OOTB.NET

Architecting Security Onion for Enterprise Resilience

A Case Study in Scaling Open-Source SIEM for High-Performance Threat Detection

Korrawit Chaikangwan
Peerapong Thongpubet
Piroon Srisawang

JiTech Company Limited
บริษัท ไจเทค จำกัด

Out of The Box, Bangkok
20 - 21 August, 2025

$ /usr/bin/whoami

OOTB.NET

- A group of researchers spun off from a research lab to develop a high-performance product, leveraging our expertise in open-source software
- Initial focus was on creating high-performance firewalls and filtering solutions, which led us to then develop monitoring solutions
- Over the past several years, we have pivoted to specializing in high-performance security products, specifically log collectors and SIEMs

$ /usr/bin/whoami

OOTB.NET

DPDK
DATA PLANE DEVELOPMENT KIT

eBPF

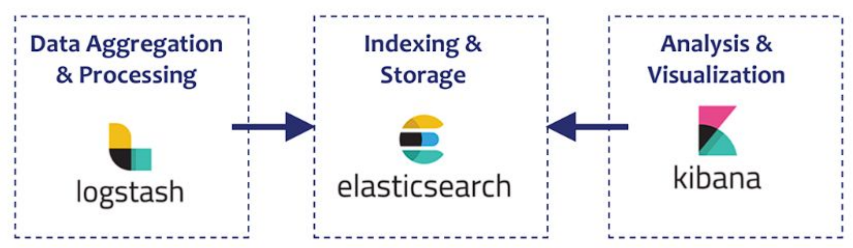
FAST NETMON

BIRD

ORY

KVM

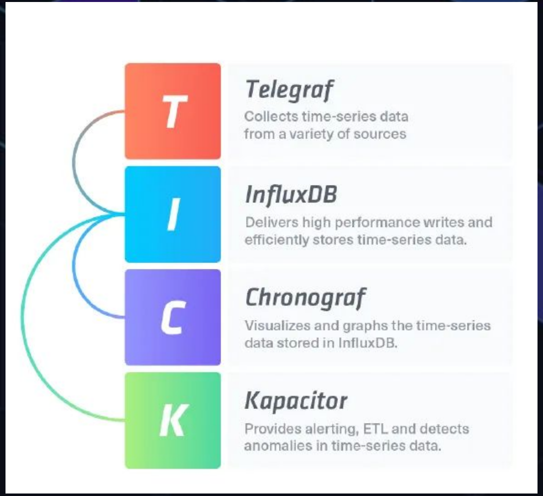
SURICATA®



Data Aggregation & Processing
logstash

Indexing & Storage
elasticsearch

Analysis & Visualization
kibana



T Telegraf
Collects time-series data from a variety of sources

I InfluxDB
Delivers high performance writes and efficiently stores time-series data.

C Chronograf
Visualizes and graphs the time-series data stored in InfluxDB.

K Kapacitor
Provides alerting, ETL and detects anomalies in time-series data.

Security Onion

Grafana

Disclaimer

- The content of this presentation is based on our experience developing and implementing a Security Information and Event Management (SIEM) solution over the past year.
- The discussion is mostly from an engineering perspective, focusing on the technical purpose and implementation of the system.
- All data used in this presentation is for illustrative purposes only. This is a case study of our implementation, not a discussion of real-world data or live events.
- The views and opinions expressed in this presentation are our own and do not necessarily reflect the official policy or position of our company.
- This presentation is for informational purposes only and should not be considered as professional advice or a definitive guide to implementing a SIEM.

Agenda

OOTB.NET

- Why Open-Source SIEM in Enterprise?
- Security Onion Overview
- Custom Enhancements & Solutions
  - Multi-Tenancy
  - Single Sign On
  - Centralized Detection Rule Management
  - High-volume Ingestion
- Ongoing Challenges
  - Threat Intelligence Management Feature Support
  - Version Compatibility & Maintenance Overhead
- Summary
- Key Takeaways

Why Open-Source SIEM?

OOTB.NET

- Cost-Effectiveness
- Flexibility & Customization
- Transparency
- Community Support
- Scalability

Why Open-Source SIEM?

- Cost-Effectiveness
  - Significantly lower licensing costs compared to commercial SIEMs
- Flexibility & Customization
- Transparency
- Community Support
- Scalability

OOTB.NET

Why Open-Source SIEM?

- Cost-Effectiveness
- Flexibility & Customization
    - Adaptable to specific organizational needs, avoiding vendor lock-in
- Transparency
- Community Support
- Scalability

Why Open-Source SIEM?

OOTB.NET

- Cost-Effectiveness
- Flexibility & Customization
- Transparency
    - Ability to inspect source code enhances security confidence
- Community Support
- Scalability

Why Open-Source SIEM?

OOTB.NET

- Cost-Effectiveness
- Flexibility & Customization
- Transparency
- Community Support
  - Global community of developers and users
  - Rapid development and troubleshooting
- Scalability

Why Open-Source SIEM?

- Cost-Effectiveness
- Flexibility & Customization
- Transparency
- Community Support
- Scalability
    - Easily scalable to accommodate data growth

OOTB.NET

Cons

- High Technical Expertise Required
- Lack of Dedicated Vendor Support
- Hidden Costs
- Limited Features and Functionality

Our Chosen Path

After evaluating various open-source SIEM solutions we've opted for *Security Onion* as our core platform

Disclaimer

- Some features are available in the paid Pro version, but we decided to focus on the open-source version to ensure cost-efficiency and adaptability
- The main development and customizations we're presenting are based on Security Onion version 2.3, a widely used version at the time of our work.
- This content is based on our own research and prototype development and is not directly affiliated with the core developers of the Security Onion project.

Security Onion

Why Security Onion?

Our decision to adopt Security Onion is driven by its core strengths.

And we'll explore the key advantages in the next two slides:

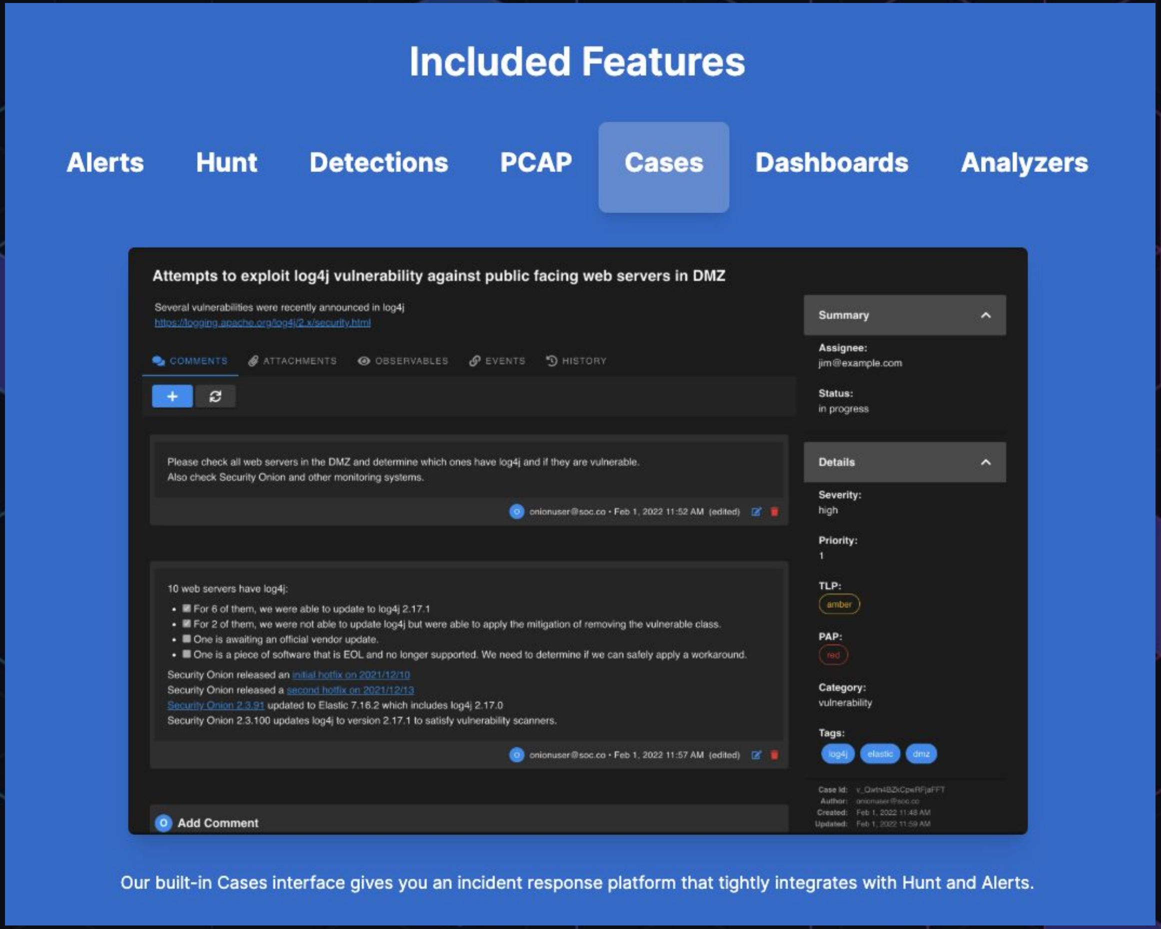
- All-in-One
- Practical and Community Power

Why Security Onion?

All-in-One

- Full Visibility
  - Network (NSM, IDS/IPS)
  - Host (EDR)
- Handle Cases with Ease
  - Create, track, and resolve incidents from the dashboard
- Log Management & Threat Hunting
- Analyst Tools & Built-in Rules

OOTB.NET



Included Features

Attempts to exploit log4j vulnerability against public facing web servers in DMZ

Several vulnerabilities were recently announced in log4j
https://logging.apache.org/log4j/2.x/security.html

Please check all web servers in the DMZ and determine which ones have log4j and if they are vulnerable.
Also check Security Onion and other monitoring systems.

onionuser@soc.co • Feb 1, 2022 11:52 AM (edited)

10 web servers have log4j:

- ☑ For 6 of them, we were able to update to log4j 2.17.1
- ☑ For 2 of them, we were not able to update log4j but were able to apply the mitigation of removing the vulnerable class.
- □ One is awaiting an official vendor update.
- □ One is a piece of software that is EOL and no longer supported. We need to determine if we can safely apply a workaround.

Security Onion released an initial hotfix on 2021/12/10
Security Onion released a second hotfix on 2021/12/13
Security Onion 2.3.91 updated to Elastic 7.16.2 which includes log4j 2.17.0
Security Onion 2.3.100 updates log4j to version 2.17.1 to satisfy vulnerability scanners.

onionuser@soc.co • Feb 1, 2022 11:57 AM (edited)

Summary

Assignee:
jim@example.com

Status:
in progress

Details

Severity:
high

Priority:
1

TLP:
amber

PAP:
red

Category:
vulnerability

Tags:
log4j elastic dmz

Case Id: v_Qwtn4BZkCpwRFjaFFT
Author: onionuser@soc.co
Created: Feb 1, 2022 11:48 AM
Updated: Feb 1, 2022 11:59 AM

Our built-in Cases interface gives you an incident response platform that tightly integrates with Hunt and Alerts.

Why Security Onion?

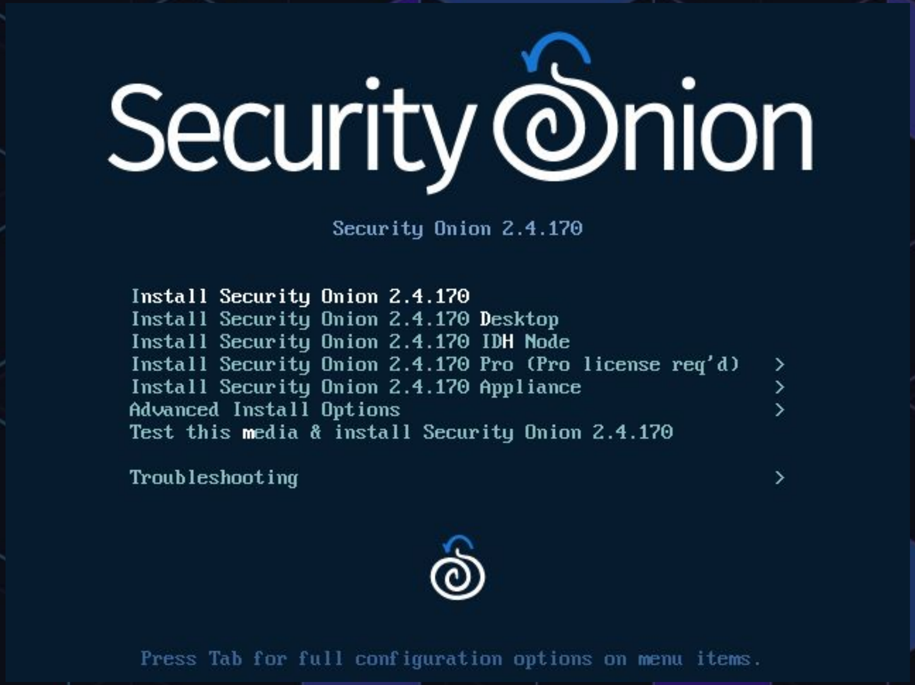
Practical and Community Power

- Easy Setup
- Scalability
- Strong Community
- Cost-Effective

Why Security Onion?

Practical and Community Power

- Easy Setup
  1. Install OS
  2. Config
  3. Use



Security Onion 2.4.170

```
Install Security Onion 2.4.170
Install Security Onion 2.4.170 Desktop
Install Security Onion 2.4.170 IDH Node
Install Security Onion 2.4.170 Pro (Pro license req'd)    >
Install Security Onion 2.4.170 Appliance                  >
Advanced Install Options                                  >
Test this media & install Security Onion 2.4.170

Troubleshooting                                           >
```

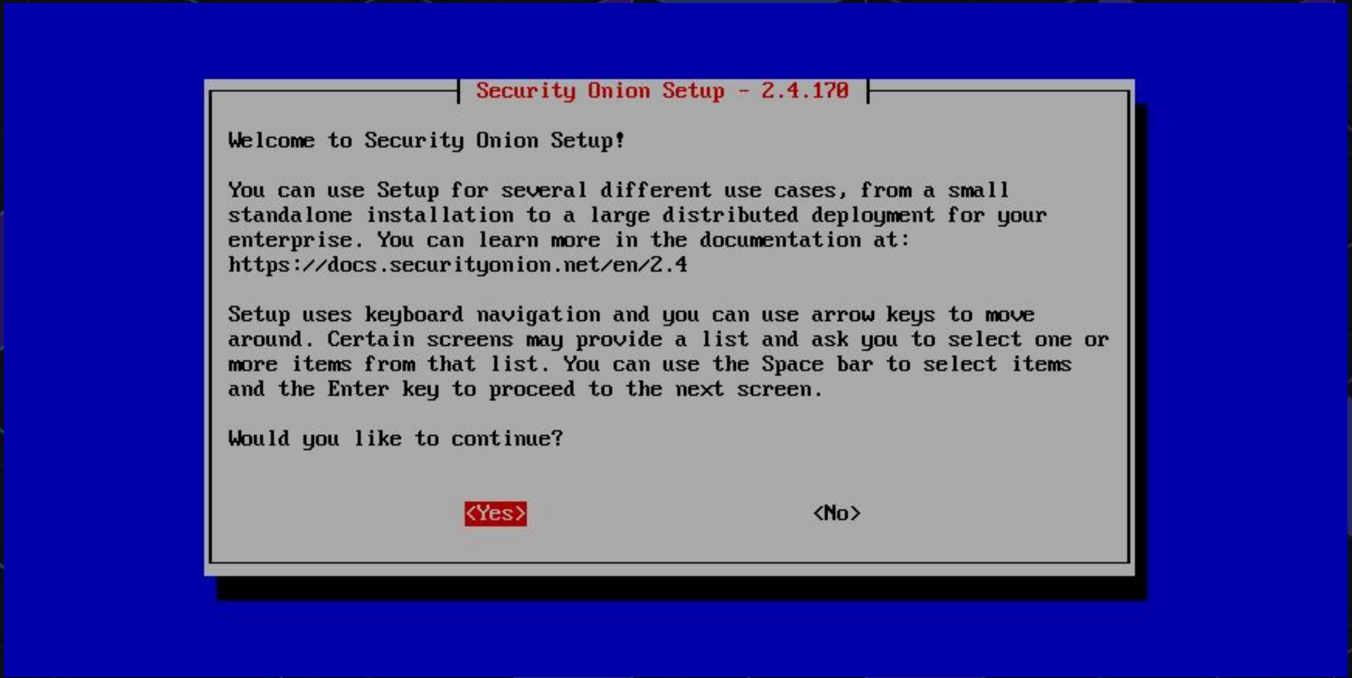
Press Tab for full configuration options on menu items.

Why Security Onion?

Practical and Community Power

OOTB.NET

- Easy Setup
  1. Install OS
  2. Config
  3. Use



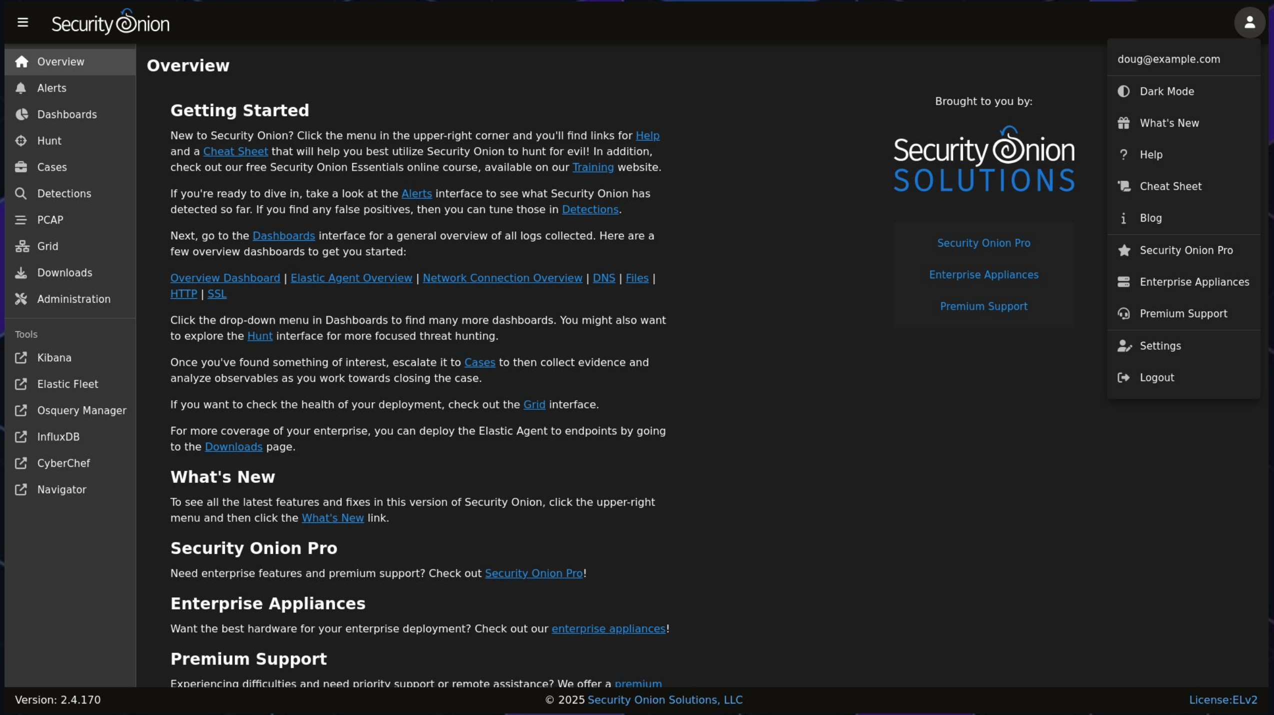
```
Security Onion Setup - 2.4.170

Welcome to Security Onion Setup!

You can use Setup for several different use cases, from a small
standalone installation to a large distributed deployment for your
enterprise. You can learn more in the documentation at:
https://docs.securityonion.net/en/2.4

Setup uses keyboard navigation and you can use arrow keys to move
around. Certain screens may provide a list and ask you to select one or
more items from that list. You can use the Space bar to select items
and the Enter key to proceed to the next screen.

Would you like to continue?
```

Why Security Onion?

Practical and Community Power

OOTB.NET

- Easy Setup
  1. Install OS
  2. Config
  3. Use



Overview

Getting Started

New to Security Onion? Click the menu in the upper-right corner and you'll find links for Help and a Cheat Sheet that will help you best utilize Security Onion to hunt for evil! In addition, check out our free Security Onion Essentials online course, available on our Training website.

If you're ready to dive in, take a look at the Alerts interface to see what Security Onion has detected so far. If you find any false positives, then you can tune those in Detections.

Next, go to the Dashboards interface for a general overview of all logs collected. Here are a few overview dashboards to get you started:

Overview Dashboard | Elastic Agent Overview | Network Connection Overview | DNS | Files | HTTP | SSL

Click the drop-down menu in Dashboards to find many more dashboards. You might also want to explore the Hunt interface for more focused threat hunting.

Once you've found something of interest, escalate it to Cases to then collect evidence and analyze observables as you work towards closing the case.

If you want to check the health of your deployment, check out the Grid interface.

For more coverage of your enterprise, you can deploy the Elastic Agent to endpoints by going to the Downloads page.

What's New

To see all the latest features and fixes in this version of Security Onion, click the upper-right menu and then click the What's New link.

Security Onion Pro

Need enterprise features and premium support? Check out Security Onion Pro!

Enterprise Appliances

Want the best hardware for your enterprise deployment? Check out our enterprise appliances!

Premium Support

Experiencing difficulties and need priority support or remote assistance? We offer a premium

Version: 2.4.170

© 2025 Security Onion Solutions, LLC

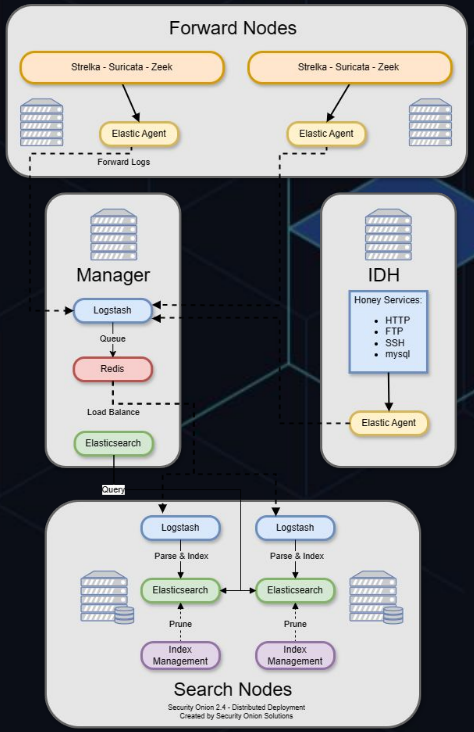
License:ELv2

Why Security Onion?

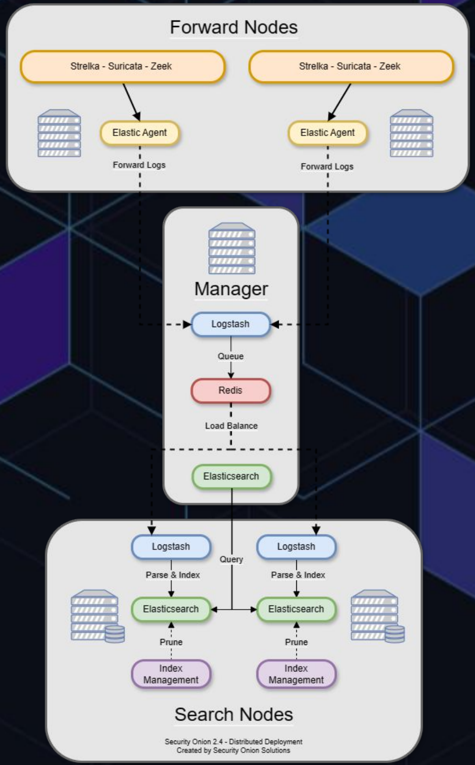
Practical and Community Power

OOTB.NET

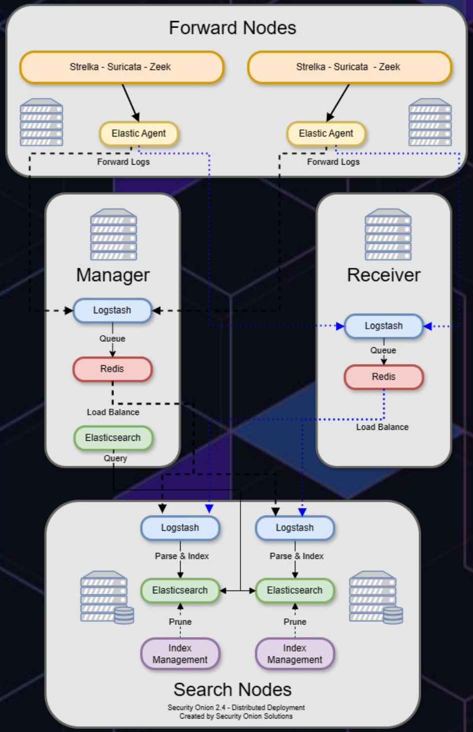
- Easy Setup
- Scalability: Support horizontal scaling



Security Onion 2.4 - Distributed Deployment
Created by Security Onion Solutions



Security Onion 2.4 - Distributed Deployment
Created by Security Onion Solutions



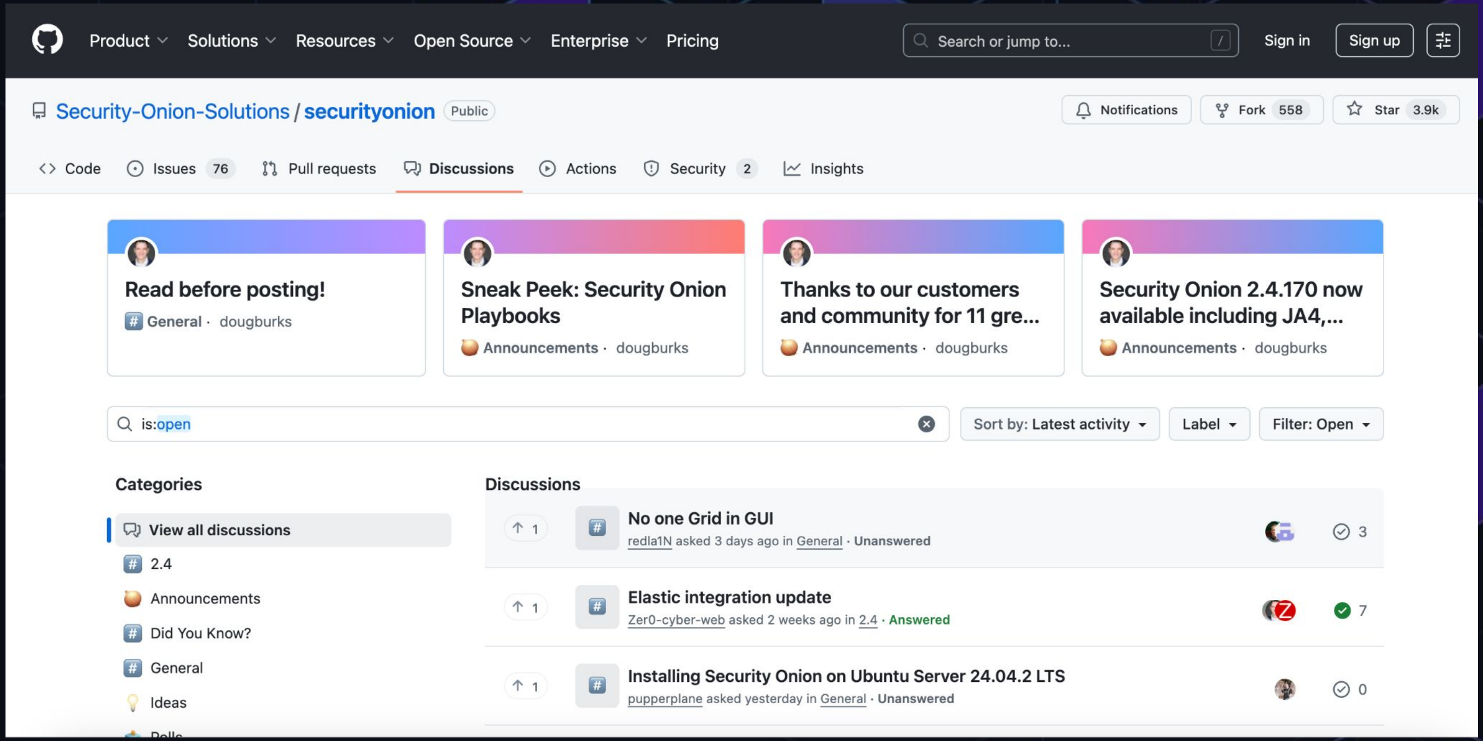
Security Onion 2.4 - Distributed Deployment
Created by Security Onion Solutions

Why Security Onion?

Practical and Community Power

OOTB.NET

- Easy Setup
- Scalability
- Strong Community: Active Dev & Support



Security-Onion-Solutions / securityonion Public

Read before posting!
General · dougburks

Sneak Peek: Security Onion Playbooks
Announcements · dougburks

Thanks to our customers and community for 11 gre...
Announcements · dougburks

Security Onion 2.4.170 now available including JA4,...
Announcements · dougburks

is:open

Categories

- View all discussions
- 2.4
- Announcements
- Did You Know?
- General
- Ideas
- Polls

Discussions

↑ 1	No one Grid in GUI redla1N asked 3 days ago in General · Unanswered	3
↑ 1	Elastic integration update Zer0-cyber-web asked 2 weeks ago in 2.4 · Answered	7
↑ 1	Installing Security Onion on Ubuntu Server 24.04.2 LTS pupperplane asked yesterday in General · Unanswered	0

Why Security Onion?

Practical and Community Power

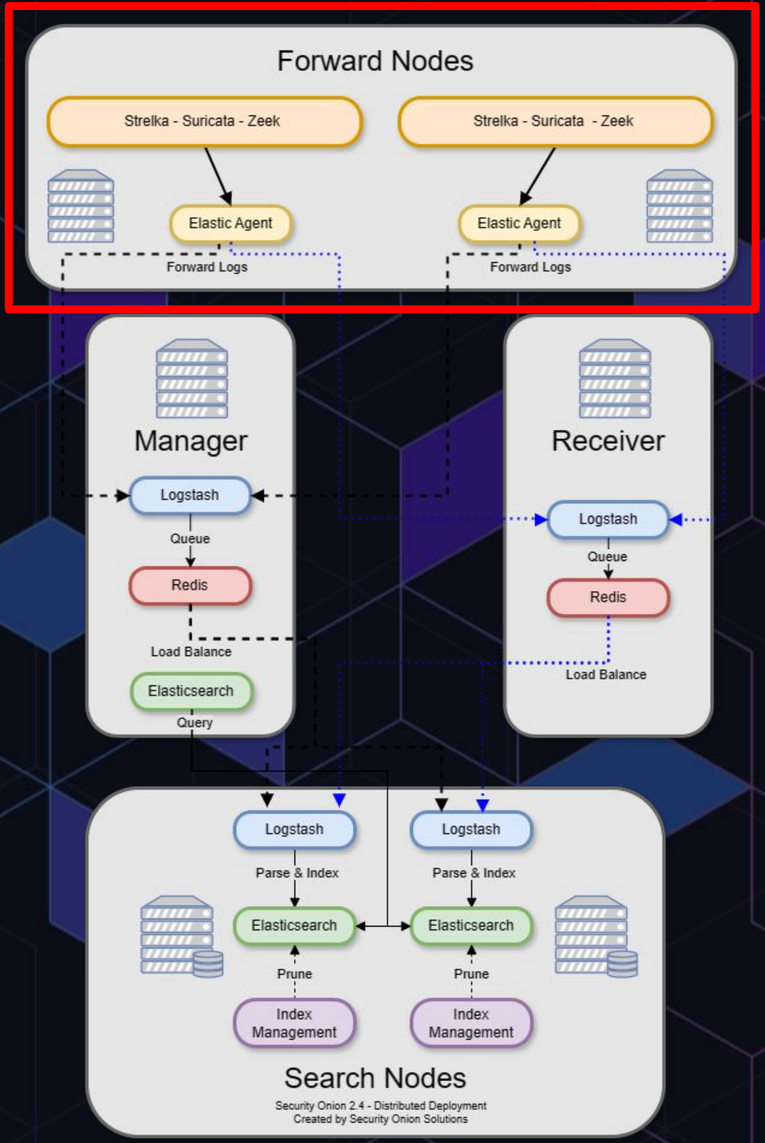
- Easy Setup
- Scalability
- Strong Community
- Cost-Effective: No License Fees

OOTB.NET

Open Source Behind Security Onion

Forward/Sensor Nodes

- Zeek
- Suricata
- Strelka
- Elastic Agent

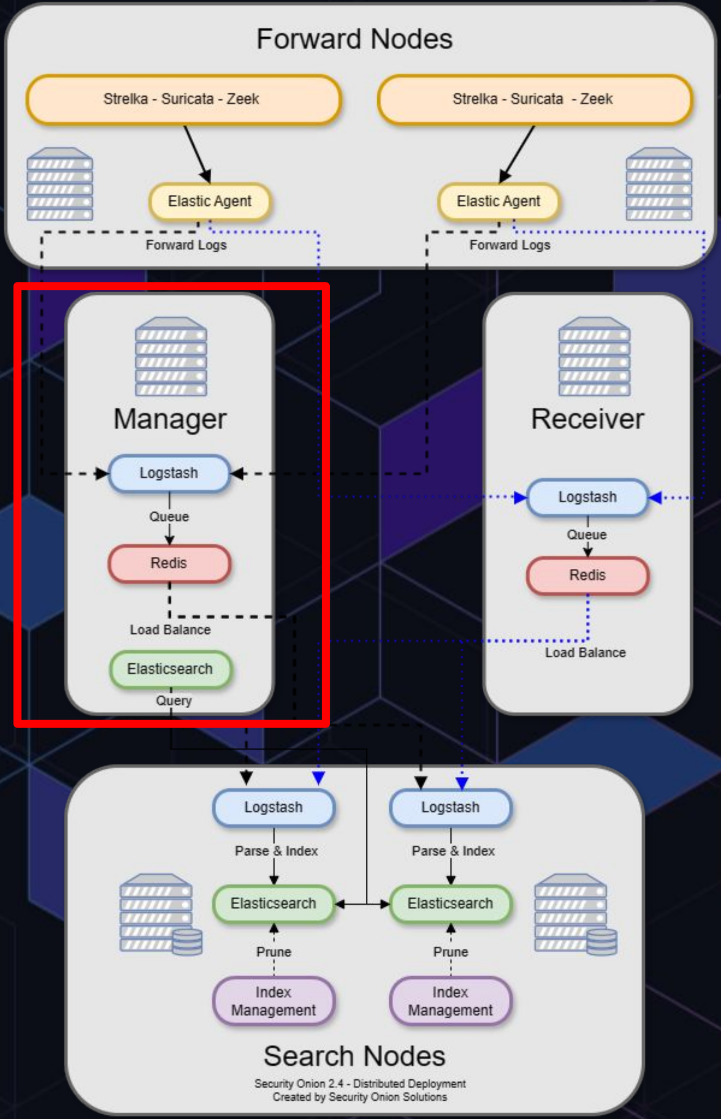


Security Onion 2.4 - Distributed Deployment
Created by Security Onion Solutions

Open Source Behind Security Onion

Manager Node

- Elasticsearch
- Logstash
- Kibana
- Redis
- InfluxDB

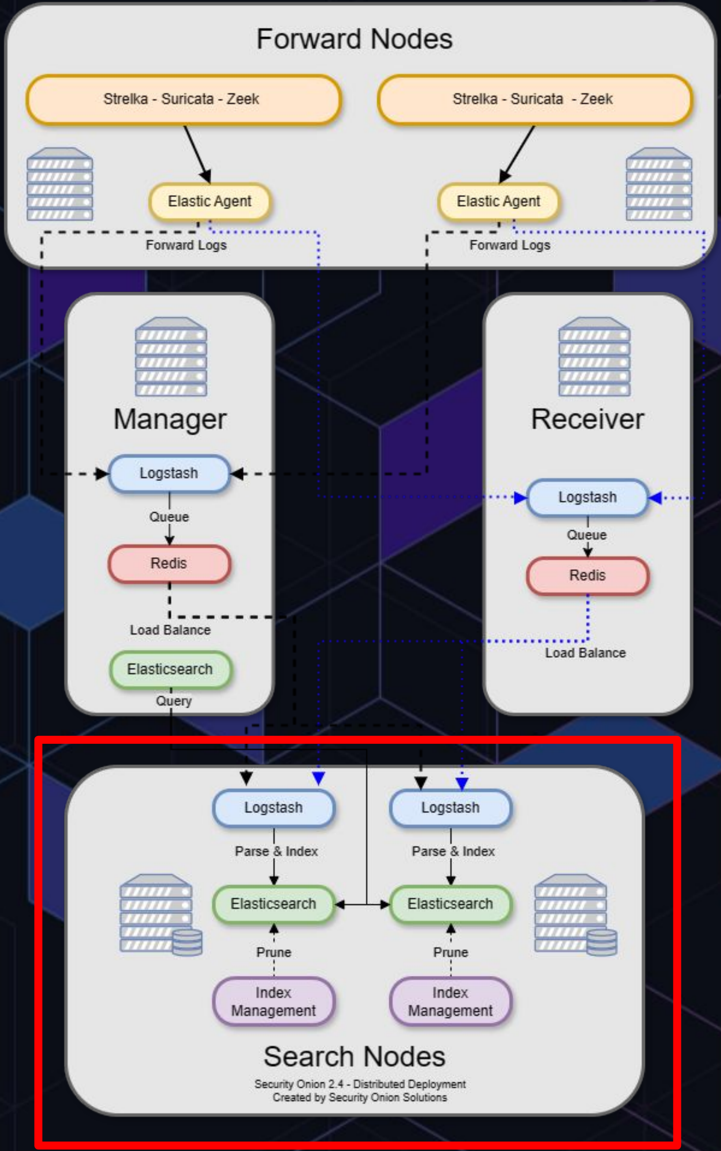


OOTB.NET

Open Source Behind Security Onion

Search Node

- Elasticsearch
- Logstash



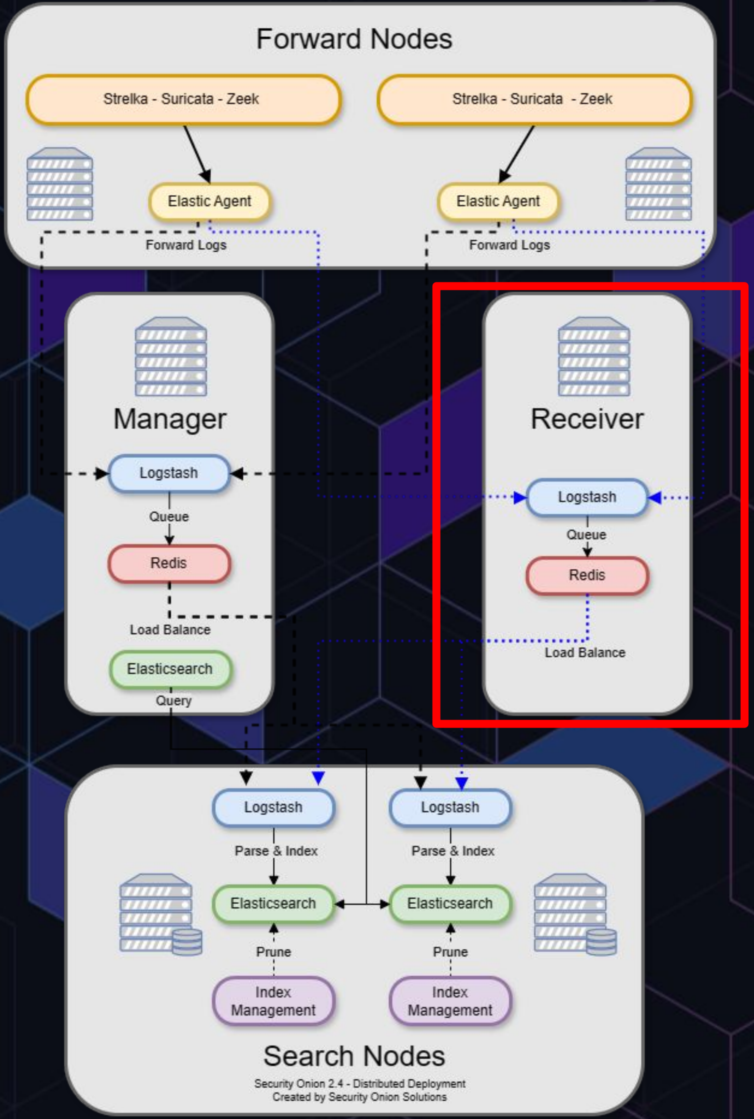
OOTB.NET

Open Source Behind Security Onion

OOTB.NET

Receiver node

- Logstash
- Redis



Beyond the Box

Addressing Enterprise Gaps

OOTB.NET

Even with powerful open-source tools like Security Onion enterprise environments often demand more

Enterprise gaps

limitation of Open Source Security Onion

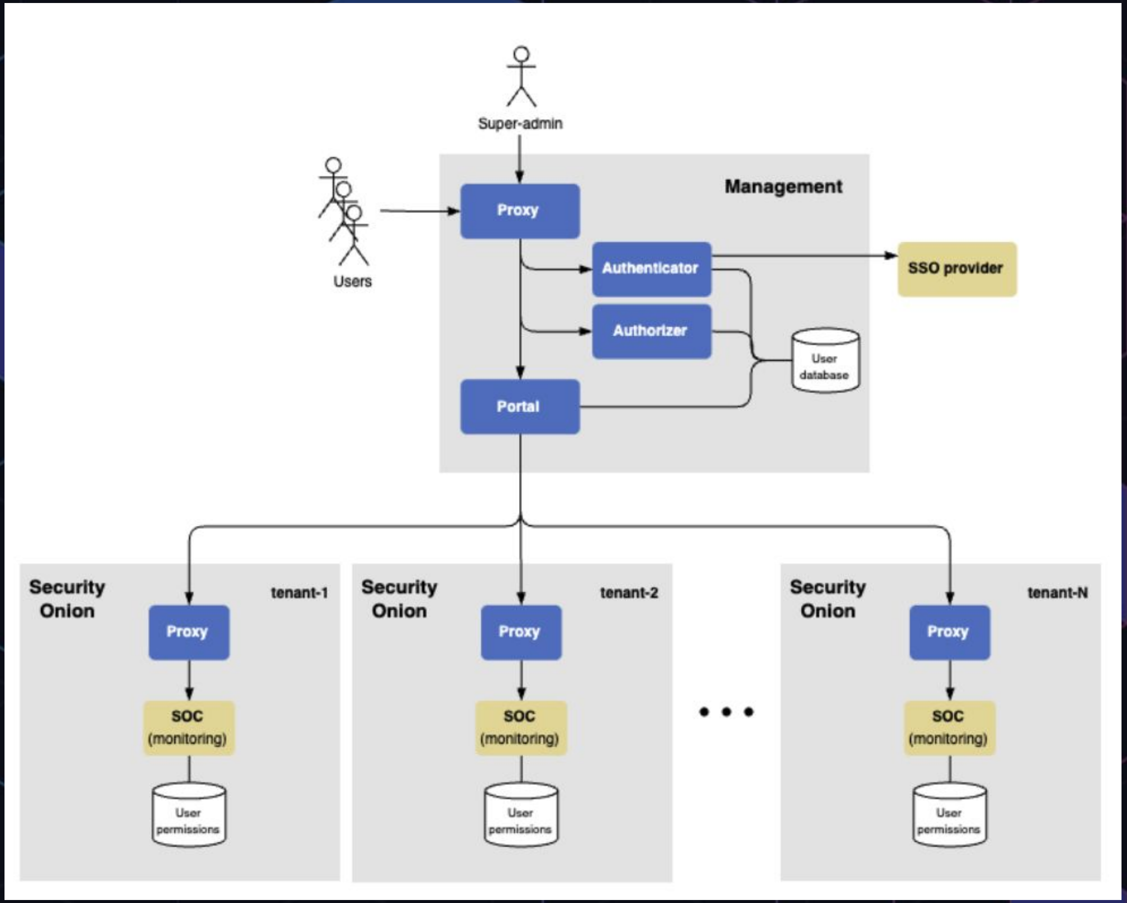
- Lacks native data isolation
- Lack of Centralized management support

OOTB.NET

Custom Enhancements & Solutions

OOTB.NET

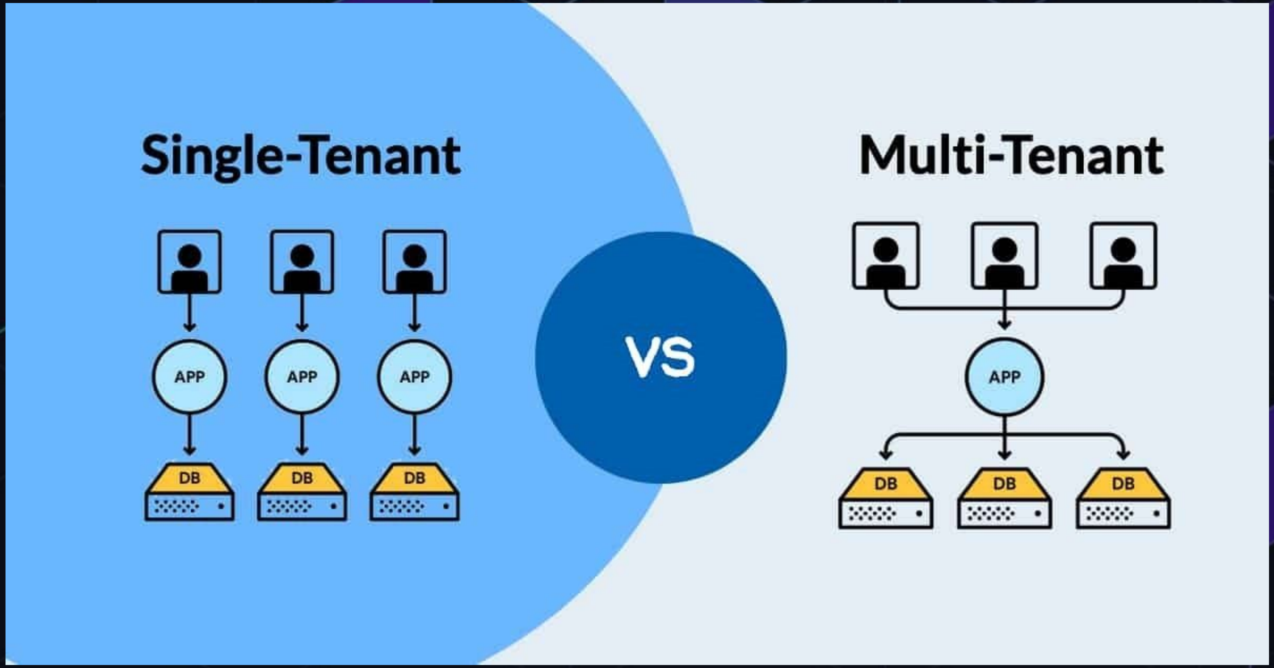
- Multi-Tenancy
- Single Sign On
- Centralized Rule Management
- High-Volume Log Ingestion



Multi-tenancy

Serving Multiple Customers with a Single System

- It is a single instance of software that serves multiple customers
- It uses a shared infrastructure while keeping data and resources for each customer separate



Multi-tenancy

The Problems We Faced

OOTB.NET

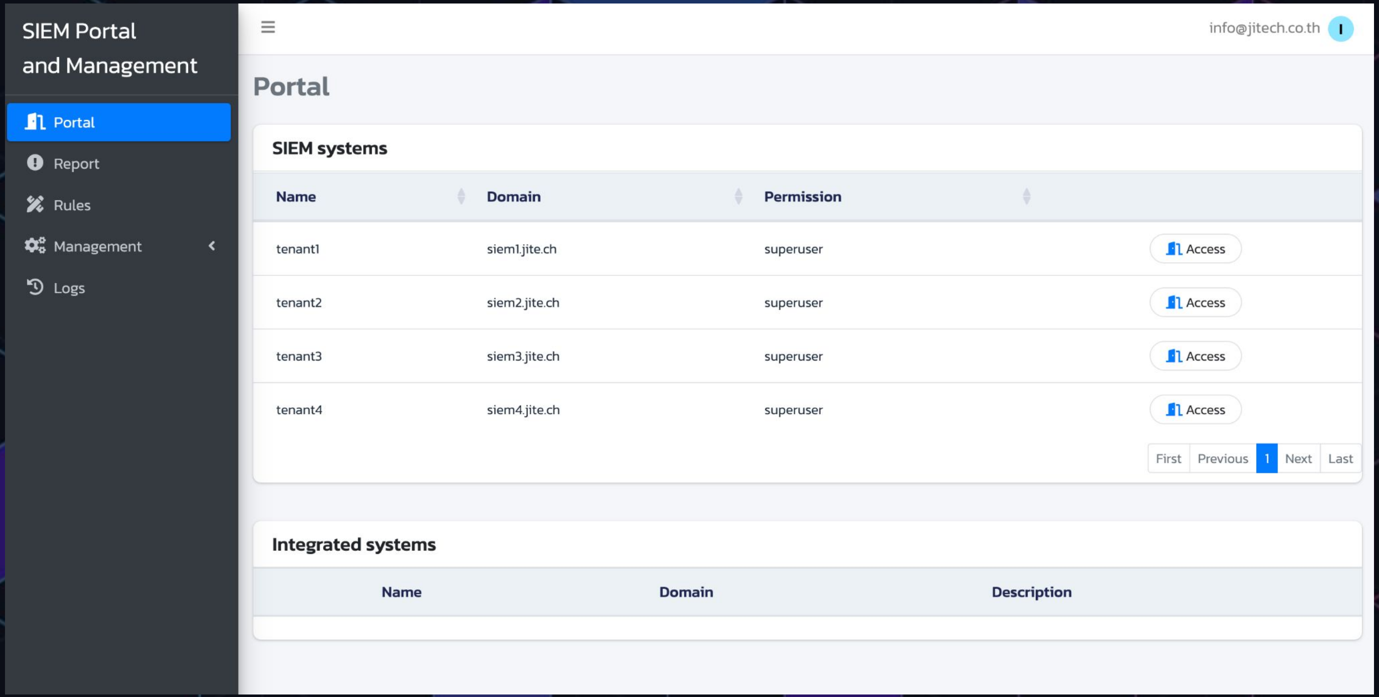
- Data from different clients is all in one place
- One client's data could be seen by another
- Running a separate system for each client wastes resources
- An issue with one client could cause problems for all others
- It's difficult to add resources for each client and keep it balanced.

Multi-tenancy

Our Solution

OOTB.NET

- Single Portal for All Tenants
- Easy Access
- Data Isolation
- RBAC Control



Portal

SIEM systems

Name	Domain	Permission	
tenant1	siem1.jite.ch	superuser	Access
tenant2	siem2.jite.ch	superuser	Access
tenant3	siem3.jite.ch	superuser	Access
tenant4	siem4.jite.ch	superuser	Access

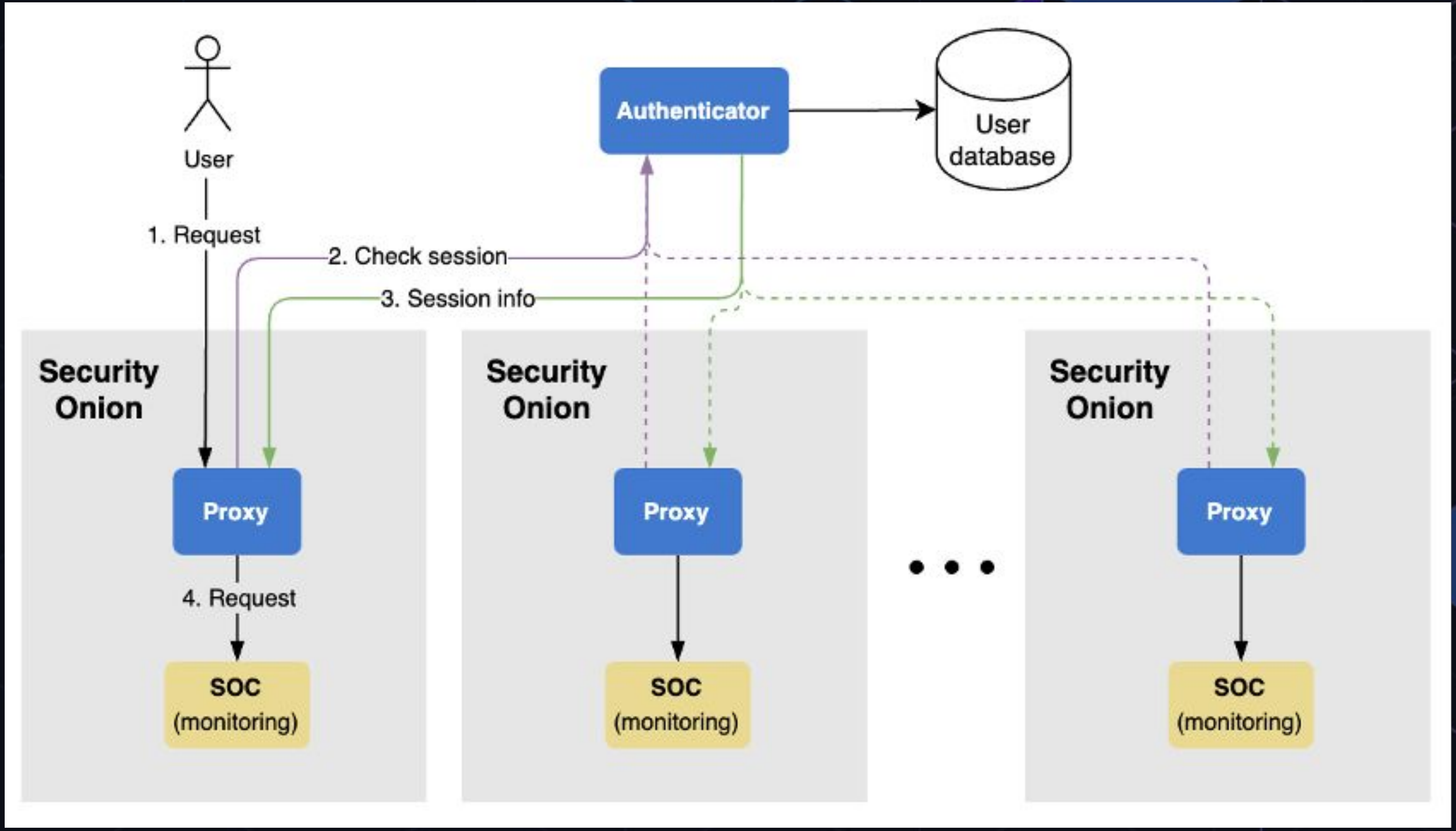
First Previous 1 Next Last

Integrated systems

Name	Domain	Description

Multi-tenancy

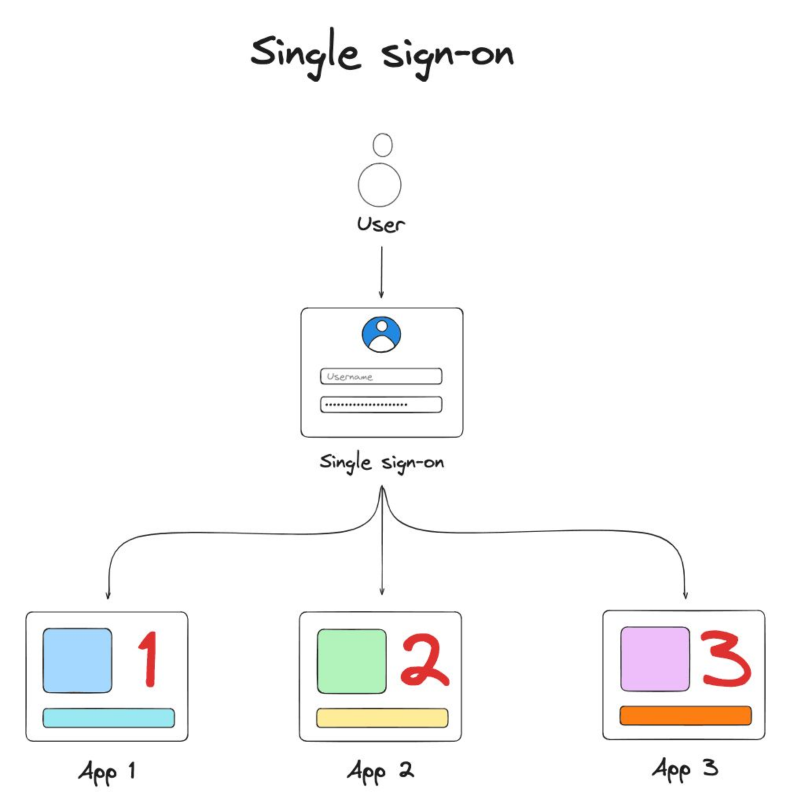
Our Solution (Technical Perspective)



Single Sign On

One Login for Many Systems

- Use one single login for multiple applications
- Log in to a central provider just once
- The provider confirms your identity and gives you access to other systems
- It also simplifies user management for IT teams



OOTB.NET

Single Sign On

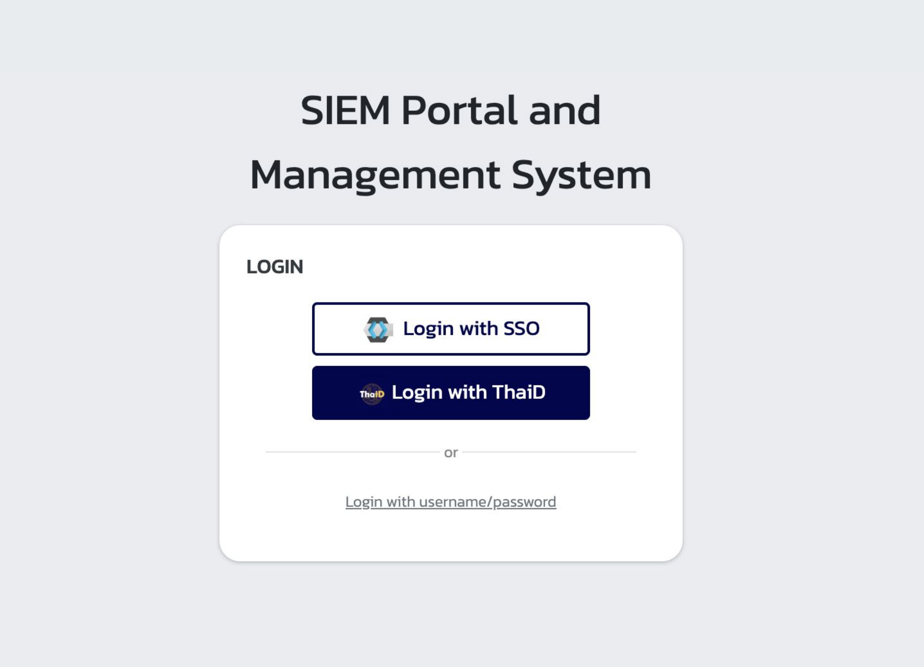
The Problems We Faced

- Each tenant required its own unique logins
- Users had to log in to multiple systems
- Too many accounts created a security risk
- We had to manually manage user accounts for each tenant
- There was no single place to manage all user permissions

Single Sign On

Our Solution

- One Login for All Tenants & Systems
- Easy Access & Efficiency
- Centralized User Management



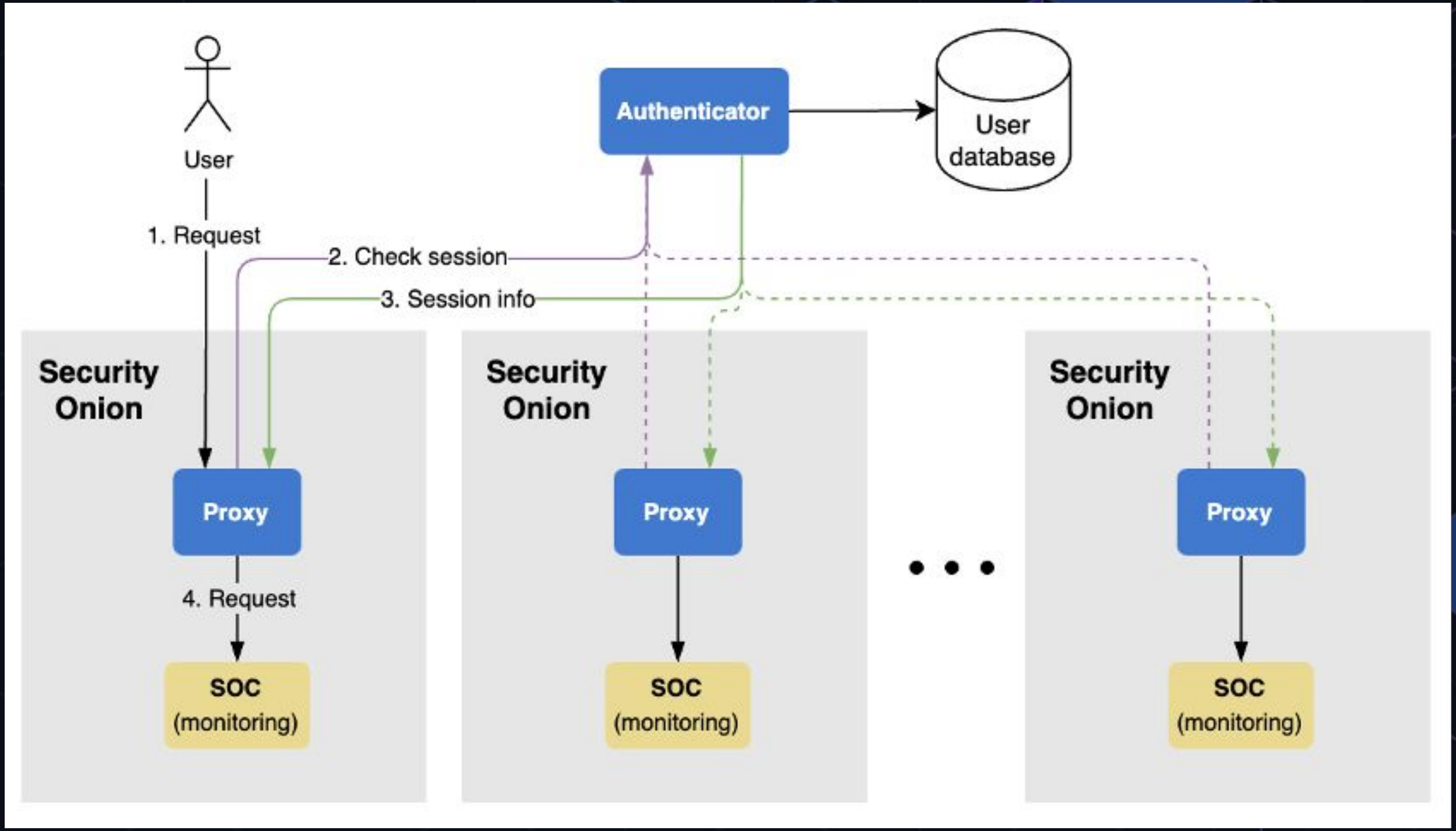
SIEM Portal and Management System

LOGIN

OOTB.NET

Single Sign On

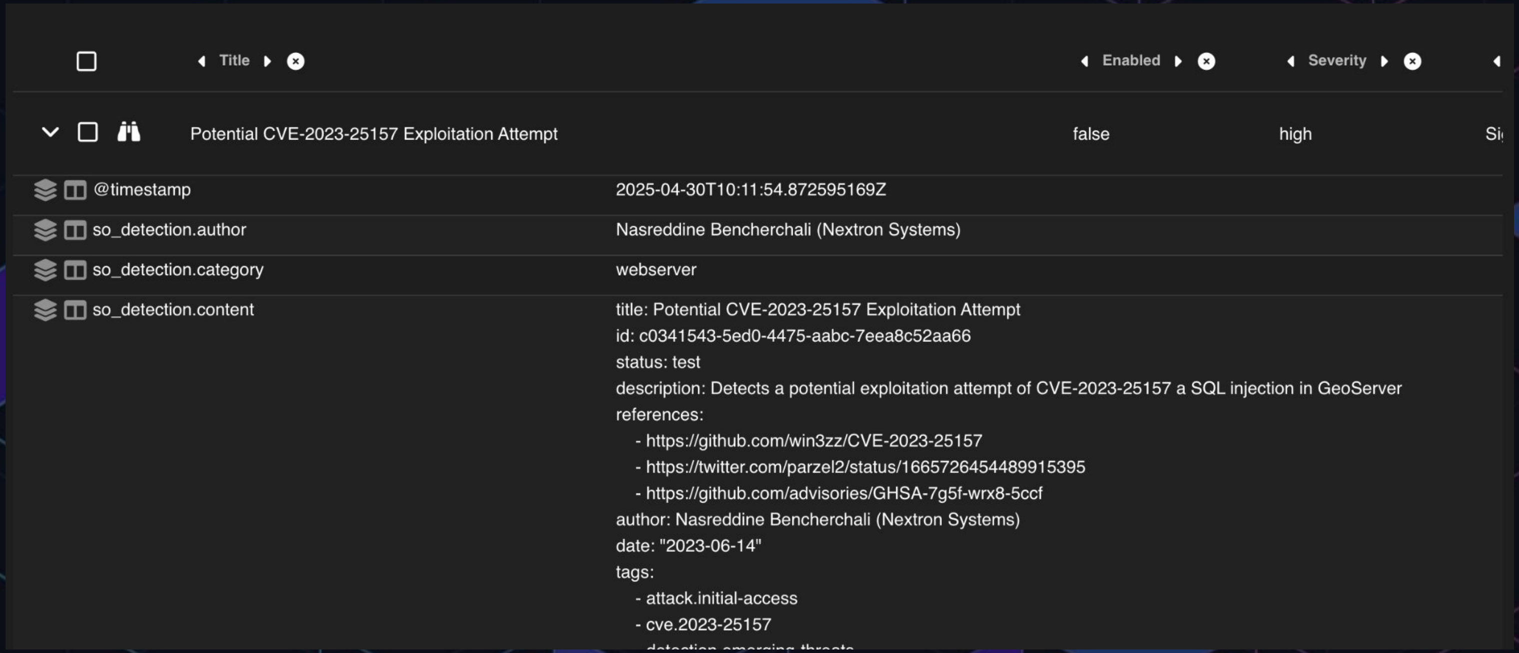
Our Solution (Technical Perspective)



Security Onion Rule Management

Feature

- Sigma Rule
- YARA Rule
- IDS Rule (Suricata)



□	Title	Enabled	Severity
□	Potential CVE-2023-25157 Exploitation Attempt	false	high

@timestamp	2025-04-30T10:11:54.872595169Z
so_detection.author	Nasreddine Bencherchali (Nextron Systems)
so_detection.category	webserver
so_detection.content	

```
title: Potential CVE-2023-25157 Exploitation Attempt
id: c0341543-5ed0-4475-aabc-7eea8c52aa66
status: test
description: Detects a potential exploitation attempt of CVE-2023-25157 a SQL injection in GeoServer
references:
    - https://github.com/win3zz/CVE-2023-25157
    - https://twitter.com/parzel2/status/1665726454489915395
    - https://github.com/advisories/GHSA-7g5f-wrx8-5ccf
author: Nasreddine Bencherchali (Nextron Systems)
date: "2023-06-14"
tags:
    - attack.initial-access
    - cve.2023-25157
    - detection.emerging-threats
```

Rule Management

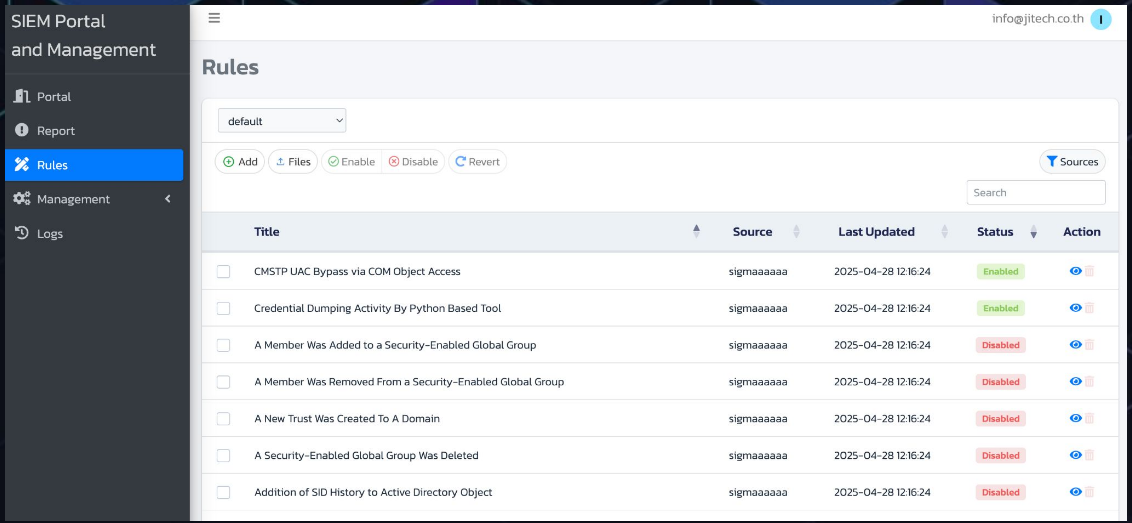
The Problems We Faced

- Lack of Central Rule Management
  - Import Rule
  - Change Management
  - Separate Rule Stored
- Lack of 3rd Party Support

Rule Management

Our Solution

- We created a single place in our portal to manage all rules
- You can import rules by file or just copy and paste them
- Admins can add, delete, view, and edit any rule from one spot
- We added support for outside rule sources to get more threat data
- The system automatically sends the right rules to each grid



Rules

	Title	Source	Last Updated	Status	Action
□	CMSTP UAC Bypass via COM Object Access	sigmaaaaaa	2025-04-28 12:16:24	Enabled	
□	Credential Dumping Activity By Python Based Tool	sigmaaaaaa	2025-04-28 12:16:24	Enabled	
□	A Member Was Added to a Security-Enabled Global Group	sigmaaaaaa	2025-04-28 12:16:24	Disabled	
□	A Member Was Removed From a Security-Enabled Global Group	sigmaaaaaa	2025-04-28 12:16:24	Disabled	
□	A New Trust Was Created To A Domain	sigmaaaaaa	2025-04-28 12:16:24	Disabled	
□	A Security-Enabled Global Group Was Deleted	sigmaaaaaa	2025-04-28 12:16:24	Disabled	
□	Addition of SID History to Active Directory Object	sigmaaaaaa	2025-04-28 12:16:24	Disabled	

High-volume Ingestion Challenge

Limitation We Face

- Our goal is to scale the SIEM to handle 100,000 event per second log data
  - Security Onion itself is difficult to achieve
- Security Onion is not designed to manage raw logs directly
  - External log server could be help Security Onion to do it
- Default Security Onion configuration would not design for High-volume Ingestion
  - Security Onion configuration needs to be reviewed and adjusted for optimal performance

High-volume Ingestion Challenge

Our Solution

Four strategy for handle high-volume log ingestion

1. Horizontal Scaling
2. Log Filtering
3. Dedicated Resources
4. Fine-tune the configuration

Strategy 1: Horizontal Scaling

OOTB.NET

Security Onion Support Horizontal Scaling

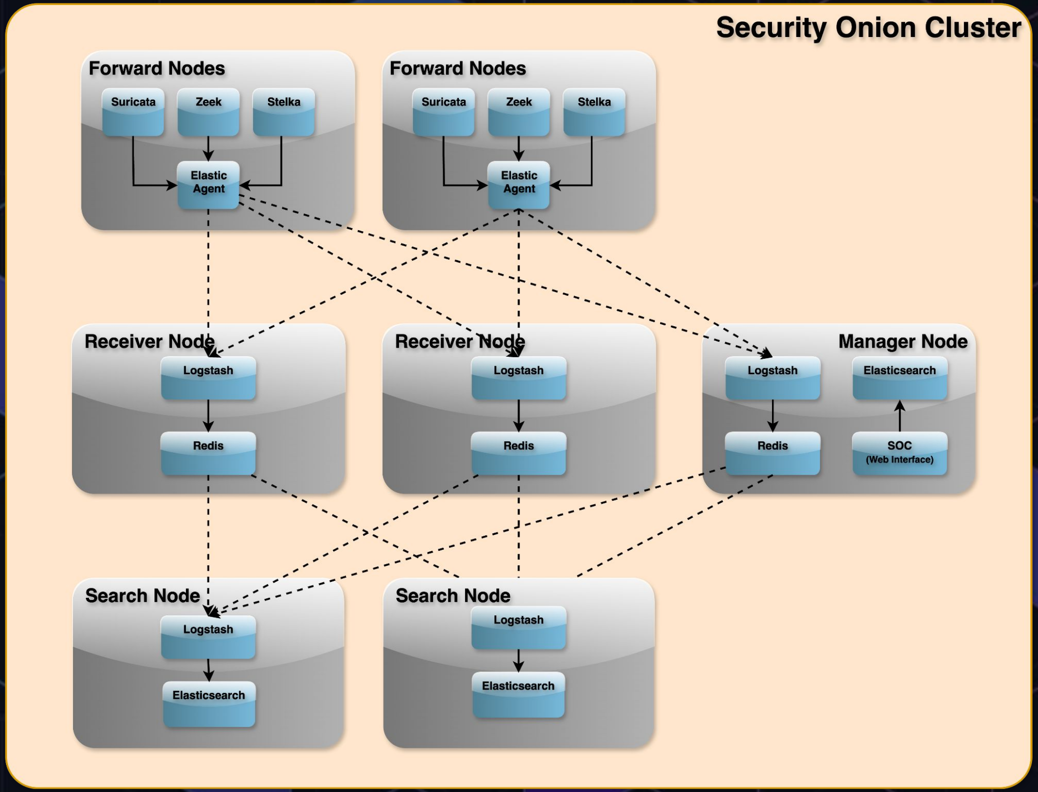
- Forward Node
- Receive Node
- Search Node

Pros

- Easy for use and manage

Cons

- Require more computing power



Strategy 2: Log Filtering (with Syslog Server)

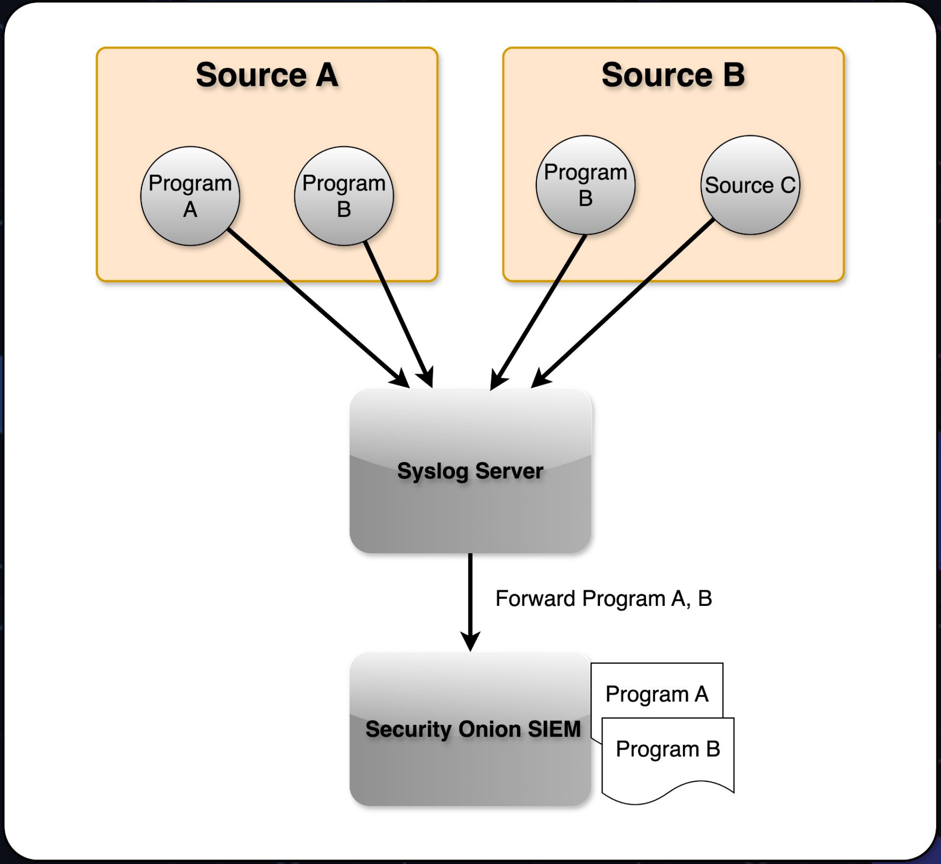
- Deploy syslog server for manage input log
- Forward only important log for threat detection
- All log data is still stored on the syslog server.

Pros

- Reduce computing resource allocation

Cons

- This method is effective only when using the syslog protocol.
- Inconvenient to use and manage log data

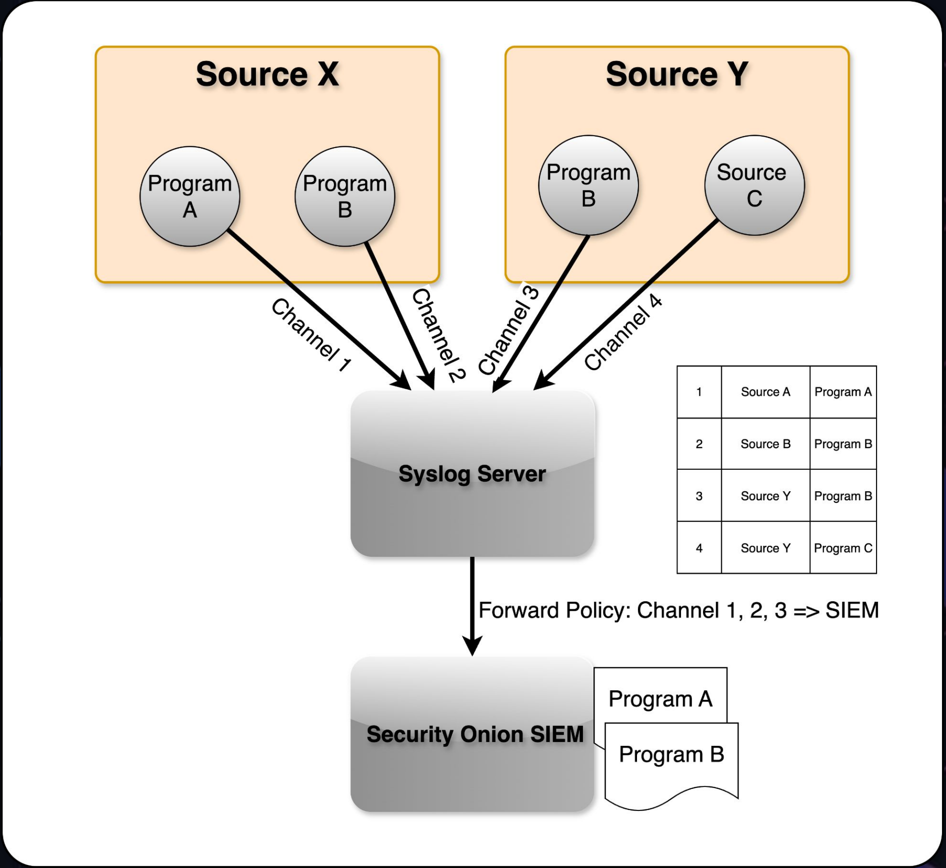


High Performance Syslog Server

OOTB.NET

We have developed a syslog server to improve the performance of the SIEM system.

1. Receive the log up to 500,000 event per second
2. Store log data organized by unique channel, using source IP address and port.
   (Assign one application per channel)
3. Forward only the necessary channels.



1	Source A	Program A
2	Source B	Program B
3	Source Y	Program B
4	Source Y	Program C

Forward Policy: Channel 1, 2, 3 => SIEM

Strategy 3: Dedicated Resources

OOTB.NET

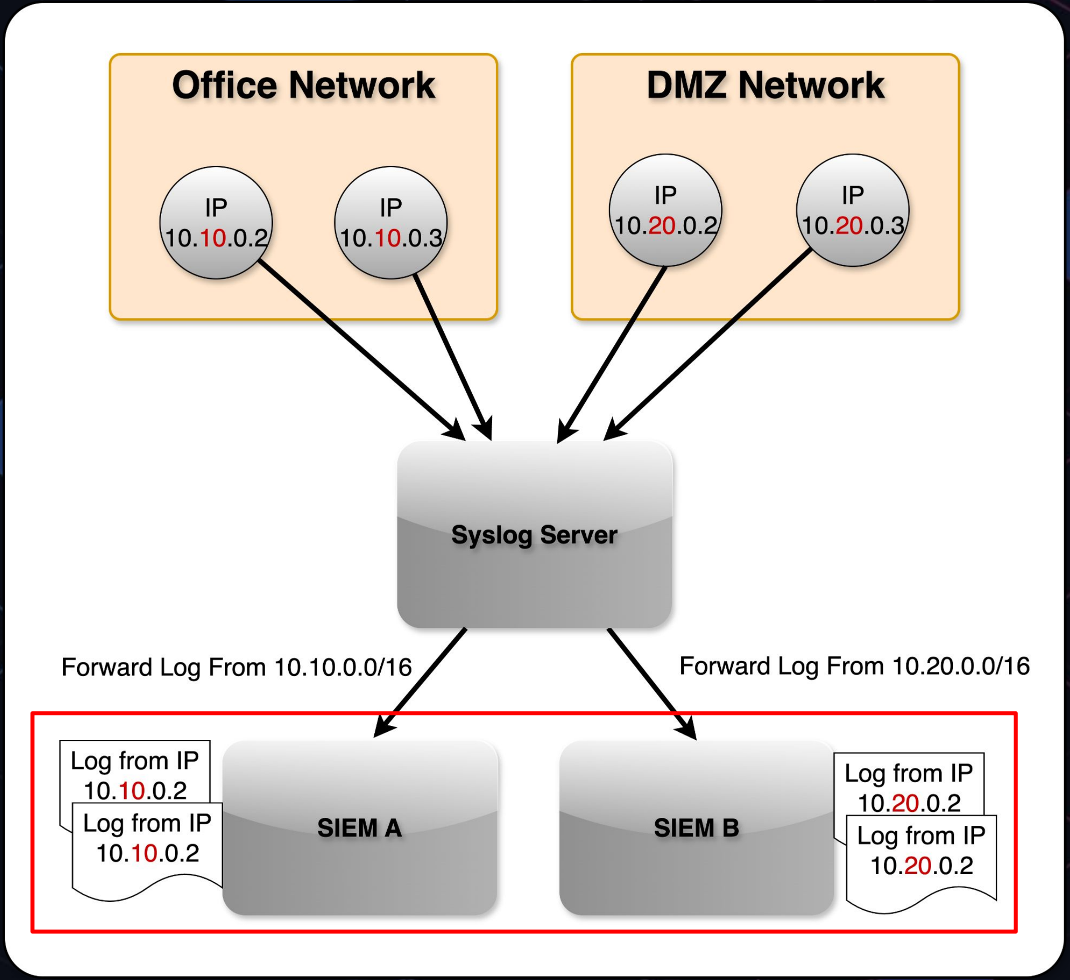
- Deploy separate SIEM instants by network zones
- Allocate dedicated resources for each zone
- Using a syslog server allows for easier management and centralization of syslog data.

Pros

- Prevent collateral damage

Cons

- It may be inconvenient to manage and access data.



Strategy 4: Fine-Tune The Configuration

- Data retention policy (Logs age on the SIEM)
- Elasticsearch configuration tuning
- Optimize Alert engine (Elastalert)

Pros

- Additional resources are not required

Cons

- It may not be significantly effective
- High risk; recommended to consult an expert

Data Retention Policy in Security Onion

Index Lifecycle Management (ILM)

- Menu: Administration > Configuration
- Sub-menu: elasticsearch > index_settings > global_overrides > policy > phases

Phase	Default Age	High-Volume Age
Hot	< 30 days	<1 days
Worm	< 60 days	< 2 days
Cold	< 365 days	> 2 days
Delete	> 365 days	> 2 days

Elasticsearch Tuning

OOTB.NET

Enhance indexing and searching performance

- Disable Swaff for search node (Elasticsearch recommendation)
  - #sudo swapoff -a
- Disable Replication
  - disabled by default on Security Onion
- Heap Size
  - Default Security Onion's heap size set to be 33% of system's memory
  - For search node, the heap size may increased to 50-60% of system's memory

Precautions of Elasticsearch

OOTB.NET

- Always ensure that more than 20% of disk space remains free
  - To prevent a full disk, Elasticsearch blocks writes to any index on the node
- Insufficient heap memory, it can lead to various issues
  - Unresponsive
  - Crash
- Use faster hardware
  - Local storage generally performs better than remote storage
  - SSD drives perform than better spinning disks

Ongoing Challenges

Waiting for solution

OOTB.NET

1. Threat Intelligence Management Feature Support
2. System Version Incompatibility

Cyber Threat Intelligence

OOTB.NET

- Process of gathering, analyzing, and interpreting information related to cyber threats to help organizations respond to cybersecurity incidents.
- Used to understand cyber threats, enabling organizations to effectively prepare for, prevent, and respond to the threat
- The system used to collect threat intelligence is often referred to as a Threat Intelligence Platform (TIP)
- Many SIEM tools support Threat Intelligence Management features for searching threat within security events

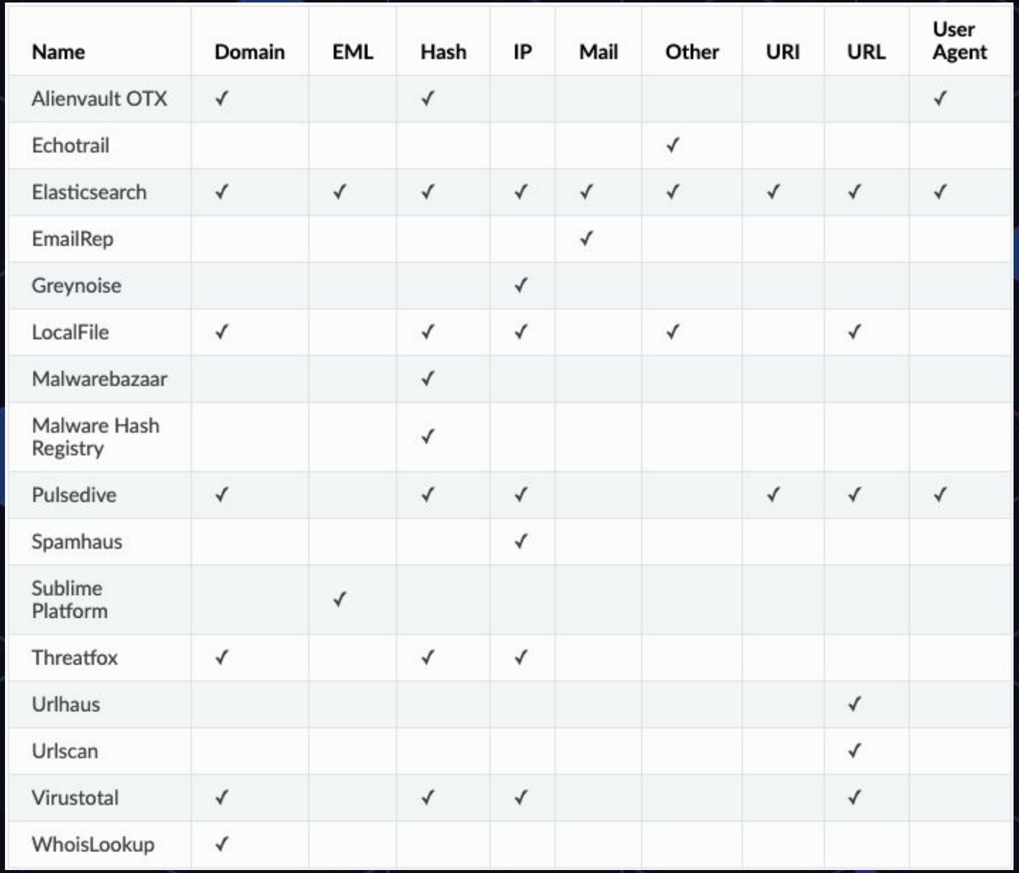
Threat Intelligence Management Challenge

OOTB.NET

- Security Onion supports to search indicator of compromise (IoC) within the Analyzers feature (Investigation process)

- Security Onion does not support real-time detection with IoC from TIP

- SIEM should support for search IoC in real-time data within
  - Log (with SIEM rule)
  - File (with Yara rule)
  - Network traffic (with IDS rule)



Name	Domain	EML	Hash	IP	Mail	Other	URI	URL	User Agent
Alienvault OTX	✓		✓						✓
Echotrail						✓			
Elasticsearch	✓	✓	✓	✓	✓	✓	✓	✓	✓
EmailRep					✓				
Greynoise				✓					
LocalFile	✓		✓	✓		✓		✓	
Malwarebazaar			✓						
Malware Hash Registry			✓						
Pulsedive	✓		✓	✓			✓	✓	✓
Spamhaus				✓					
Sublime Platform		✓							
Threatfox	✓		✓	✓					
Urlhaus								✓	
Urlscan								✓	
Virustotal	✓		✓	✓				✓	
WhoisLookup	✓								

Source: https://docs.securityonion.net/en/2.4/cases.html

System Version Incompatibility

OOTB.NET

- New versions of Security Onion are released quickly
- Often have big changes that break our custom tools
- Forces us to spend a lot of time and resources fixing our tools

Summary

OOTB.NET

- We chose Security Onion for its completeness and customized it for enterprise use
- Our key features address major gaps like user access, data isolation, and rule management
- We built a central log system to improve scalability and resource utilization
- Our solution is highly cost-effective and flexible due to its open-source foundation
- However, we still lack support for features found in COTS SIEMs, such as native Threat Intelligence

Key Takeaways

OOTB.NET

- Default open-source SIEMs, like Security Onion, require fine-tuning to achieve optimal performance and meet an organization's specific needs.
- In a high-performance environment, a SIEM requires a filtering function—in this case, server logs—to reduce the volume of data sent to the SIEM itself.
- While customization is both possible and highly beneficial, it requires a significant time investment and a high level of engineering skill. This can lead to increased costs, which, although potentially less than a paid solution, should still be carefully considered.
- The current trend is shifting away from collecting all raw logs and sending them to a central SIEM. Instead, the focus is now on processing data at the endpoint and sending only the essential information to the central system

OOTB.NET

Thank You

Questions?