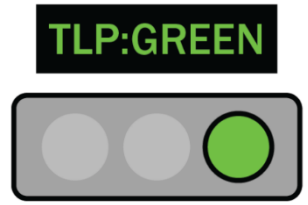


RNEP-GW

MÓDULO IDS

fct csirt

RNEP-GW

DETECÇÃO DE INTRUSÕES

Performance (multithread)

IDS/IPS

Assinaturas

Integração

SURICATA

suricata.io

Suricata is far more than an IDS/IPS

Network Traffic
Cloud & On-premise

SURICATA®

- IDS Alerts
- Protocol Transactions
- Network Flows
- PCAP Recordings
- Extracted Files

PERFORMANCE

Maior volume de dados = mais recursos necessários

- CPU
- Capacidade de escrita em disco

Processar tráfego de várias portas de rede ao mesmo tempo pode ser um problema

HARDWARE

Características em uso, sobredimensionadas

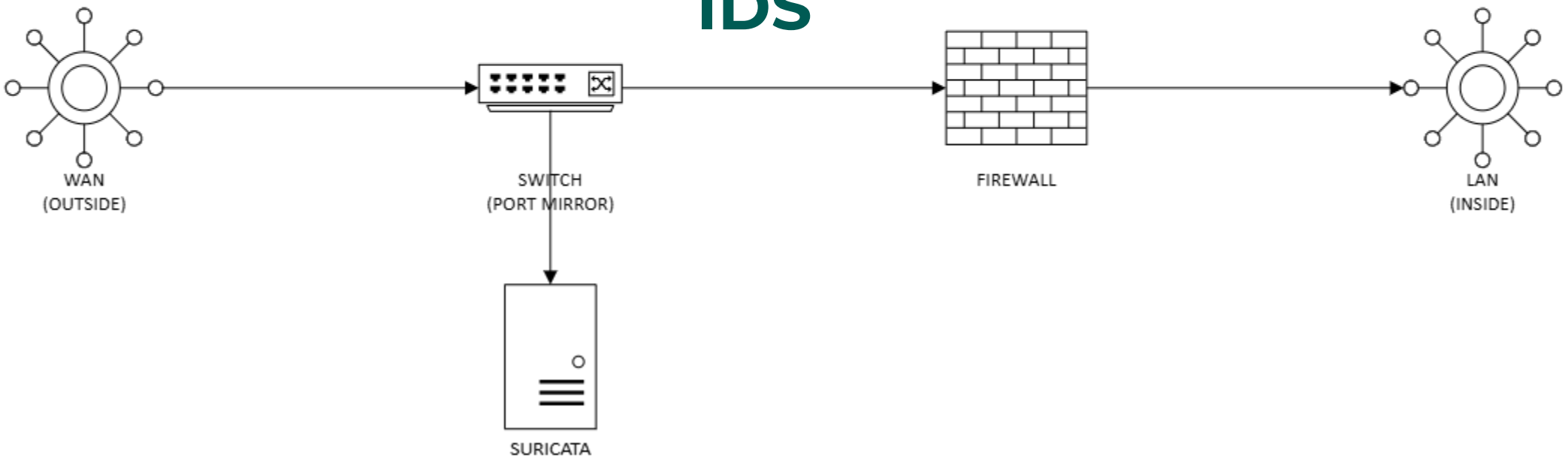
- CPU: 40 cores
- Memória: 64GB
- Storage: 1.3TB
- Rede: 2x 10Gbps + 4x 1Gbps

Aconselhável consultar documentação

IPS


WAN
(OUTSIDE)
SURICATA
FIREWALL
LAN
(INSIDE)

IDS


WAN
(OUTSIDE)
SWITCH
(PORT MIRROR)
SURICATA
FIREWALL
LAN
(INSIDE)

ASSINATURAS

Permitem identificar anomalias

Imperativo actualizar a base de dados de assinaturas com frequência

Algumas assinaturas são «free», outras comerciais (pagas)

INTEGRAÇÃO

Envio de logs para um SIEM

- Opções: Splunk, Logstash, etc

Importante monitorizar o volume de dados

- Para evitar esgotamento de storage
- Para impedir exaustão de licenciamento (Splunk)

INTEGRAÇÃO (ENVIO DE QUEIXAS)

Dear Sir or Madam,

RCTS CERT is the Computer Security Incident Response Team for the Portuguese Research and Education Network (RCTS).

We are writing you to inform that we have detected malicious activity from 121.229.3.166 at our constituency's Network addresses.

We kindly request your help in order to investigate and cease the reported activity.

========== Evidence (WEST Timezone)==========

Timestamp: 2025-05-15T18:02:36.320101+0100

Source IP: 121.229.3.166

Source port: 50997

Destination IP: 193.136.192.107

Destination port: 80

Alert Signature: ET HUNTING Suspicious PHP Code in HTTP POST (Inbound)

Timestamp: 2025-05-15T18:02:36.320101+0100

Source IP: 121.229.3.166

Source port: 50997

Destination IP: 193.136.192.107

Destination port: 80

Alert Signature: ET WEB_SERVER PHP tags in HTTP POST

Timestamp: 2025-05-15T18:02:36.320101+0100

Source IP: 121.229.3.166

Source port: 50997

Destination IP: 193.136.192.107

Destination port: 80

Alert Signature: ET HUNTING Suspicious PHP Code in HTTP POST (Inbound)

EXEMPLOS (ET SCAN POTENTIAL SSH SCAN)

{"timestamp":"2025-07-12T00:00:45.085576+0100","flow_id":1823078721867336,"in_iface":"eno49","event_type":"alert","src_ip":"195.178.110.160","src_port":38651,"dest_ip":"193.136.46.233","dest_port":22,"proto":"TCP","alert":{"action":"allowed","gid":1,"signature_id":2001219,"rev":20,"signature":"ET SCAN Potential SSH Scan","category":"Attempted Information Leak","severity":2,"metadata":{"created_at":["2010_07_30"],"updated_at":["2010_07_30"]}},"flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-07-12T00:00:45.085576+0100"},"payload_printable":"","stream":0}

EXEMPLOS (ET SCAN POTENTIAL VNC SCAN)

{"timestamp":"2025-07-12T00:00:48.617864+0100","flow_id":652300701953416,"in_iface":"eno49","event_type":"alert","src_ip":"83.222.191.166","src_port":58093,"dest_ip":"193.136.46.43","dest_port":5900,"proto":"TCP","alert":{"action":"allowed","gid":1,"signature_id":2002911,"rev":6,"signature":"ET SCAN Potential VNC Scan 5900-5920","category":"Attempted Information Leak","severity":2,"metadata":{"created_at":["2010_07_30"],"updated_at":["2010_07_30"]}},"flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2025-07-12T00:00:48.617864+0100"},"payload_printable":"","stream":0}

EXEMPLOS (ET SCAN SUSPICIOUS INBOUND TO MYSQL PORT 3306)

{"timestamp":"2025-07-13T00:03:01.549919+0100","flow_id":15622
4765387807,"in_iface":"eno49","event_type":"alert","src_ip":"147.1
85.132.246","src_port":49426,"dest_ip":"193.136.193.81","dest_port"
:3306,"proto":"TCP","alert":{"action":"allowed","gid":1,"signature_i
d":2010937,"rev":3,"signature":"ET SCAN Suspicious inbound to
mySQL port 3306","category":"Potentially Bad Traffic","severity":
2,"metadata":{"created_at":["2010_07_30"],"former_category":["H
UNTING"],"updated_at":["2018_03_27"]}},"flow":{"pkts_toserver":1
,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclient":0,"start":"2
025-07-13T00:03:01.549919+0100"}}

EXEMPLOS (GPL RPC PORTMAP LISTING UDP 111)

{"timestamp":"2025-07-13T00:02:35.257449+0100","flow_id":1854789840006569,"in_iface":"eno49","event_type":"alert","src_ip":"162.142.125.81","src_port":62659,"dest_ip":"194.210.142.36","dest_port":111,"proto":"UDP","alert":{"action":"allowed","gid":1,"signature_id":2101280,"rev":10,"signature":"GPL RPC portmap listing UDP 111","category":"Decode of an RPC Query","severity":2,"metadata":{"created_at":["2010_09_23"],"updated_at":["2010_09_23"]}},"app_proto":"failed","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":82,"bytes_toclient":0,"start":"2025-07-13T00:02:35.257449+0100"}}

EXEMPLOS (ET DROP SPAMHAUS DROP LISTED TRAFFIC INBOUND GROUP 10)

{"timestamp":"2025-07-13T00:03:01.671675+0100","flow_id":1367444197556155,"in_iface":"eno49","event_type":"alert","src_ip":"122.8.185.158","src_port":33642,"dest_ip":"193.137.196.76","dest_port":443,"proto":"TCP","metadata":{"flowbits":["ET.Evil","ET.DROPIP"]},"alert":{"action":"allowed","gid":1,"signature_id":2400009,"rev":3189,"signature":"ET DROP Spamhaus DROP Listed Traffic Inbound group 10","category":"Misc Attack","severity":2,"metadata":{"affected_product":["Any"],"attack_target":["Any"],"created_at":["2010_12_30"],"deployment":["Perimeter"],"signature_severity":["Minor"],"tag":["Dshield"],"updated_at":["2022_03_10"]}},"flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":74,"bytes_toclient":0,"start":"2025-07-13T00:03:01.671675+0100"}}

DASHBOARDS (SPLUNK)

Suricata_IDS - Assinaturas LIS2 e LIS3

Edit | Export | ...

LIS2 (suricata2)

201 BACKUP

LIS3 (suricata3)

82,710 PRINCIPAL

LIS2

	alert.signature	count
1	ET DROP Dshield Block Listed Source group 1	151
2	ET SCAN Potential SSH Scan	20
3	ET SCAN Potential VNC Scan 5900-5920	14
4	ET SCAN Potential SSH Scan OUTBOUND	3
5	ET SCAN HID VertX and Edge door controllers discover	2
6	ET SCAN Potential VNC Scan 5800-5820	2
7	GPL RPC portmap listing UDP 111	2
8	ET EXPLOIT HackingTrio UA (Hello, World)	1
9	ET POLICY Spotify P2P Client	1
10	ET SCAN Mirai Variant User-Agent (Inbound)	1
11	ET WEB_SERVER 401TRG Generic Webshell Request - POST with wget in body	1
12	ET WEB_SERVER WebShell Generic - wget http - POST	1
13	GPL POLICY PCAnywhere server response	1
14	GPL RPC xdmcp info query	1

LIS3

	alert.signature	count
1	ET DROP Dshield Block Listed Source group 1	28324
2	ET SCAN Suspicious inbound to MSSQL port 1433	12434
3	ET SCAN Suspicious inbound to mySQL port 3306	5263
4	GPL DNS named version attempt	4933
5	ET SCAN Suspicious inbound to PostgreSQL port 5432	3868
6	GPL SNMP public access udp	3817
7	ET INFO Observed Free Hosting Domain (*.000webhostapp .com in DNS Lookup)	3564
8	ET SCAN Potential SSH Scan	2928
9	GPL SCAN PING CyberKit 2.2 Windows	2015
10	ET SCAN Suspicious inbound to Oracle SQL port 1521	1591
11	ET SCAN Potential VNC Scan 5900-5920	1430
12	GPL WEB_SERVER 403 Forbidden	1303
13	ET DROP Spamhaus DROP Listed Traffic Inbound group 10	1078
14	GPL RPC xdmcp info query	875
15	GPL RPC portmap listing UDP 111	613

IDEIAS CHAVE

- Em termos de detecção é importante termos uma visão sobre todo o tráfego que entra e sai de uma organização
- A detecção funciona principalmente com base em assinaturas
- Podem desencadear-se acções na sequência de uma detecção, ou interagir com outros sistemas

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc