

# New Generation SIEM

## Solution Development

# Big Picture of Solution





# Indicator of Compromise Collector

## **Solution/Service Title**

Indicator of Compromise Collector

## **Client Industry**

Information System Security

## **Client Challenge**

Providing their service on monitoring end-client infrastructure, it's needed to have fast, reliable and easy-to-use solution which helps to collect, pre-process and forward logs for further analysis

## **Scope**

Scripts for collecting various indicators of compromise for Windows, Linux, MacOS

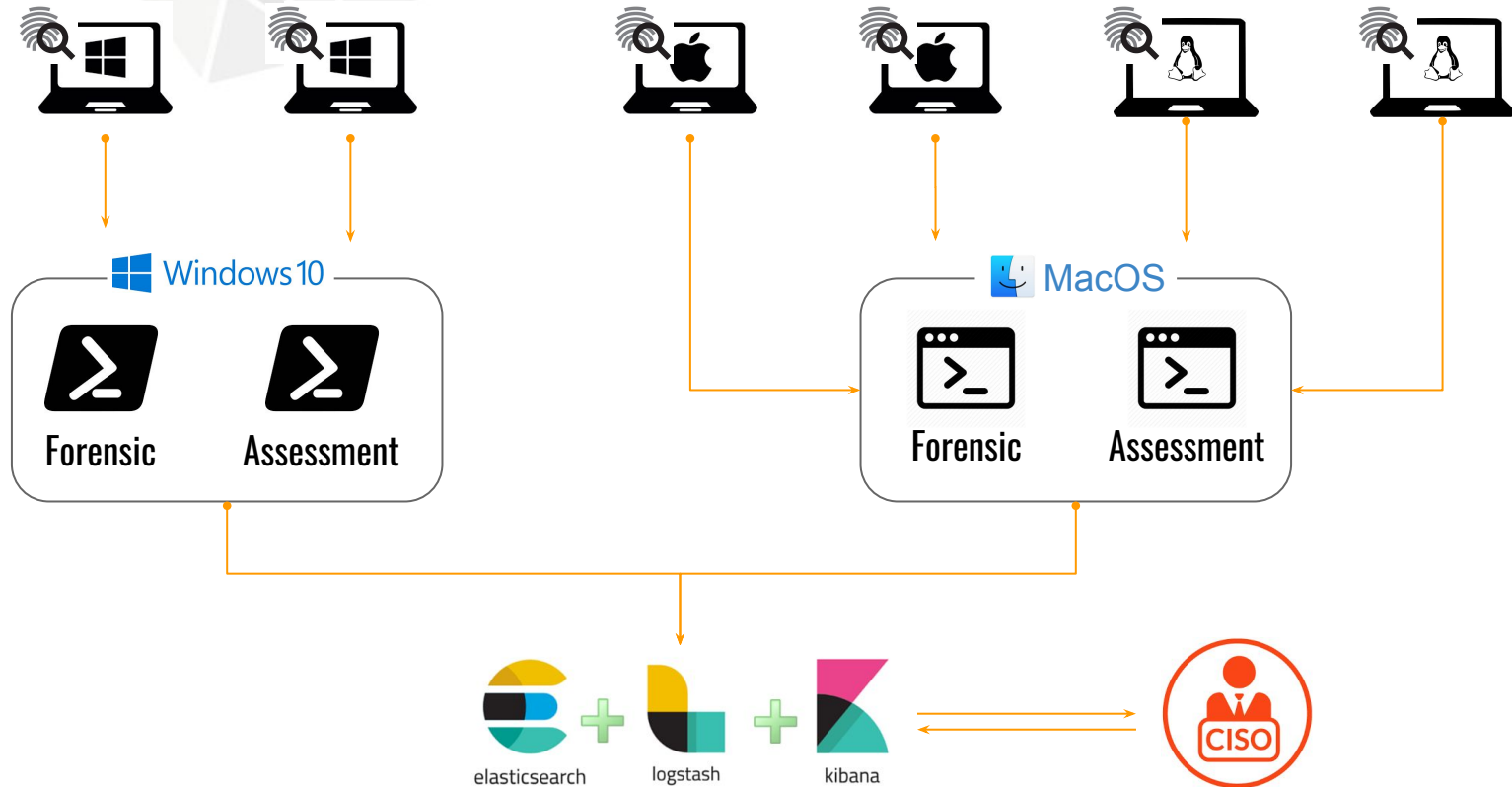
## **Key Benefits**

Automation of manual check for indicators of compromise, assessment of various systems. Unified data model, to further processing in ELK

## **Results**

Fast, portable, crossversion scripts for 3 most widespread systems (Linux, MacOS, Windows). Full coverage for most compromised attack surfaces, accordingly to mitre att&ck

# IoC Collector Architecture



# IoC Collector Technologies



PowerShell

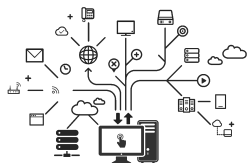


**BASH**  
THE BOURNE-AGAIN SHELL

  
**ziften**

# Workload time distribution

25%



## Configuration assessment

Assessment of various mostly misconfigured system services. Creating of widespread system-view for subsequent analyse and improve of system security

- Microsoft Windows
- PowerShell
- Linux
- MacOS
- Bash

65%



## Forensic assessment

Indicators of compromise collection automation. Used in system that are suspected to be compromised. Build on top of common security knowledge model ATT&CK Matrix.

- Microsoft Windows
- PowerShell
- Linux
- MacOS
- Bash

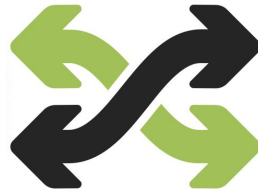
10%



## Logs analysis on ELK

Automation and visualization of various data sources. Processing and anomaly detection.

- ElasticSearch
- Logstash
- Kibana



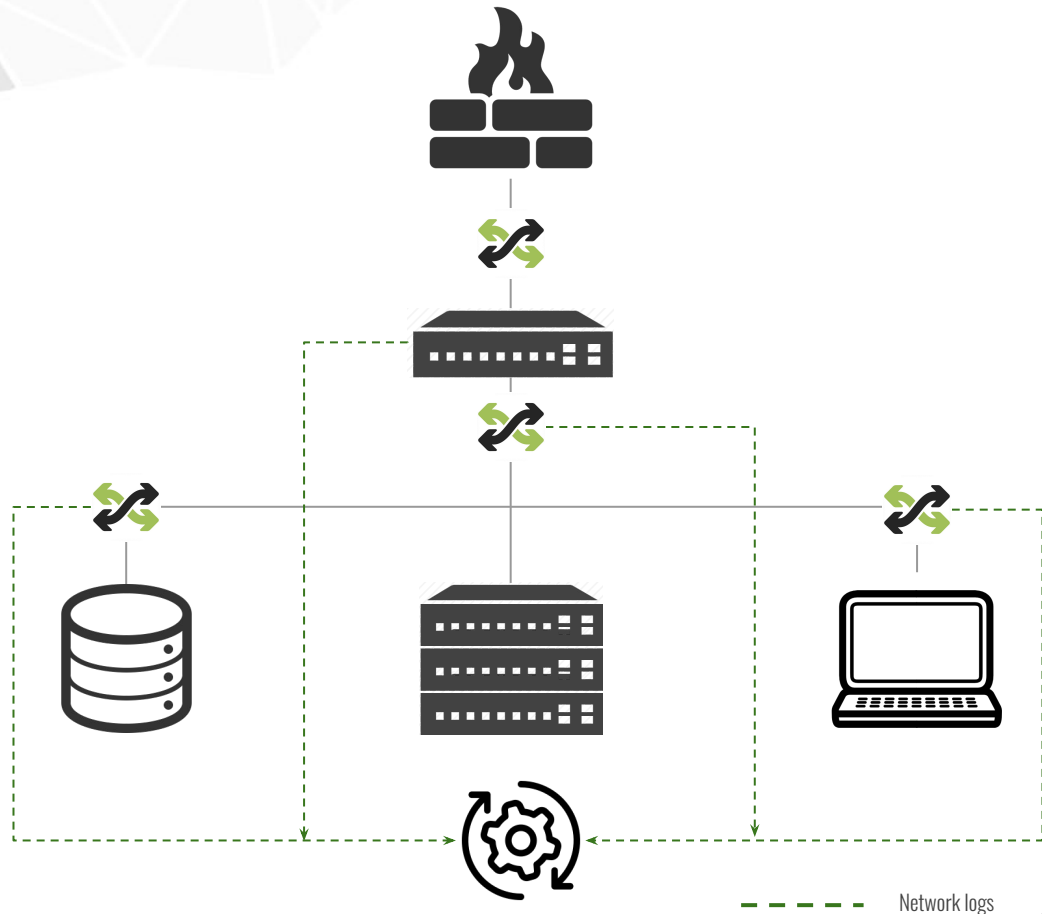
**IDS Forwarder**



# IDS Forwarder Architecture

**IDS Forwarder** solution is supposed to preprocess and forward network-based intrusion detection systems logs

It's a **custom** solution designed for company's clients needs, instead of using 3d-party product, developed for different purposes and platforms.



# IDS Forwarder Solution

## Preprocessing:

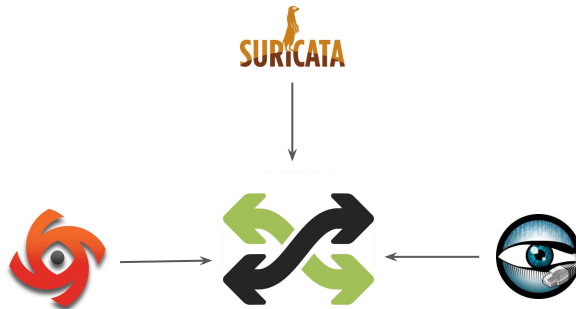
1. Pull network logs from installed IDS: Suricata, Bro, Ossec
2. Transform logs into unified data model
3. Export unified data into json format

## Fault-tolerance:

1. Sys-v daemon on system start-up
2. Custom watchdog
3. Broad, multiple level rotatable logging system

## Assessment:

1. Create taxonomy for rules using statistical natural language processing
2. Evaluate group threat level using internal security knowledge model
3. Create general assessment model for all IDS



# IDS Forwarder Technologies



elasticsearch



logstash



kibana





# Event Tracking System

## **Solution/Service Title**

Event Tracking System

## **Client Industry**

Information System Security

## **Client Overview**

US MSSP, a cyber security advisory and operations concern comprised of some of the world's most knowledgeable cyber experts.

## **Client Challenge**

Event Tracking System is a event management solution for tracking and acting upon different system incidents. The current state of the system was first built as a proof of concept and has outgrown its limited shell. It was decided to transfer ETS into a set of frameworks that will ensure ease of collaborative development in the system's future.

## **Scope**

SIEM, Events Tracking, CISO, API

## **Key Benefits**

Same technology stack, easy 3d party integration, collaborative development, designed "by the analyst for the analyst"

## **Results**

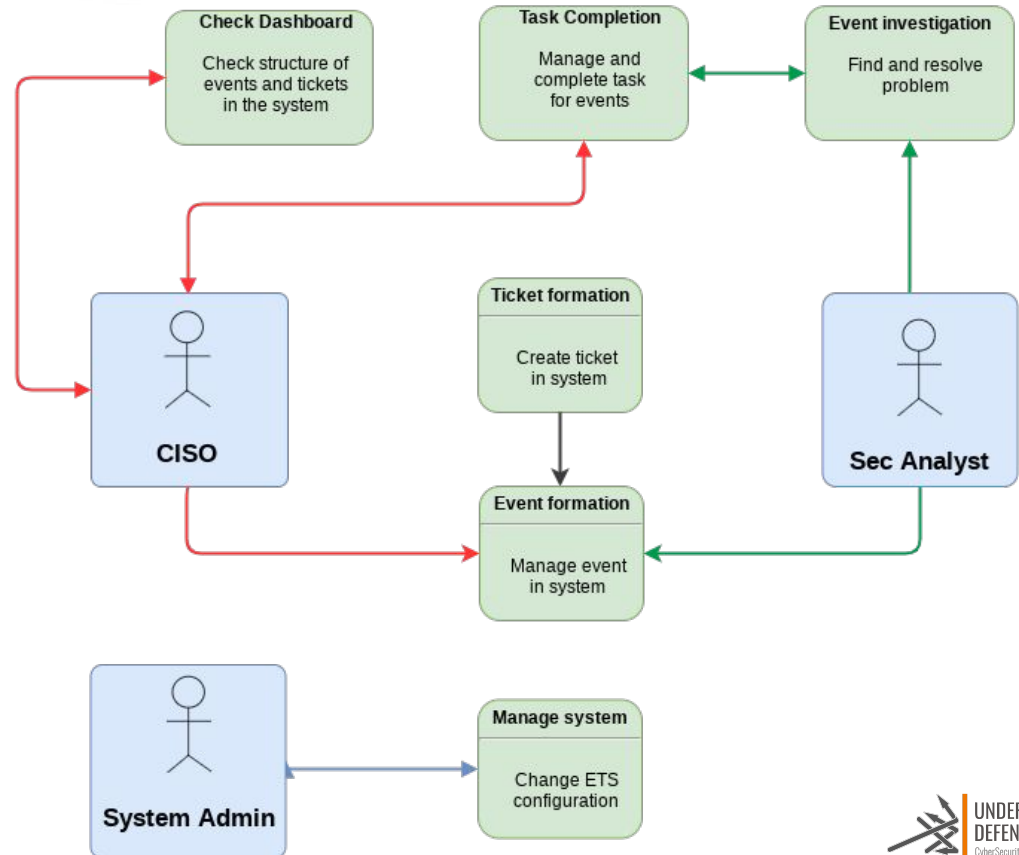
Redesigned and delivered main parts of MVP with using new technologies stack. New UI/UX implemented from the scratch.

# ETS general workflow

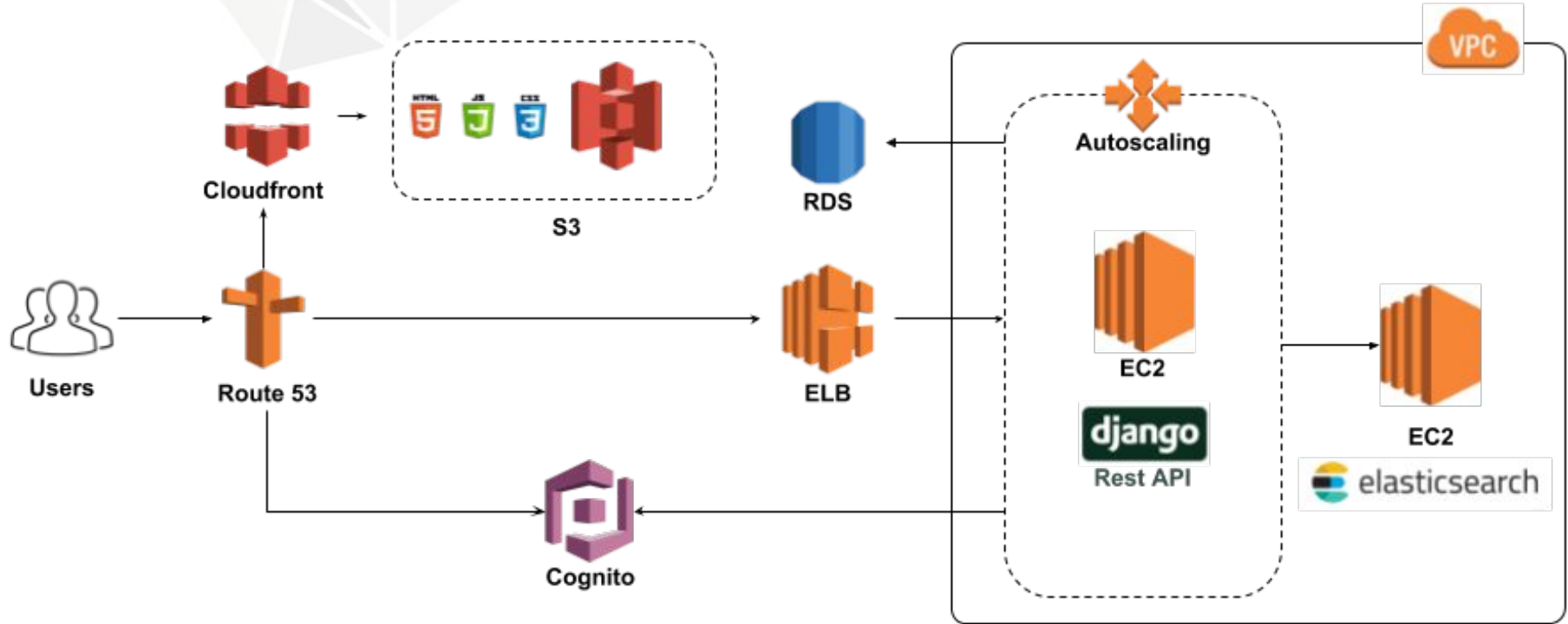
**Event Tracking System** is a customly designed security incidents and event management system which helps to gather, process, analyze and forward to response team security incidents happened within host network.

**ETS** is used by CISO, Security Analyst and System Administrator as a main tool for managing security events within the company.

Event Tracking System - Use Case Diagram



# ETS redesigned infrastructure



Event Tracking System

← → ↺

Not Secure

192.168.100.119:1234/events

☆

ABP

G

26

i

Home

Tickets

Events

Investigation

Playbook

Database

Filter

ITy

Create new event

Id	Title	Organization	Status	Type	Severity	Outcome	Analyst Update	Customer Update ↑	Owner
75	Example Title	CyberSecurITy	In Progress	Backdoor	Info	Resolved	Thu Feb 05 2015 14:42:02 GMT+0200 (EET)	Fri Jul 06 2012 16:00:23 GMT+0300 (EEST)	ETS
66	Example Title	CyberSecurITy	In Progress	Denial of Service	Low	Benign	Tue Feb 09 2016 10:31:19 GMT+0200 (EET)	Thu Mar 14 2013 20:58:15 GMT+0200 (EET)	ETS
99	Example Title	CyberSecurITy	In Progress	Denial of Service	Low	Benign	Fri Jan 06 2012 02:04:55 GMT+0200 (EET)	Wed Mar 27 2013 14:28:28 GMT+0200 (EET)	IYUROCH
61	Example Title	CyberSecurITy	Resolved	Denial of Service	High	Benign	Fri Jan 09 2015 17:42:33 GMT+0200 (EET)	Wed Oct 02 2013 16:24:38 GMT+0300 (EEST)	IYUROCH
15	Example Title	CyberSecurITy	In Progress	Exfiltration	Info	Resolved	Sun Feb 19 2012 07:58:07 GMT+0200 (EET)	Fri Feb 21 2014 19:43:08 GMT+0200 (EET)	SYSTEM

Items per page: 5

1 - 5 of 25

<

>

1 - 5 of 25



# ETS redesigned interface

Home

Tickets

Events

Investigation

Playbook

Database

Filter

Create new ticket

Create new Ticket

Organization

Category

Status

Merge Into Event

Title

Description

Owner

2018-09-05 11:26 AM

☐ Send email notification

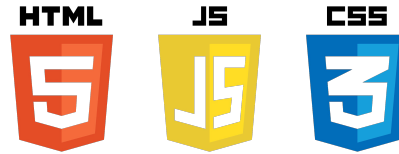
Cancel

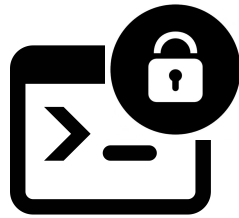
Save Ticket

Title	Organization	Status	Owner	Merged with
1		Resolved	IYUROCH	roman
2	UnderDefense	In Progress	SYSTEM	vitalik
1	CyberSecuriTy	On Hold	SYSTEM	roman
3	ETS	In Progress	ETS	NONE
1	CyberSecuriTy	On Hold	IYUROCH	NONE
3	UnderDefense	On Hold	IYUROCH	NONE
3	ETS	On Hold	SYSTEM	vitalik
2		In Progress	ETS	NONE
1		Resolved	SYSTEM	vitalik
2	CyberSecuriTy	On Hold	SYSTEM	vitalik
2	UnderDefense	On Hold	SYSTEM	vitalik
1	CyberSecuriTy	In Progress	ETS	vitalik
3		Resolved	ETS	NONE

	Denial of Service	2018-08-03 21:30 PM			
	Exfiltration	2018-07-28 22:28 PM			

# ETS Technologies





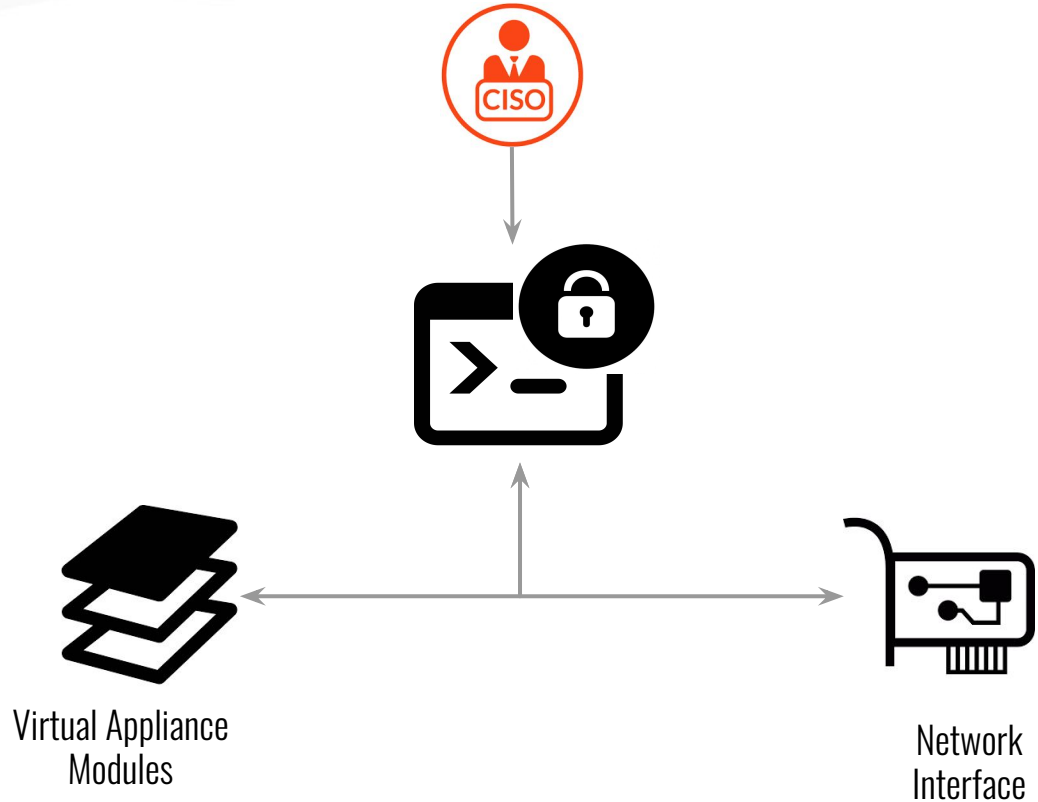
# Restricted Shell

# Restricted Shell Architecture

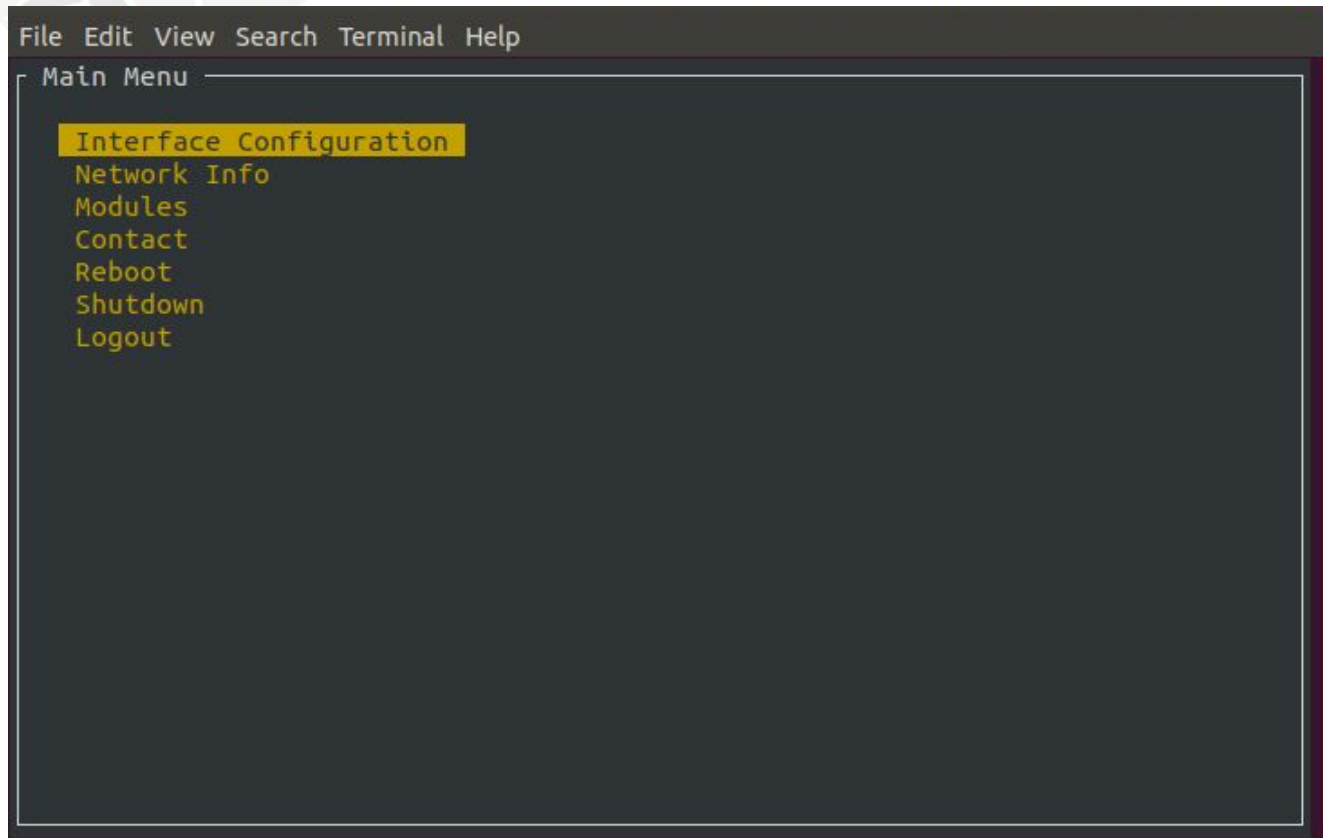
**Restricted Shell** is a terminal user interface for setting up, controlling and auditing system tools (networking) and installed modules.

**CISO** as well as security analyst will use restricted shell for running modules on-demand and testing correctness of system setup.

**Virtual Appliance** comes with **Restricted Shell** decreasing mental load for system administrators to make their life easier and more effective



# Restricted Shell UI



# Restricted Shell Technologies



**CentOS**



systemd



# Virtual Appliance

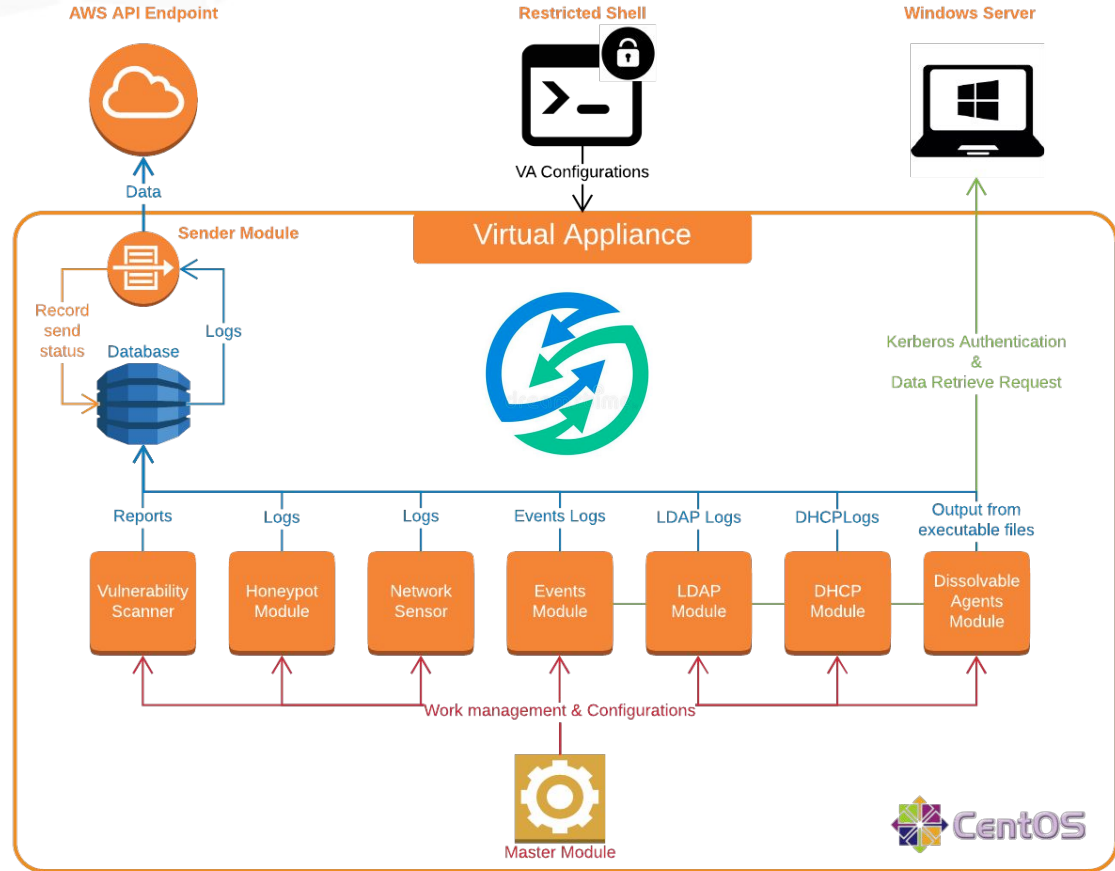
# Virtual Appliance architecture

**Virtual Appliance** is a toolset of a modules build upon **Linux CentOS** distro which might be deployed in any part of the client's network.

Configuration management is performed remotely using **Restricted Shell** app.

Connection to Windows Server established via authentication protocol **Kerberos**.

Collected network data is stored on **AWS** for further analysis by client CISOs.





# Virtual Appliance Modules

## Vulnerability Scanner

Scan network for known vulnerabilities using custom signature database

## Honeypot Module

Collect high-value data about intruders through the detection of their attempt of network recon

## Network Sensor Module

Analyze network traffic for anomalies using rule-based IDS mechanism

## Events Module

Scheduled query of specific Windows Events on Windows Server

## LDAP Module

Collect data from Active Directory related to User, User Group and PC.

## DHCP Module

Pull DHCP log from the Windows Server, convert it to JSON and save to DB

## Dissolvable Agents Module

Run agents on remote host to retrieve data available only for privileged users



Possibility to add any other modules “on the fly” for extra functionality

# Virtual Appliance technologies



# Business goals reached

**Cost efficiency**



**Customer satisfaction**



+

**Brand awareness**



**Automatization**



- Reduced operating costs using custom build SIEM
- Delivered constant excellence to clients
- Automated CISO daily routine tasks
- Developed brand awareness contributing in Open Source

# Strategic recommendations



Prepare Virtual Appliance solution to enterprise and distribute it in freemium model



Develop Event Tracking System as an Anti-SIEM “from analytics for analytics”



Establish Secure Development Lifecycle best practices



Extend client security expert Team using 3d party partnership

# Thank you!

**Call us now at +1 929 999 5101**