events, the **IDS event viewer** allows deep packet investigation. As shown in the following figure, all events are listed in a table and can be sorted and filtered by IP address, ports and signatures. Even a full text signature search is available. All notified events are linked to the corresponding ticket that tracks the escalation procedure and contains all findings and investigations.

| Timestamp | External Host | Direction | Internal Host | Proto | Ext. Port | Int. Port | Signature |
|---------------------|---------------|-----------|---------------|-------|-----------|-----------|---|
| 27.11.2008 15:43:17 | | → | | UDP | 53 | 36236 | ET CURRENT_EVENTS Excessive DNS Responses with 1 or more RR's (100+ in 10 seconds) - possible Cache Poisoning Attempt |
| 27.11.2008 15:40:53 | 0.0.0.0 | → | | UDP | 8116 | 8116 | ET POLICY Reserved IP Space Traffic - Bogon Nets 1 |
| 27.11.2008 15:34:52 | 0.0.0.0 | → | | UDP | 8116 | 8116 | ET POLICY Reserved IP Space Traffic - Bogon Nets 1 |
| 27.11.2008 15:32:01 | | → | | TCP | 56885 | 80 | ET WEB Proxy HEAD Request |
| 27.11.2008 15:31:47 | | → | | TCP | 2915 | 8080 | ET WEB Proxy CONNECT Request |

Investigation of one event shows all details that are required to investigate any occurred incident including detailed event descriptions, IP DNS resolutions and follow-up packets.



mission control™
 Cockpit Services Tickets Company Users Documents Downloads Admin Mode

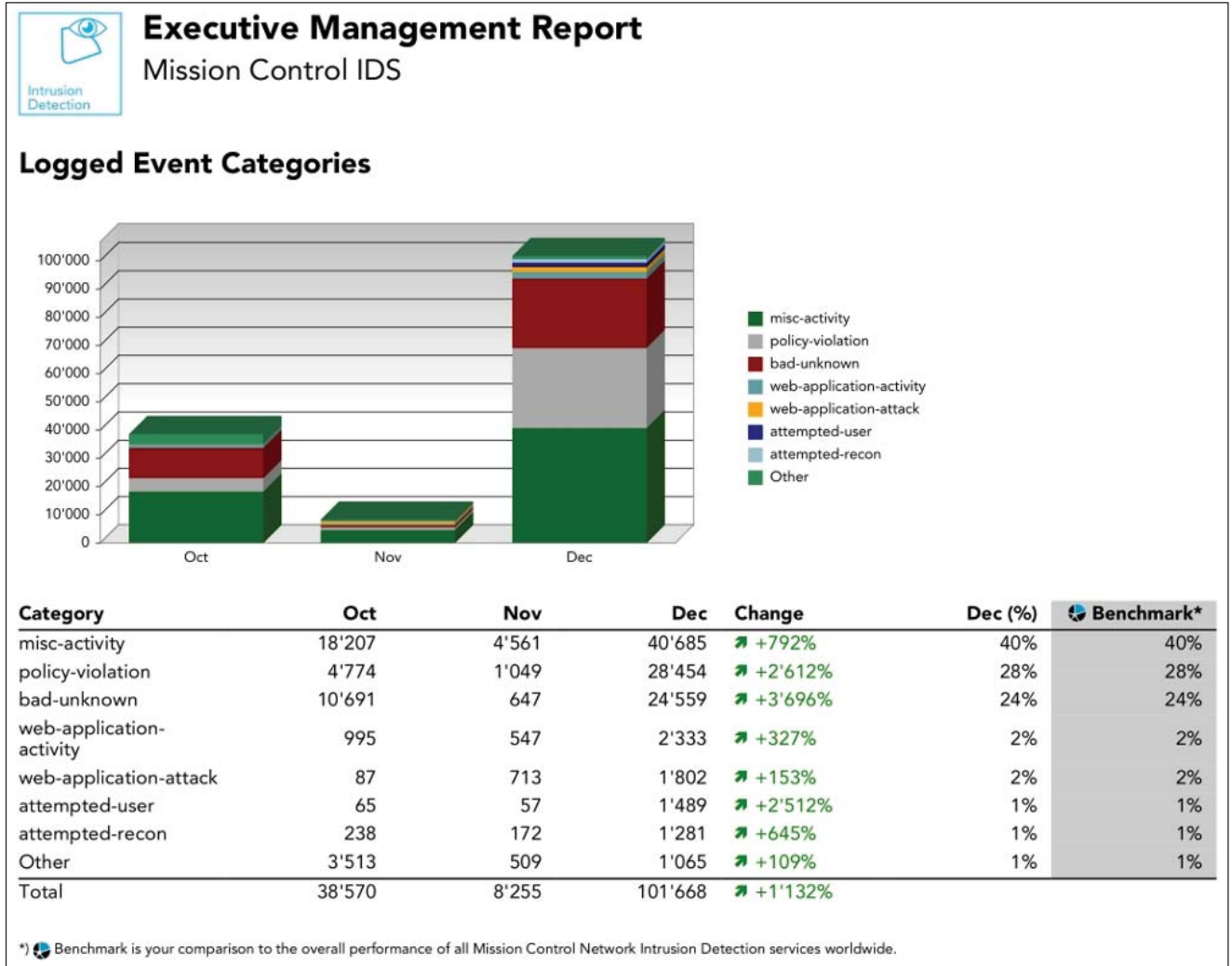
Services > Intrusion Detection NG nikita > Tools > IDS Log Viewer > Event

| Event Information | |
|---|--|
| Sensor | nikita |
| Timestamp | 04.02.2009 11:04:49 |
| Direction | Outbound |
| Ticket Nr. | 246085 |
| Classification | trojan-activity |
| Priority ? | 1 |
| Signature | [1:2007649] ET MALWARE Spylog.ru Related Spyware Checkin |
| IP Header | |
| Source IP | 213.156.111.111 (internal) |
| Dest. IP | 90.156.178.41 (external) |
| Protocol | TCP (6) |
| Data Length ? | 603 bytes |
| TCP Header | |
| Source Port | 48783 |
| Dest. Port | 80 (http) |
| Data Offset ? | 32 bytes |
| Flags | PSH, ACK |
| Payload | |
| <pre>GET /cnt?cid=679&p=0&rn=0.3621061653152853&c=1&t1=0&ls=0&ln=0&t=-60&j=Y&wh=1920x1200&px=32 &sl=1.3&r=&fr=0&pg=http%3A//www.gaap-ifrs.com/diary/ HTTP/1.1 Accept: image/png,image/*;q=0.8,*/*;q=0.5 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.5) Gecko/2008120122</pre> | |
| Followup Packets | |
| <pre>213.156.111.111 << 90.156.178.41 HTTP/1.1 200 OK Server: nginx Date: Wed, 04 Feb 2009 10:04:49 GMT Content-Type: image/gif</pre> | |

Reporting

Mission Control issues a **monthly IDS report** which focuses on the executive management audience. On the introduction and summary page, event occurrences and event categories are compared to previous months. On the following pages, the IDS report focuses on each sensor and provides more information about the monitored environment and reported incidents at that location.

Event categories summaries and trends:





Ticket statistics, trends, and per sensor logged events:

Executive Management Report

Mission Control IDS

Ticket Statistics

| Tickets | Change | Type |
|---------|--------|----------|
| 0 | ↘ -1 | Change |
| 0 | | Incident |
| 0 | | Other |
| 0 | ↘ -1 | Total |

Sensors

| Hostname | Location | Description | Page |
|----------------------|---------------------------------|----------------------------|------|
| amande | Zürich (Switzerland, Europe) | Test IDS host @ ETH Zurich | 4 |
| nikita | Amsterdam (Netherlands, Europe) | IDS test | 5 |
| ████████████████████ | Zürich (Switzerland, Europe) | Test IDS host @ ██████████ | 6 |

Total Logged Events

| Sensor | Oct | Nov | Dec | Change |
|----------------------|---------------|--------------|----------------|------------------|
| amande | - | 488 | 10'935 | ↗ +2'141% |
| nikita | 38'570 | 7'767 | 70'026 | ↗ +802% |
| ████████████████████ | - | - | 20'707 | - 0% |
| Total | 38'570 | 8'255 | 101'668 | ↗ +1'132% |

Per-sensor detail information including single event descriptions



Executive Management Report

Mission Control IDS

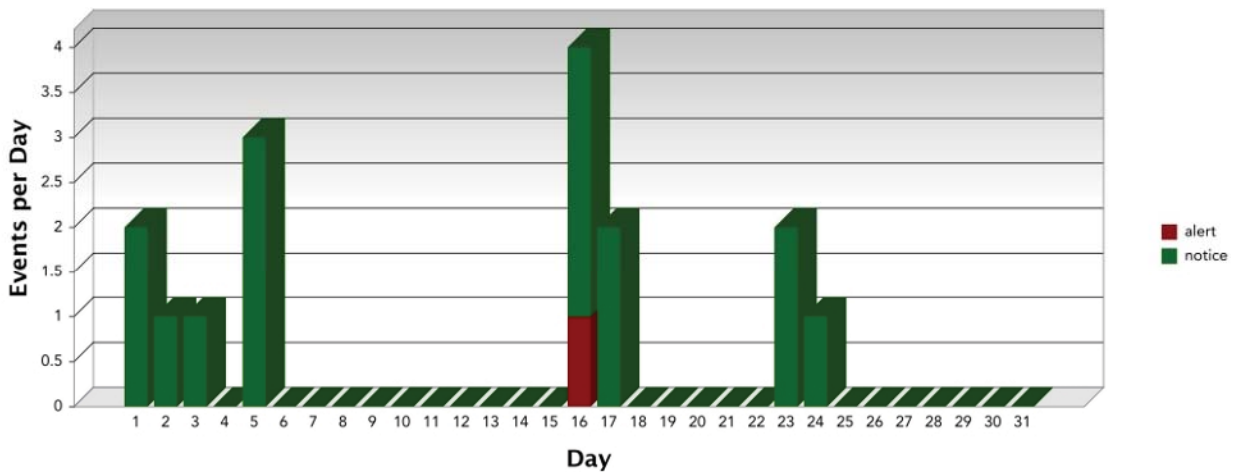
Details for sensor amande

Configuration

| | |
|-------------------------------|------------------------------|
| Hostname: | amande |
| Location: | Zürich (Switzerland, Europe) |
| Description: | Test IDS host @ ETH Zurich |
| Management IP address: | 213.156.228.51 |
| Monitored Networks: | 213.156.230.80/28 |

Monthly Distribution of Events Requiring Attention

Number of events analyzed by Mission Control: 15
Number of events immediately escalated to Open Systems AG: 1



Comments

The following events required special attention and were the most frequent cause for tickets:

- The **ET POLICY FTP Login Successful (non-anonymous)** event was triggered 5 times. It was caused by outbound traffic only. 2 different internal hosts and 4 different external hosts were involved in this event.
- The **ET TROJAN Vipdataend C&C Traffic - Status OK** event was triggered 3 times. It was caused by outbound traffic only. One internal host and 2 different external hosts were involved in this event.
- The **ET POLICY Outbound Multiple Non-SMTP Server Emails** event was triggered 2 times. It was caused by outbound traffic only. 2 different internal hosts and 2 different external hosts were involved in this event.
- The **INFO FTP Bad login** event was triggered 1 time. It was caused by outbound traffic only. One internal host and one external host were involved in this event.
- The **ET MALWARE Suspicious User-Agent (Installer)** event was triggered 1 time. It was caused by outbound traffic only. One internal host and one external host were involved in this event.
- The **ET MALWARE Suspicious User Agent (Microsoft Internet Explorer)** event was triggered 1 time. It was caused by outbound traffic only. One internal host and one external host were involved in this event.