



CryptoGen Nepal



 Saycure.

Solution Sheet

Use case Document

#Made4Security


















www.cryptogennepal.com



SayCure is a modern threat detection and response platform with threat detection capabilities which helps organizations neutralize threats before they have a negative impact on your business(s). Active response and vulnerability management capabilities out-of-the-box makes Saycure a one-stop solution for Threat life cycle management.






We focus on 3 key features:

- Cyber risk focused alerts
- Active monitoring and Response
- Compliance Monitoring
- Vulnerability Detection

Critical Cases				
				Search: <input type="text"/>
Name	Team Name	Members	Status	Actions
CASE : #4051 10 Jan 2024	Nirmal Poudel	  	<div><div></div></div> 38%	⋮
CASE : #4052 03 Jan 2024	Nirmal Poudel	  	<div><div></div></div> 45%	⋮
CASE : #4053 12 Jan 2024	Simran Karki	  	<div><div></div></div> 92%	⋮
CASE : #4054 19 Jan 2024	Rishav Pandit	  	<div><div></div></div> 56%	⋮
CASE : #4055 08 Jan 2024	Bishesh Shrestha	  	<div><div></div></div> 25%	⋮
Rows per page: 5 1-5 of 10 < >				

Cases By Assignee

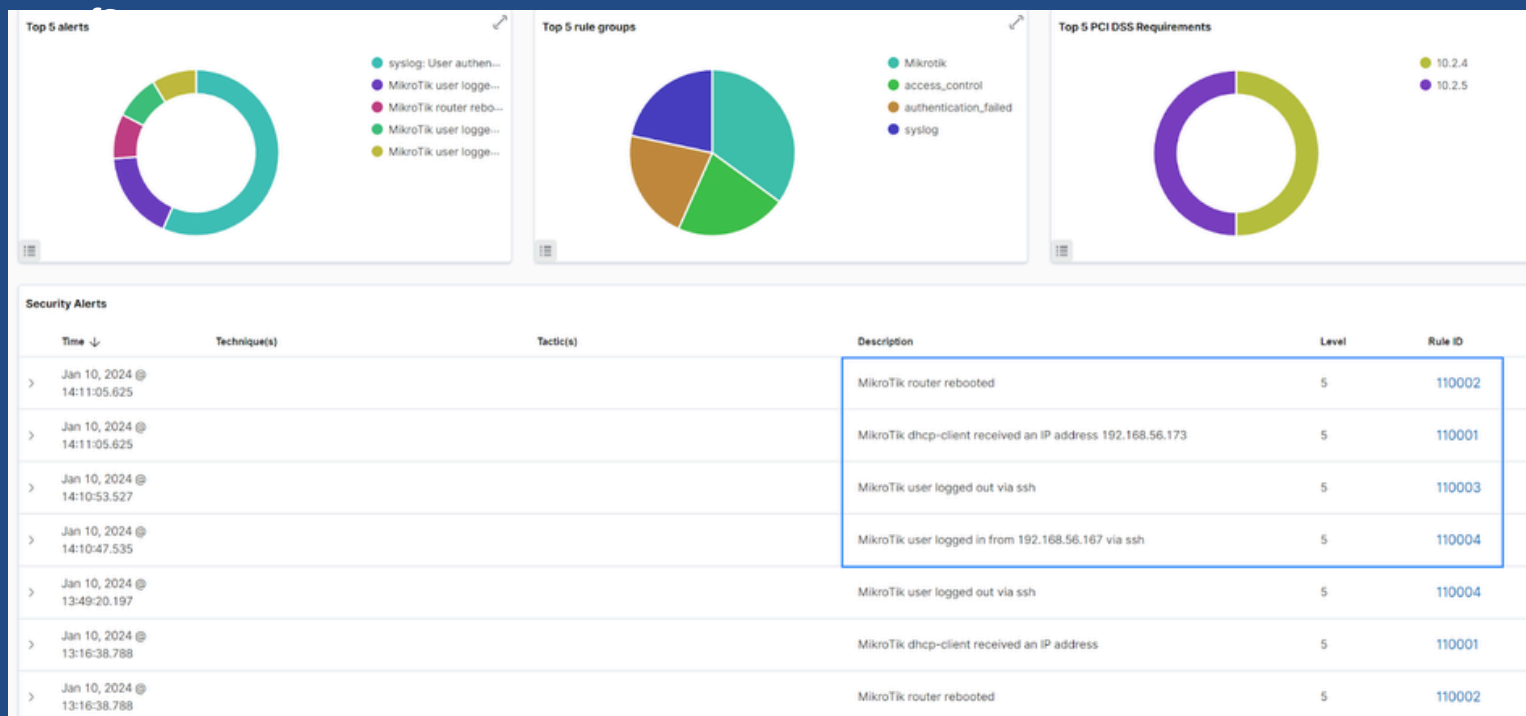
Total Cases

-  **Shreenkhala Bhattarai**
SOC Lead
-  **Nirmal Poudel**
SOC Analyst
-  **Simran Karki**
Sr. SOC Analyst
-  **Nayan Bhattarai**
SOC Analyst
-  **Aaditya Khati**
SOC Manager

Integrations

Network Monitoring components are directly embeded in the saycure platform. SayCure supports wide range of networking devices not limited to the out of the box parsers:

- Cisco PIX, ASA, and FWSM (all versions)
- Cisco IOS routers (all versions)
- Juniper Netscreen (all versions)
- SonicWall firewall (all versions)
- Checkpoint firewall (all versions)
- Cisco IOS IDS/IPS module (all versions)
- Sourcefire (Snort) IDS/IPS (all versions)
- Dragon NIDS (all versions)
- Checkpoint Smart Defense (all versions)
- Bluecoat proxy (all versions)
- Cisco VPN concentrators (all versions)
- VMWare ESXi 4.x
- Huawei USG



Saycure.

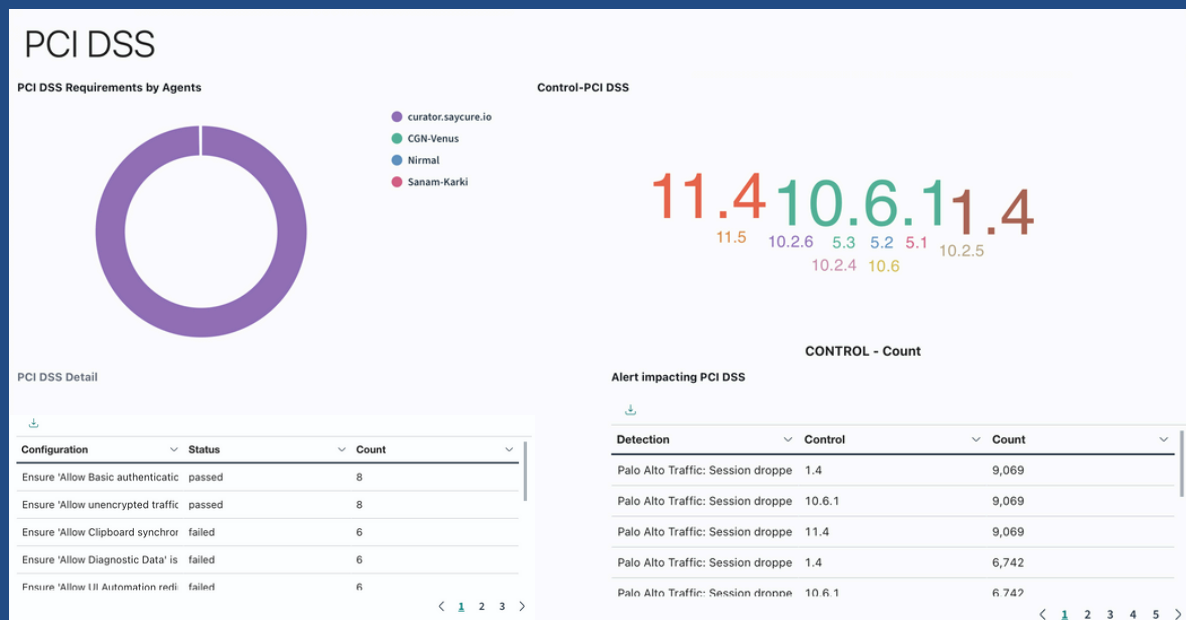
Integrations

SayCure has the capabilities to integrate with multiple third-party platform with access to API. The integration are but not limited to, SOAR, Threat Intelligence, Case Management, Email and more.

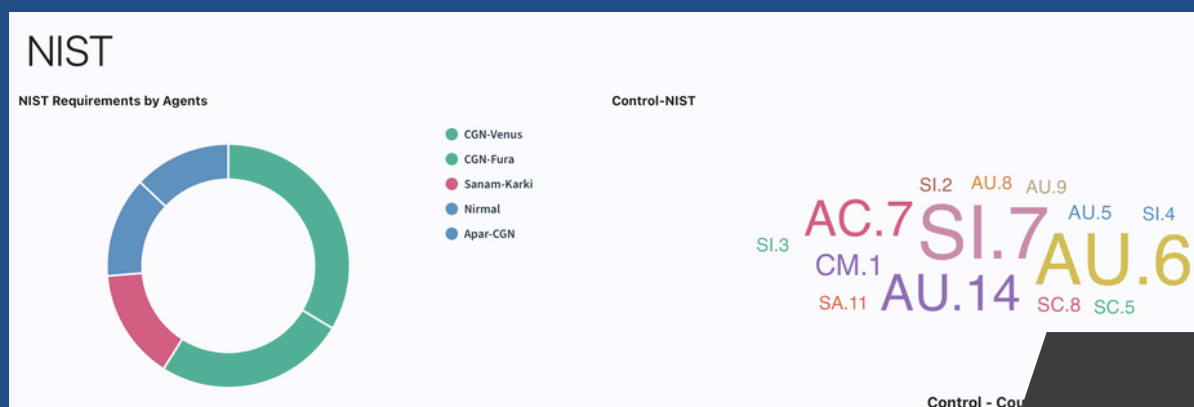


Compliance

SayCure helps to implement compliance requirement for regulatory compliance support and visibility. This is done by providing automation, improved security controls, log analysis, and incident response. The default SayCure ruleset provides support for PCI DSS, HIPAA, NIST 800-53, TSC, and GDPR frameworks and standards. SayCure rules and decoders are used to detect attacks, system errors, security misconfigurations, and policy violations.



SayCure supports dashboard creation for Local Compliances along with regulatory. The logs and events are mapped with local compliances.





Internal Mapping (RBAC)

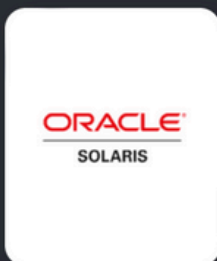
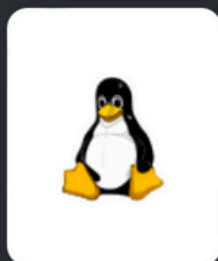
Wazuh RBAC allows access to Wazuh resources based on the roles and policies assigned to the users. It is an easy-to-use administration system that enables to manage users' or entities' permissions to the system resources. To learn more, see the [Role-Based Access Control](#) section.

The Wazuh platform includes an internal user database that can be used for authentication. It can also be used in addition to an external authentication system such as LDAP or Active Directory. Learn how to create users and map them with Wazuh in the below sections.

- [Creating and setting a Wazuh admin user](#)
- [Creating and setting a Wazuh read-only user](#)
- [Creating an internal user and mapping it to Wazuh](#)
- [Use case: Give a user permissions to read and manage a group of agents](#)

Agent Support

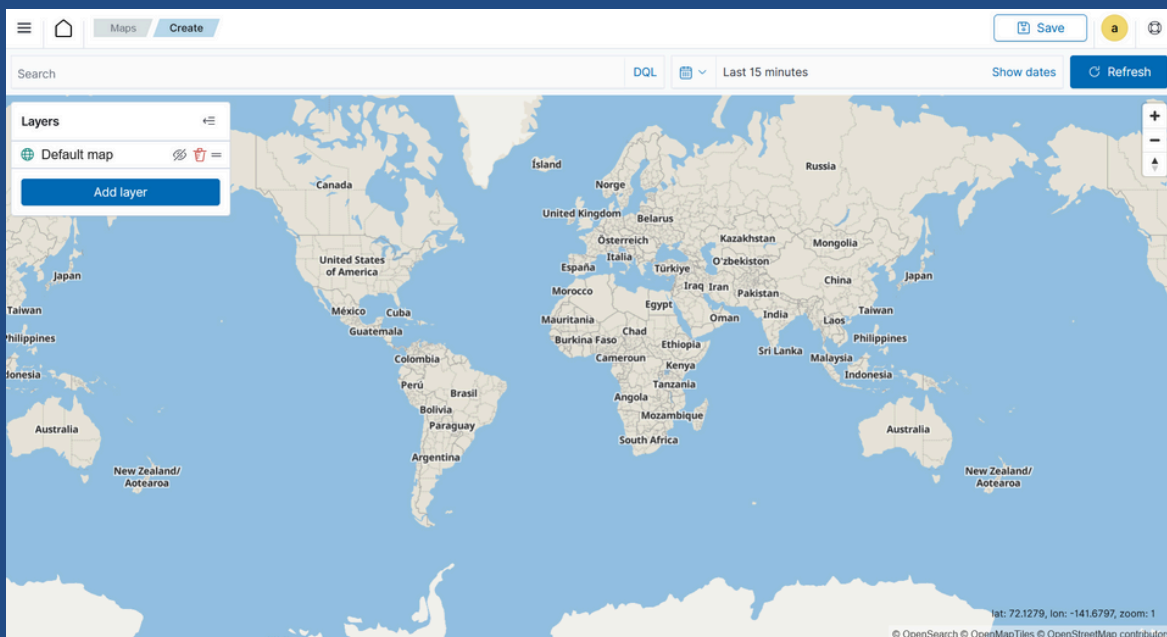
SayCure platform supports wide range of Operating Systems (OS) and with a high number of servers or endpoints, keep in mind that this deployment might be easier using automation tools such as [Puppet](#), [Chef](#), [SCCM](#), or [Ansible](#).



Dashboard

Maps:

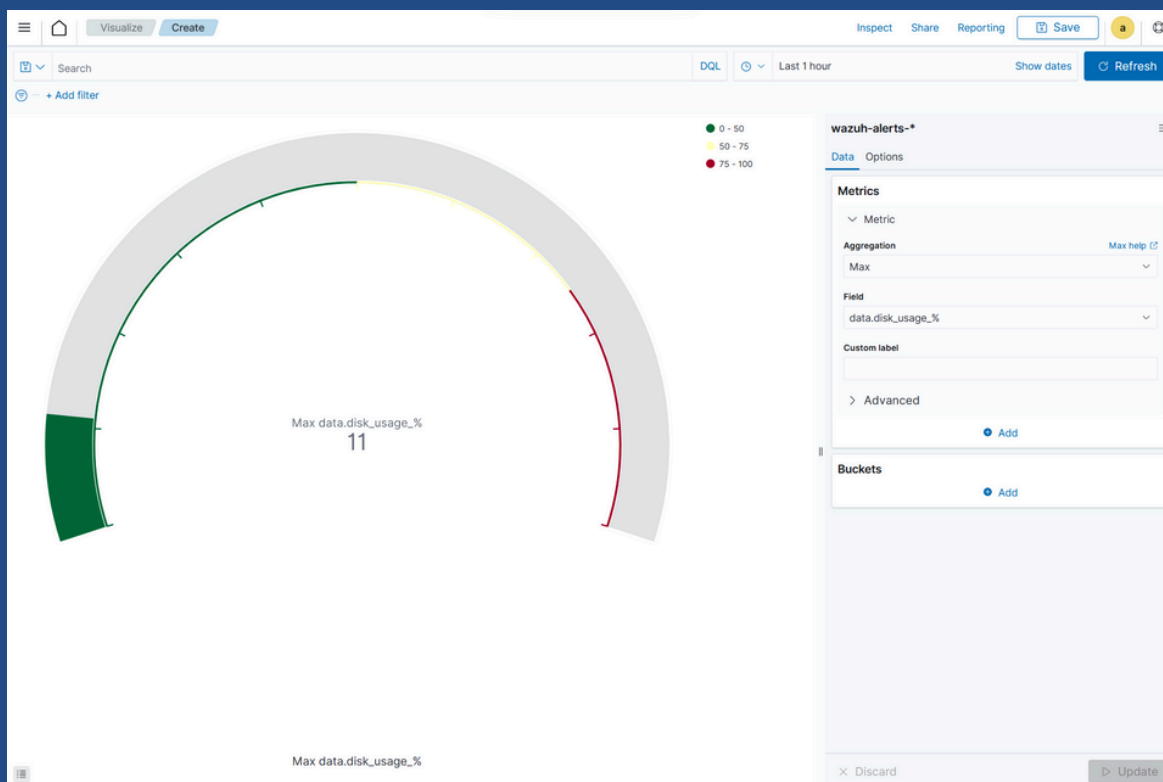
Maps: These are visual representations of geographical regions. Maps display spatial data, such as locations, boundaries, or distributions, on a graphical interface. They provide a means to explore and analyze geographic information, making them valuable for various applications, including navigation, data visualization, and spatial analysis.



Gauge:

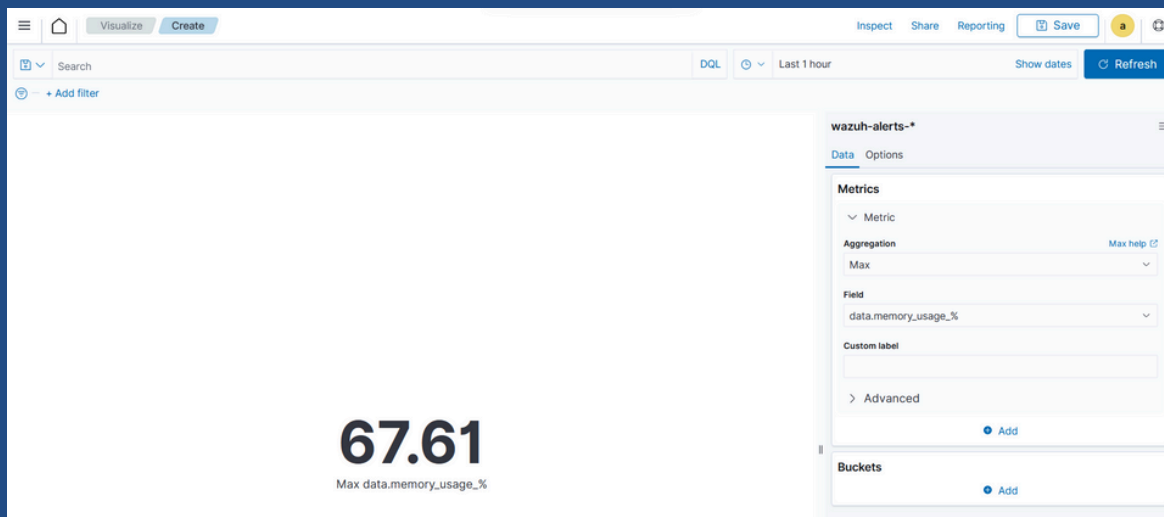
This is a visualization that is represented as a meter. It is commonly used to display a single value within a specific range. The gauge consists of a pointer that shows the current value. This is displayed as a position along a circular or linear scale.

Gauges are used to indicate progress, performance metrics, or levels of achievement. It shows how a metric's value relates to reference threshold values.



Metric:

This is a quantifiable measurement that is used to evaluate performance, progress, or specific characteristics. Metric represents a calculation as a single numerical value. They are applicable in various domains, including business analytics, key performance indicators (KPIs), and performance monitoring.



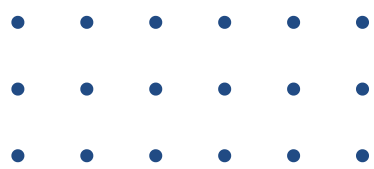
Data:

Data metric visualization is a single number that displays any count or calculation.

The following is a list of data visualizations:

- **Data table:** This is where the data is shown in tabular form.
- **Metric:** This is where a single number is displayed, which we can use to show any important metric data.
- **Goal and gauge:** This is used when we want to display any progress.

Contact Us



Cases by type

My Cases

Open Cases

Open Incidents

Closed Cases



SENDER

Multiple Bruteforce Attempt

#4058-0987-2193



SENDER

URL Matched to Threat Intel

#4050-7261-9836

Case Activity



Possible Malware De

Case Updated



Multiple Bruteforce A

Case Resolved



URL Matched to Thre

Case Updated



New Vulnerability De

Awaiting Response



+977 980-112-8471



sales@cryptogennepal.com



www.cryptogennepal.com



Naxal, Kathmandu, Nepal

Stay SayCure