SID (Space Intrusion Detection)

Heinrich Elsigan

September 2026

Contents

Figure 1: UFO series: SID Space Intrusion Detection

1 Introduction

SID is a concept for an intrusion detection system for linux servers in internet or local network including cloud linux servers,

1. SID daily monitors (and highlights changes to yesterday)
   - all mounted data filesystems in detail (except log files, caches, /var/sppol/*)
   - installed kernel, kernel modules lsmod, kernel config and boot (initrd image
   - current kernel and system settings (/proc fs)
   - attached and registered devices
   - network interfaces and netfilter iptables ip6tables rules
   - all running daemons especially those who allocate listening network tcp/udp socket descriptors
2. SID hourly monitors
   - available free disk space
   - load average
   - currently active users and daemons
   - all system inter-process communications ipcs lsipc
   - all file descriptors, locks, ... lsfd lslocks,
   - ...
3. SID permanently monitors
   - successful and failed authentications
   - errors with hints of critical intrusion in all logfies
   - heavy process or cpu load, which could be an internal privilege escalation or brute force attack

...

1.1 Prequel

In UFO TV Series 1970s a SID Space Intrusion Detection, that scans permanently for unidentified flight objects, detects and tracks them and probabilistic calculates most possible ufo's attack vectors. Ufo series intro outro

2 Actions

2.1 Regular monitoring activities

SID writes a daily report and highlites all changes to yesterday. filesystem files changed content (sha512), special permissions and all filesystem date time entry changes are emphasized too.

When a concern or intrusion rule matches at daily changes, SID sends additionally an email or SMS. (We don't want to have too many SPAMs for sysadmin / manager like in Nagios.) Nevertheless SID should send a weekly or montly 'all well and alive' email message, so that you know, that SID is still operating.

2.2 YELLOW and RED alerts intrusion triggers

SID sends immediate an email / sms or Endpoint Service message in case of yellow / red alert at intrusion detection.

. . . . . .

3 SID protection

SID binaries are launched from a readonly not modifyable squash fs mounted image e.g. by snapcraft, a hardware protected usb stick, a LUKS encrypted readonly mounted filesystem or cd / dvd. SID config files should also only mounted rw, when changing them. SID reports could be signed, symmetric or asymmetric encrypted (with passwd or key or X509 certificate).

. . . . . .

4 Epilog

4.1 Good luck!

We hope you find SID useful and good luck. To contact me, use the contacts at https://heinrichelsigan.area23.at.

Abstract

Hi, I'm Heinrich Elsigan I am interested in C#, Java, MSSQL, .Net Core, Android and politics, society and the future; currently working as freelancer (one person company) and planning a secure endpoint 2 endpoint chat and looking to collaborate on reviews for other repositories and projects. Article written in LaTeX.

1. personal tech and political blog blog.area23.at
2. GitHub repositories github.com/heinrichelsigan/
3. StackOverflow stackoverflow.com/users/12213151/heinrich-elsigan
4. Curriculum vitae heinrichelsigan.area23.at/cv
5. live demo .Net area23.at/net

References