MikroTik

Реализуем проактивную систему IPS/IDS защиты на Mikrotik + Suricata

MUM Moscow 2018
mikrotik-training.ru

ОБО МНЕ

- Козлов Роман Сергеевич
- Сертифицированный тренер по MikroTik
- Технический директор IntegaSky
- Провожу бесплатные обучающие вебинары по MikroTik
- Более 200 выполненных проектов MikroTik
- Проводим мини-тренинги – mikrotik.team
- Являюсь соведущим linkmeup_sysadmins

Канал на youtube
https://goo.gl/DSL6VG

Запись на вебинары
http://mikrotik-training.ru/webinar/

Канал в телеграм
https://t.me/miktrain

Содержание

- Общие сведения о IPS/IDS
- Проблема отсутствия встроенного функционала в RouterOS и варианты решений
- Обзор бесплатного решения Suricata
  - Принцип работы
  - Работа со списками правил
  - Интеграция с firewall RouterOS
- Отправка трафика routerOS
  - Port mirroring
  - TZSP – pcap
- SELKS – готовое решение

OSI

firewall vs IDS/IPS

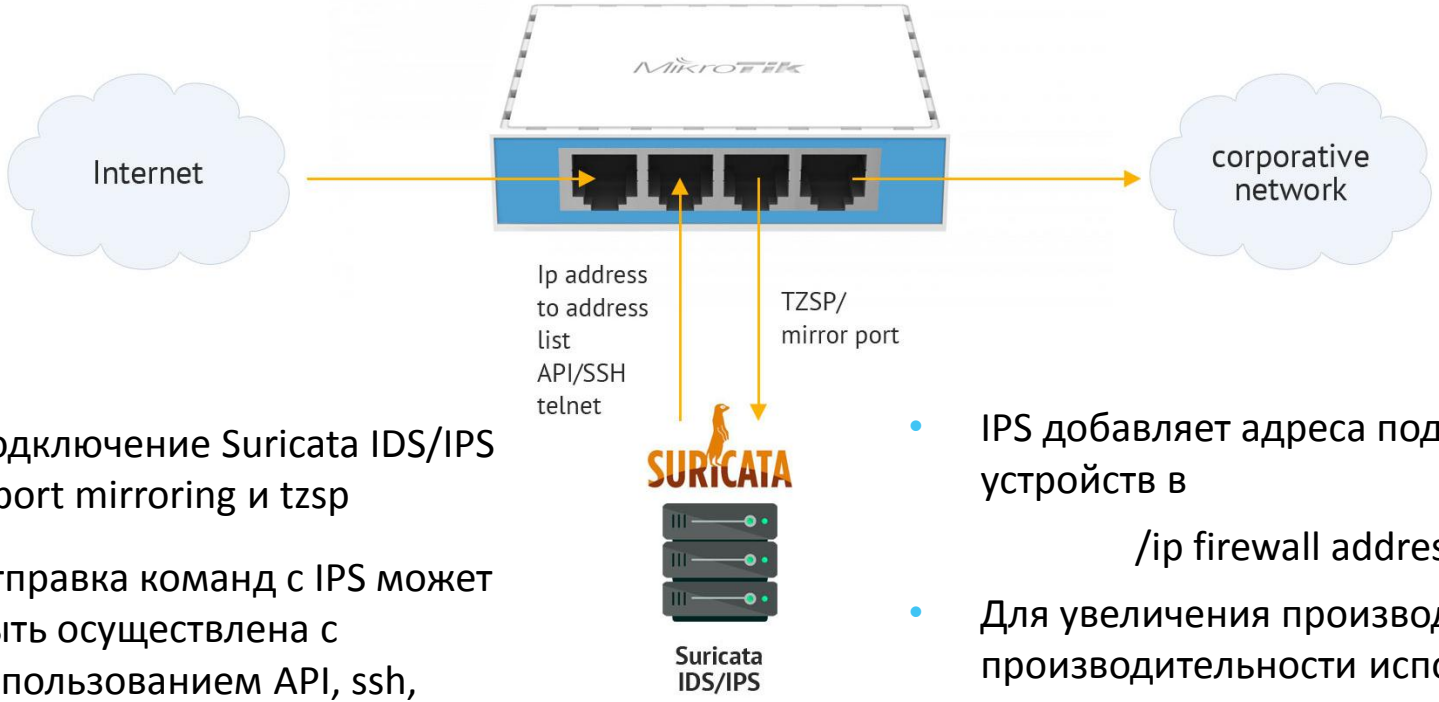
firewall			IDS/IPS
firewall filter L7/content *	7	Прикладной уровень	Проверка сигнатурами
firewall filter L7/content *	6	Представительный уровень	Поведенческая проверка
firewall filter *	5	Сеансовый уровень	
firewall filter	4	Транспортный уровень	
firewall filter	3	Сетевой уровень	
bridge firewall	2	Канальный уровень	
	1	Физический уровень	

Общие сведения о IPS/IDS

- Задача **IDS (Intrusion Detection System)** состоит в обнаружении и регистрации атак, а также оповещении при срабатывании определенного правила. В отличие от межсетевого экрана, контролирующего только параметры сессии (IP, номер порта и состояние связей), IDS «заглядывает» внутрь пакета (до седьмого уровня OSI), анализируя передаваемые данные.
- **IDS умеют:**
  - выявлять различные виды сетевых атак
  - обнаруживать попытки неавторизованного доступа или повышения привилегий
  - появление вредоносного ПО
  - отслеживать открытие нового порта и т. д.
- **IPS (Intrusion Prevention System)** - система предотвращения атак.
- **IDS** могут самостоятельно перестраивать пакетный фильтр или прерывать сеанс, отсылая TCP RST.

Проблема отсутствия встроенного функционала в RouterOS и варианты решений

1. RouterOS – это классический firewall с некоторыми дополнениями:
   - Layer 7 filter – возможность поиска по регулярным выражениям в 2kb пакета
   - Content filter – функция поиска в нешифрованных пакетах содержимого
   - TLS host - Позволяет сопоставлять трафик https на основе имени узла SNS SNI
   - Возможно настраивать поведенческие фильтры на основании количества соединений и их частоты
2. В RouterOS нет функционала IDS/IPS часть функций можно реализовать на L7/content filtering – что потребует больших трудозатрат и будет достаточно неэффективно
3. Так же подобные настройки снизят производительность нашего firewall



- Подключение Suricata IDS/IPS – port mirroring и tzsp
- Отправка команд с IPS может быть осуществлена с использованием API, ssh, telnet

- IPS добавляет адреса подозрительных устройств в

  /ip firewall address list
- Для увеличения производительности производительности используем

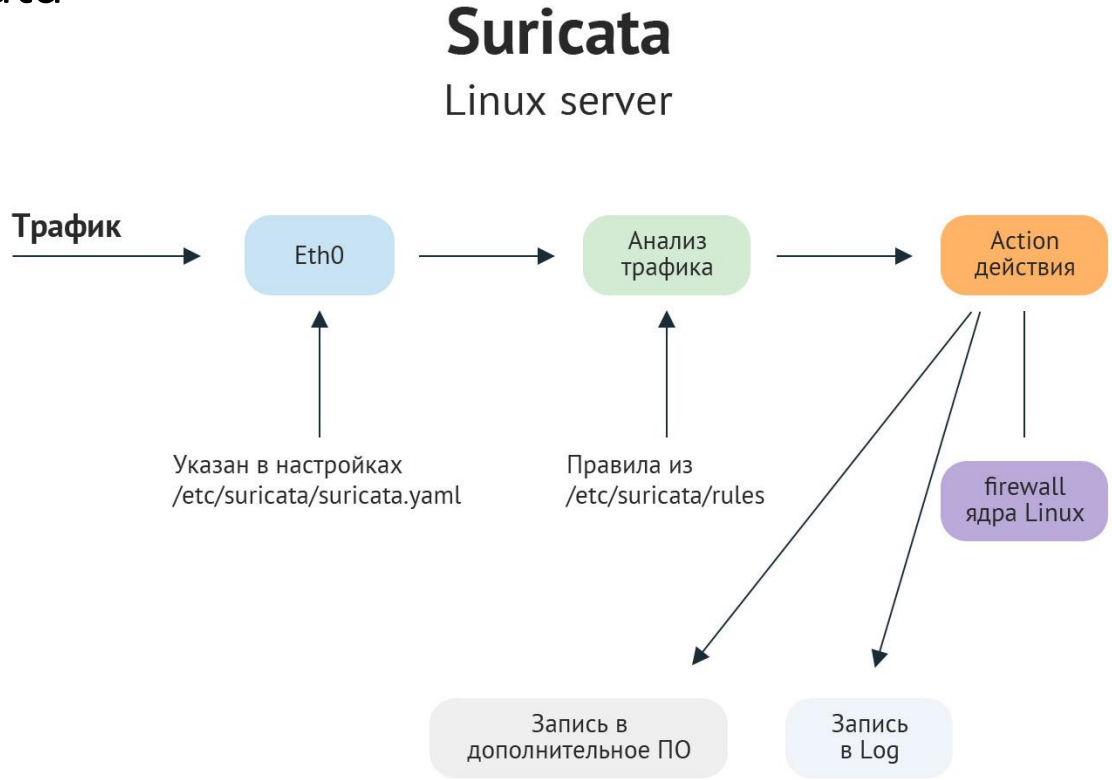
  /ip firewall raw
- Не забываем про белые списки
- Не забываем тестировать

Обзор бесплатного решения Suricata

1. Бесплатное решение IDS / IPS GPLv2
2. Suricata работает в многопоточном режиме
3. Возможность аппаратного ускорения на стороне GPU
4. Поддерживается IPv6
5. Движок автоматически определяет протоколы IP, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB, SMTP и SCTP
6. Интерфейсы и анализаторы, написанные для Snort (Barnyard, Snortsnarf, Sguil и т. д.), без доработок работают и с Suricata
7. Основу механизма детектирования в Suricata составляют правила (rules)
8. Не поддерживает TZSP

Принцип работы Suricata

- Изначально Suricata получает трафик на интерфейс, указанный в настройках /etc/suricata/suricata.yaml
- По правилам указанным в файле конфигурации с помощью сигнатур в /etc/suricata/rules происходит обработка трафика и детектирование угроз
- Поведение по умолчанию предполагает запись обнаруженных угроз в log
- Так же есть возможность исполнять различные действия



Работа со списками правил Suricata

1. Собственный формат правил rules,
2. Правило состоит из трех компонентов:
   - действие - pass, drop, reject или alert
   - заголовок - IP/порт источника и назначения
   - описание (что искать).
3. В настройках используются переменные, позволяющие, например, создавать счетчики.
4. При этом информацию из потока можно сохранять для последующего использования.

Интеграция с firewall RouterOS

1. **На forum.mikrotik.com есть реализация интеграции с routeros**
   - PHP скрипт берет ip адреса нарушителей из /var/log/suricata/fast.log и добавляет их через API в адрес лист mikrotik
   - PHP скрипт берет ip адреса нарушителей из базы данных barnyard2(дополнительное ПО) и добавляет их через API в адрес лист mikrotik

2. **Прием трафика от mikrotik**
   - На interface
   - TZSP port – требуется виртуальный интерфейс и дополнительное ПО – trafr (mikrotik.com) или tzsp2pcap (github)

Отправка трафика RouterOS

1. **Port mirroting – функция switch**
   - /interface ethernet switch set switch1 mirror-source=ether2 mirror-target=ether3

2. **Отправка трафика по протоколу TZSP**
   - /tool sniffer set streaming-enabled=yes streaming-server=192.168.x.x
   - /ip firewall mangle add action=sniff-tzsp chain=prerouting sniff-target=192.168.x.x sniff-target-port=37008

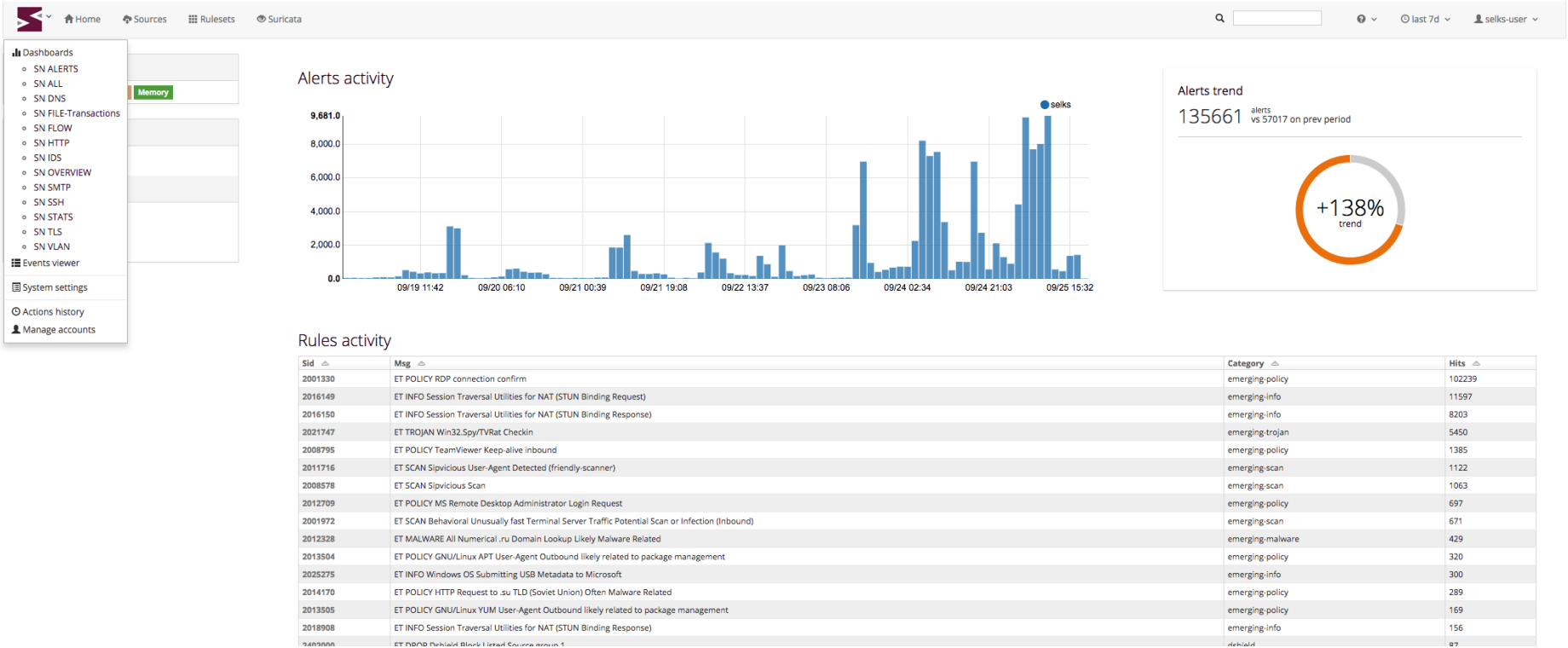
SELKS

1. Бесплатное готовое решение для работы с suricata

2. Selks состоит из
   - Suricata – IDS/IPS движек
   - Elasticsearch 5.5.2 – поисковый движок
   - Logstash 5.5.2 – сбор логов и последующая их обработка
   - Kibana 5.5.2 – веб интерфейс для отображения данных из Elasticsearch
   - Scirius – веб интерфейс для управления suricata и навигации по kibana
   - EveBox – альтернативный веб интерфейс для управления событиями suricata

3. Поставляется в виде готового iso образа.

SELKS



Sid	Msg	Category	Hits
2001330	ET POLICY RDP connection confirm	emerging-policy	102239
2016149	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)	emerging-info	11597
2016150	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	emerging-info	8203
2021747	ET TROJAN Win32.Spy/TVRat Checkin	emerging-trojan	5450
2008795	ET POLICY TeamViewer Keep-alive inbound	emerging-policy	1385
2011716	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	emerging-scan	1122
2008578	ET SCAN Sipvicious Scan	emerging-scan	1063
2012709	ET POLICY MS Remote Desktop Administrator Login Request	emerging-policy	697
2001972	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)	emerging-scan	671
2012328	ET MALWARE All Numerical .ru Domain Lookup Likely Malware Related	emerging-malware	429
2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	emerging-policy	320
2025275	ET INFO Windows OS Submitting USB Metadata to Microsoft	emerging-info	300
2014170	ET POLICY HTTP Request to .su TLD (Soviet Union) Often Malware Related	emerging-policy	289
2013505	ET POLICY GNU/Linux YUM User-Agent Outbound likely related to package management	emerging-policy	169
2018908	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	emerging-info	156
2402000	ET DROP Dshield Block Listed Source group 1	dshield	87

SELKS

Home Sources Rulesets Suricata last 7d selks-user

System status

Suricata Elasticsearch Disk Memory

Suricata selks

Ruleset: Default SELKS ruleset
Description: Suricata on SELKS
Last updated: Sept. 24, 2018, 11 p.m.

Action

Ruleset actions
Edit

CPU

Memory

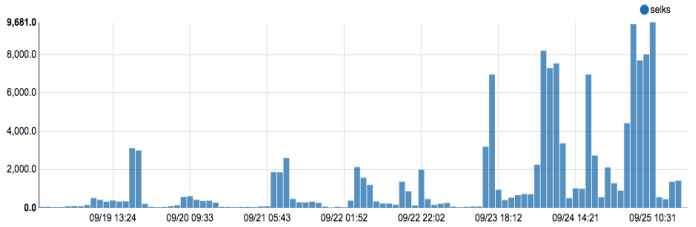
Disk

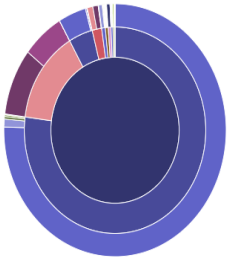
Rules activity | Capture stats | Memory usage | Problem indicators

Rules activity

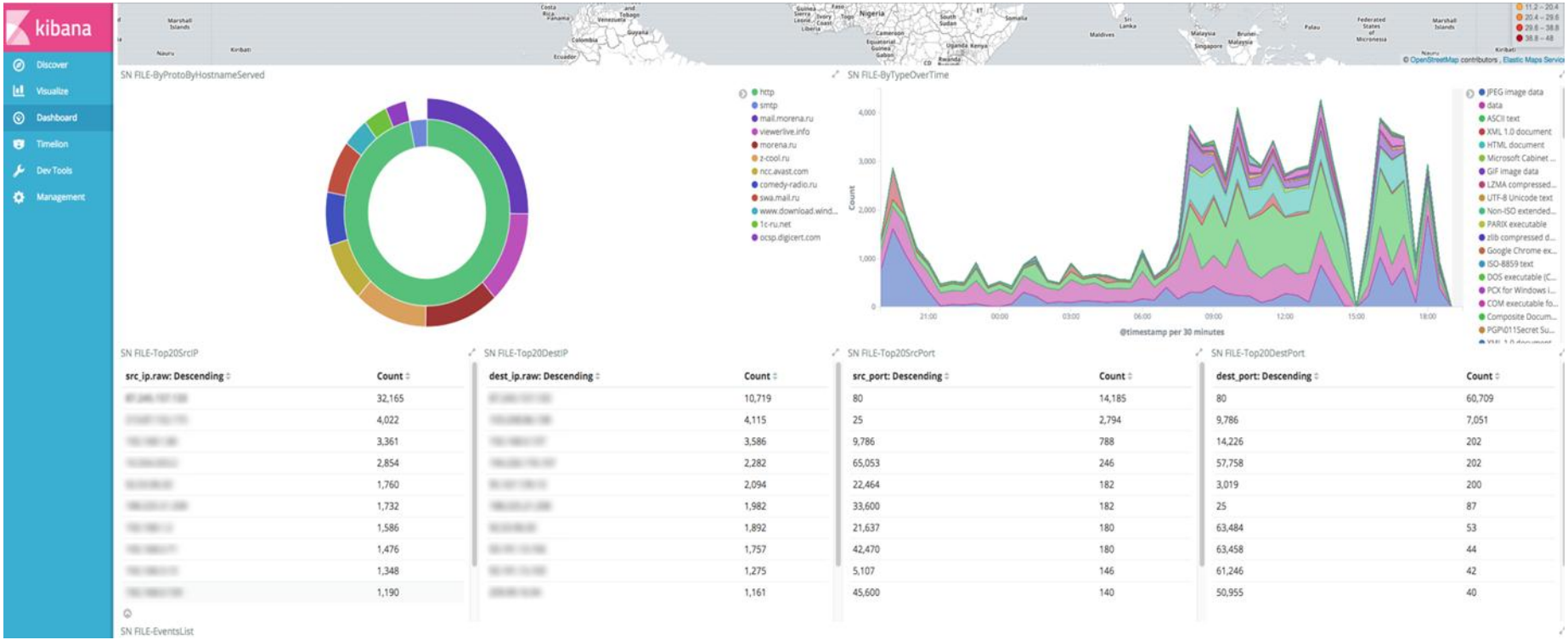
Sid	Msg	Category	Hits
2001330	ET POLICY RDP connection confirm	emerging-policy	102239
2016149	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)	emerging-info	11597
2016150	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	emerging-info	8203
2021747	ET TROJAN Win32.Spy/TVRat Checkin	emerging-trojan	5450
2008795	ET POLICY TeamViewer Keep-alive inbound	emerging-policy	1385
2011716	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	emerging-scan	1122
2008578	ET SCAN Sipvicious Scan	emerging-scan	1063
2012709	ET POLICY MS Remote Desktop Administrator Login Request	emerging-policy	697
2001972	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)	emerging-scan	671
2012328	ET MALWARE All Numerical .ru Domain Lookup Likely Malware Related	emerging-malware	429
2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	emerging-policy	320
2025275	ET INFO Windows OS Submitting USB Metadata to Microsoft	emerging-info	300
2014170	ET POLICY HTTP Request to .su TLD (Soviet Union) Often Malware Related	emerging-policy	289
2013505	ET POLICY GNU/Linux YUM User-Agent Outbound likely related to package management	emerging-policy	169
2018908	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	emerging-info	156
2402000	ET DROP Dshield Block Listed Source group 1	dshield	87
2000328	ET POLICY Outbound Multiple Non-SMTP Server Emails	emerging-policy	85
2023753	ET SCAN MS Terminal Server Traffic on Non-standard Port	emerging-scan	74
2403329	ET CINS Active Threat Intelligence Poor Reputation IP group 30	ciarmy	73
2522188	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 95	tor	66

Alerts activity

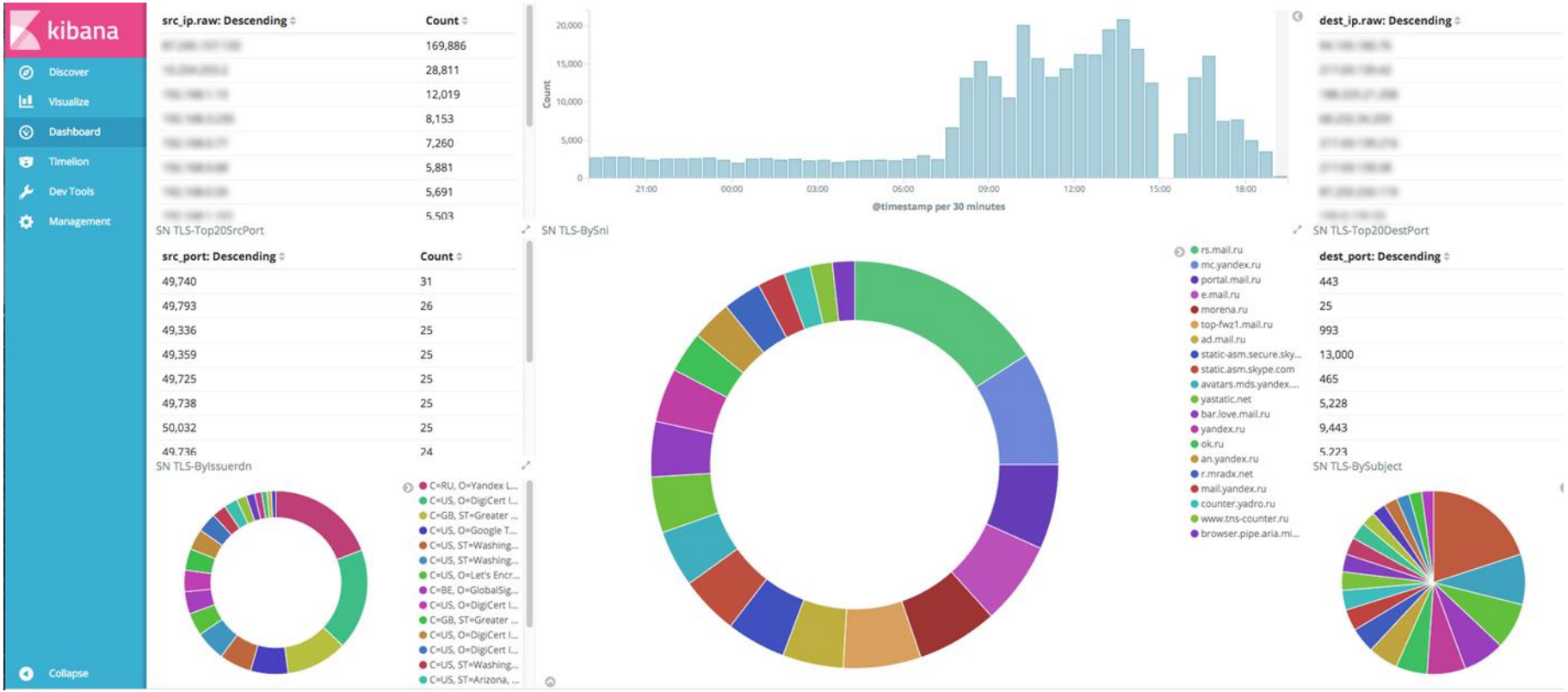




SELKS


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
SN FILE-ByProtoByHostnameServed
SN FILE-ByTypeOverTime
http
smtp
mail.morena.ru
viewerlive.info
morena.ru
z-cool.ru
ncc.avast.com
comedy-radio.ru
swa.mail.ru
www.download.wind...
1c-ru.net
ocsp.digicert.com
Count
@timestamp per 30 minutes
SN FILE-Top20SrcIP
src_ip.raw: Descending
Count
32,165
4,022
3,361
2,854
1,760
1,732
1,586
1,476
1,348
1,190
SN FILE-Top20DestIP
dest_ip.raw: Descending
Count
10,719
4,115
3,586
2,282
2,094
1,982
1,892
1,757
1,275
1,161
SN FILE-Top20SrcPort
src_port: Descending
Count
80
14,185
25
2,794
9,786
788
65,053
246
22,464
182
33,600
182
21,637
180
42,470
180
5,107
146
45,600
140
SN FILE-Top20DestPort
dest_port: Descending
Count
80
60,709
9,786
7,051
14,226
202
57,758
202
3,019
200
25
87
63,484
53
63,458
44
61,246
42
50,955
40
SN FILE-EventsList

SELKS


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
src_ip.raw: Descending
Count
169,886
28,811
12,019
8,153
7,260
5,881
5,691
5,503
SN TLS-Top20SrcPort
20,000
15,000
10,000
5,000
0
Count
21:00
00:00
03:00
06:00
09:00
12:00
15:00
18:00
@timestamp per 30 minutes
SN TLS-BySni
dest_ip.raw: Descending
SN TLS-Top20DestPort
src_port: Descending
Count
49,740
49,793
49,336
49,359
49,725
49,738
50,032
31
26
25
25
25
25
25
SN TLS-BySsuerdn
C=RU, O=Yandex L...
C=US, O=DigiCert I...
C=GB, ST=Greater ...
C=US, O=Google T...
C=US, ST=Washing...
C=US, ST=Washing...
C=US, O=Let's Encr...
C=BE, O=GlobalSig...
C=US, O=DigiCert I...
C=GB, ST=Greater ...
C=US, O=DigiCert I...
C=US, O=DigiCert I...
C=US, ST=Washing...
C=US, ST=Arizona, ...
rs.mail.ru
mc.yandex.ru
portal.mail.ru
e.mail.ru
morena.ru
top-fwz1.mail.ru
ad.mail.ru
static-asm.secure.sky...
static.asm.skype.com
avatars.mds.yandex....
yastatic.net
bar.love.mail.ru
yandex.ru
ok.ru
an.yandex.ru
r.mradx.net
mail.yandex.ru
counter.yadro.ru
www.tns-counter.ru
browser.pipe.aria.mi...
dest_port: Descending
443
25
993
13,000
465
5,228
9,443
5,223
SN TLS-BySubject

Результаты работы suricata в сети

1. **Обнаруженные угрозы**
   - Несколько пропущенных вирусов
   - Обнаружено нецелевое использование ресурсов сети интернет
   - Обнаружено ПО отправляющее логины и пароли без шифрования
   - Заблокированы торренты
   - Заблокирован teamveawer
   - Заблокированы различные сканеры портов

2. **Оптимизация firewall**

Общие рекомендации по внедрению и проблемы

1. После установки системы ее не стоит включать сразу в боевом режиме
2. Стоит запустить детектирование угроз локальной сети на отдельной группе устройств
3. Возможны ошибочные срабатывания правил
4. Добавлять белые списки возможно в исключениях правил mikrotik firewall или в suricata rules
5. Обязательно делайте белые списки – ip адреса gateway, адреса различных поставщиков услуг и тд
6. Система не должна ломать работы чего либо в сети – если это не так, то отключаем блокировки и разбираемся в чем дело
7. Периодически стоит проверять работу системы

MikroTik

БЕСПЛАТНЫЙ ВЕБИНАР

НАСТРОЙКА SURICATA + MIKROTIK

3 октября **в 11:00**

СРЕДА

СПАСИБО ЗА ВНИМАНИЕ

Приходите на наши курсы по Mikrotik и Asterisk