



# Case Studies

---

Unlocking Threat Intelligence Insights with RST Cloud

# CONTENTS

**Increasing ROI of SIEM  
and its efficiency**

**1**

**Elevating Managed Security Services  
with CTI**

**2**

**Increasing ROI of SOAR**

**3**

**Securing Web Services with CTI**

**4**

**Implementation of CTI in accordance  
with industry standards**

**5**

**Elevating Telecom Provider  
Services with CTI**

**6**

# Increasing ROI of SIEM and its efficiency

1

In the realm of cybersecurity, handling vast volumes of data while making rapid, informed decisions is imperative. Security Information and Event Management (SIEM) systems are the front line of defence, but they can be flooded with alerts.

The crucial challenge lies in deciding whether an event signal is a security incident or merely noise.

SOC analysts often struggle with insufficient information about incidents, leading to prolonged decision-making processes and the costly utilization of expert resources.

Furthermore, the risk of overlooking critical malicious activities that could cause substantial harm looms large.



# Cyber Threat Intelligence as a Solution



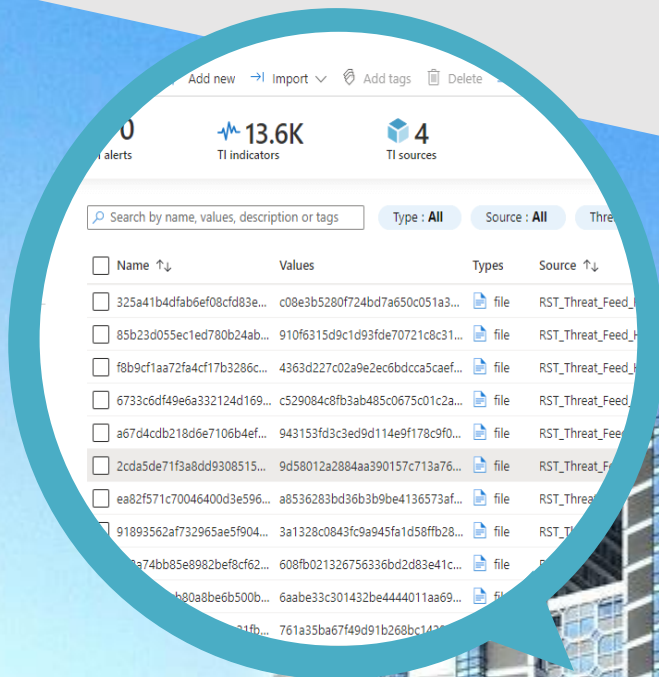
To address this challenge, having reliable and high-confidence Cyber Threat Intelligence (CTI) data is invaluable.

By using automated analysis of thousands of threat reports, **RST Report Hub** gives us a comprehensive understanding of the current threat landscape, enabling us to craft highly effective and relevant detection content.

**RST Threat Feed** provides a stream of relevant indicators of compromise, aiding real-time detection of malware, reducing time on incident triage, and helping with threat hunting activities.

Each entry in RST Threat Feed is scored and enriched, simplifying the triage and interpretation of information for cybersecurity professionals.





A screenshot of a SIEM interface showing a table of threat indicators. The table has columns for Name, Values, Types, and Source. The data is filtered by Type: All and Source: All. The table lists several indicators, each with a unique ID, a value, a type (file), and a source (RST\_Threat\_Feed).

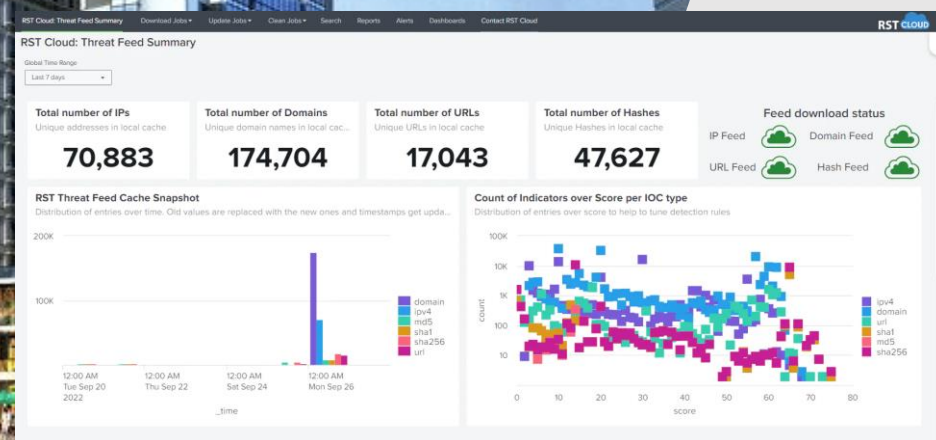
Name	Values	Types	Source
325a41b4dfab6e08cf83e...	c08e3b5280f724bd7a650c051a3...	file	RST_Threat_Feed...
85b23d055ec1ed780b24ab...	910f6315d9c1d93fd670721c8c31...	file	RST_Threat_Feed...
f8b9cf1aa72fa4c17b3286c...	4363d227c02a9e2ec6bdcca5caef...	file	RST_Threat_Feed...
6733c6df49e6a332124d169...	c529084c8fb3ab485c0675c01c2a...	file	RST_Threat_Feed...
a67d4cdb218d6e7106b4ef...	943153fd3c3ed9d114e9f178c9f0...	file	RST_Threat_Feed...
2cda5de71f3a8dd9308515...	9d58012a2884aa390157c713a76...	file	RST_Threat_Feed...
ea82f571c70046400d3e596...	a8536283bd36b3b9be4136573af...	file	RST_Threat_Feed...
91893562af732965ae5f904...	3a1328c0843fc9a945fa1d58ffb28...	file	RST_Threat_Feed...
74bb85e8982bef8cf62...	608fb021326756336bd2d83e41c...	file	RST_Threat_Feed...
b80a8be6b500b...	6aab33c01432be4444011aa69...	file	RST_Threat_Feed...
761a35ba67f49d91b268bc143...			

## Outcome

Integration of **RST Threat Feed** and use of **RST Report Hub** make SIEM systems more efficient and help to detect threats with a low False Positive rate, reducing noise and false alarms.

The enriched indicators, TTPs, threat actor and malware knowledge from RST Cloud help cybersecurity professionals expedite investigations, shorten response times, and make more informed decisions.

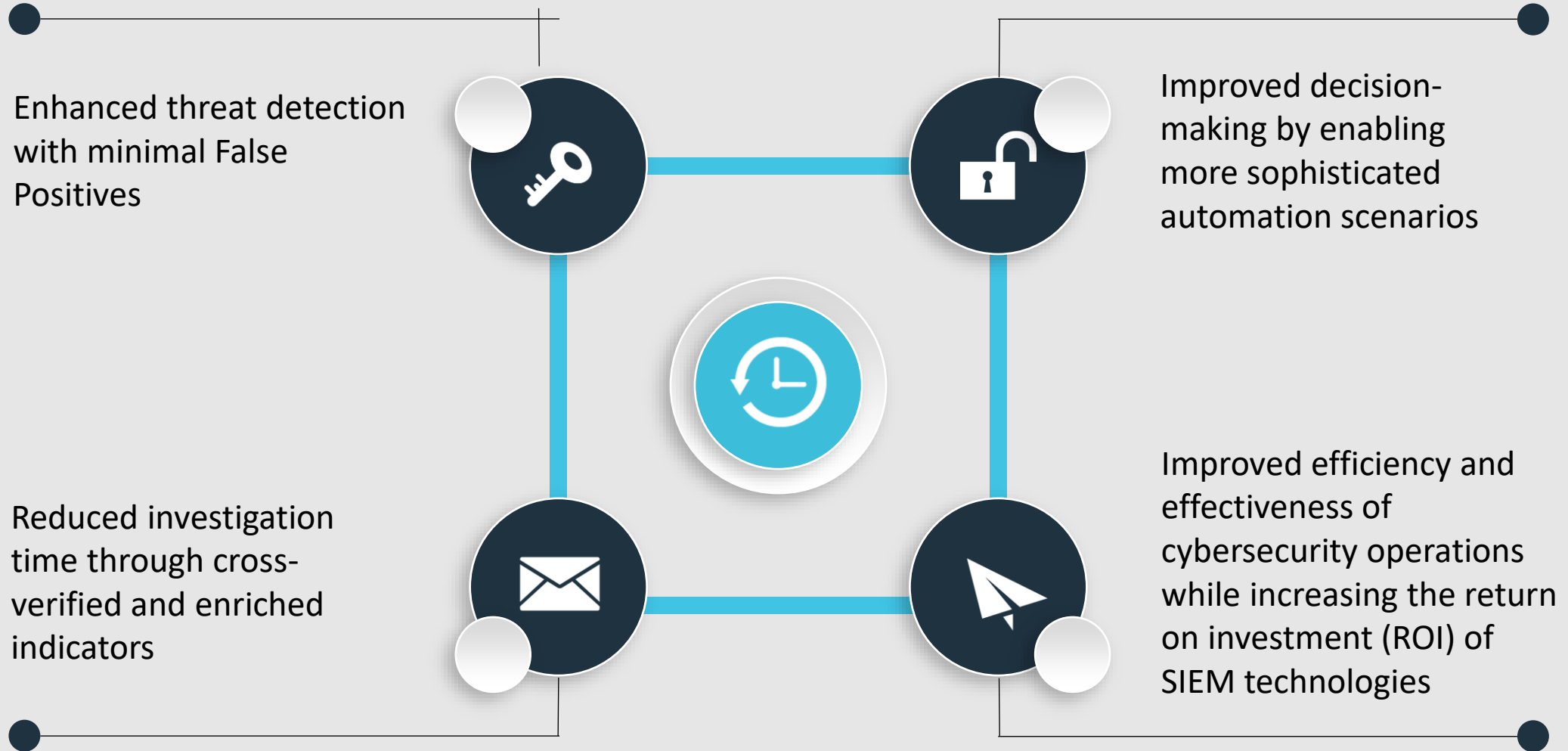
An outdated indicator that is no longer associated with real time malicious activities is treated as informational, allowing for verification without triggering automatic alert actions.





# Benefits of SIEM technology combined with CTI from RST Cloud

1



## Solution



RST Cloud CTI Solutions steps in as the catalyst for enhancing the services offered by MSSPs



Our comprehensive threat intelligence services equip MSSPs with the data and intelligence necessary to deliver top-notch cybersecurity services efficiently with pay-as-you-grow approach

## Challenge

Managed Security Service Providers (MSSPs) operate in an environment where providing top-tier cybersecurity services is imperative. Clients rely on MSSPs to protect their digital assets from evolving threats, and the need for accuracy and efficiency is paramount. Achieving this without incurring exorbitant costs is a constant challenge.



By embracing RST Cloud CTI Solutions, MSSPs can elevate their services to a new level of excellence



Enhanced Threat Detection: RST Cloud provides timely and relevant TI, empowering MSSPs to detect and mitigate cyber threats swiftly

---



Streamlined Operations: Integration with existing MSSP infrastructure streamlines operations, reducing manual efforts and improving response times

---



Improved Client Protection: MSSPs can offer more effective and efficient cybersecurity services to their clients, enhancing overall client protection

---

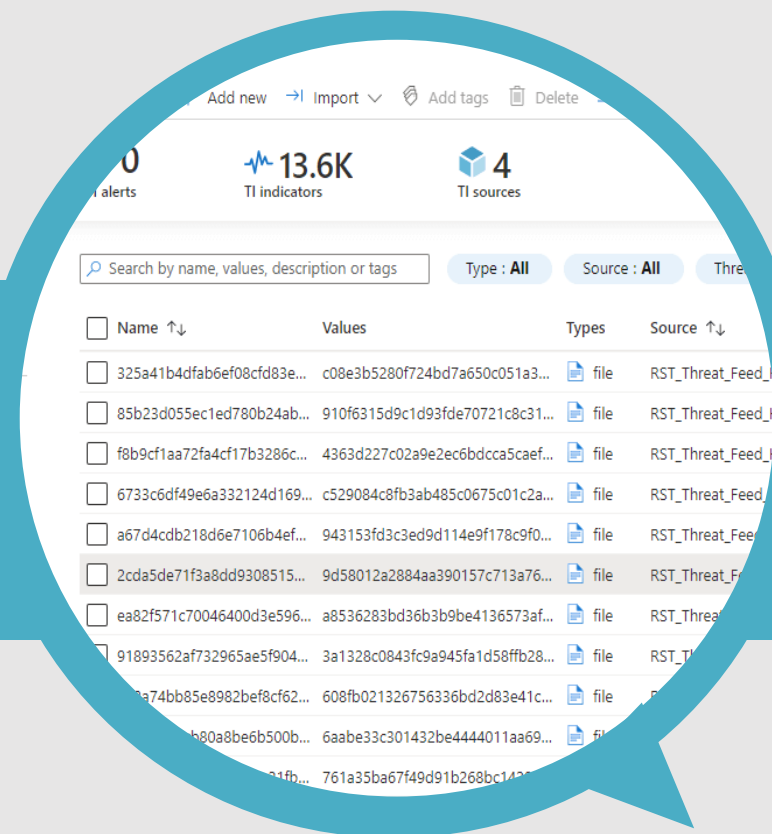


Cost-Efficiency: RST Cloud's seamless integration and automation capabilities help MSSPs optimize their operations, reducing operational costs

---



# Increasing ROI of SOAR and its efficiency



0 alerts    13.6K TI indicators    4 TI sources

Search by name, values, description or tags    Type: All    Source: All    Threat

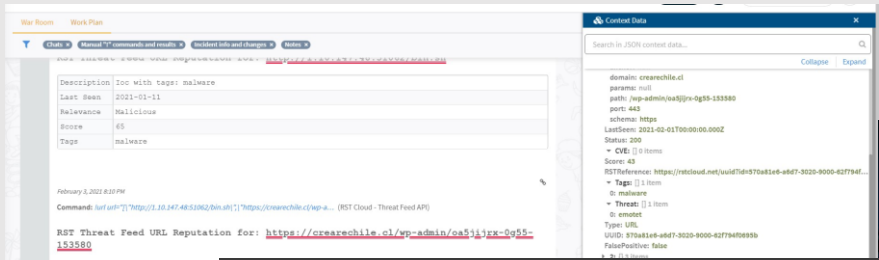
<input type="checkbox"/>	Name ↑↓	Values	Types	Source ↑↓
<input type="checkbox"/>	325a41b4dfab6ef08cfd83e...	c08e3b5280f724bd7a650c051a3...	file	RST_Threat_Feed_...
<input type="checkbox"/>	85b23d055ec1ed780b24ab...	910f6315d9c1d93fde70721c8c31...	file	RST_Threat_Feed_...
<input type="checkbox"/>	f8b9cf1aa72fa4cf17b3286c...	4363d227c02a9e2ec6bdcca5caef...	file	RST_Threat_Feed_...
<input type="checkbox"/>	6733c6df49e6a332124d169...	c529084c8fb3ab485c0675c01c2a...	file	RST_Threat_Feed_...
<input type="checkbox"/>	a67d4cdb218d6e7106b4ef...	943153fd3c3ed9d114e9f178c9f0...	file	RST_Threat_Feed_...
<input type="checkbox"/>	2cda5de71f3a8dd9308515...	9d58012a2884aa390157c713a76...	file	RST_Threat_Feed_...
<input type="checkbox"/>	ea82f571c70046400d3e596...	a8536283bd36b3b9be4136573af...	file	RST_Threat_Feed_...
<input type="checkbox"/>	91893562af732965ae5f904...	3a1328c0843fc9a945fa1d58ffb28...	file	RST_Threat_Feed_...
<input type="checkbox"/>	a74bb85e8982bef8cf62...	608fb021326756336bd2d83e41c...	file	RST_Threat_Feed_...
<input type="checkbox"/>	b80a8be6b500b...	6aabe33c301432be4444011aa69...	file	RST_Threat_Feed_...
<input type="checkbox"/>	...	761a35ba67f49d91b268bc14...	file	RST_Threat_Feed_...

## Challenge

In the realm of cybersecurity, swift and informed decision-making is paramount. The use of high-confidence indicators is crucial when deciding whether to take active actions, such as blocking, to prevent potential outages caused by outdated or false-positive indicators of compromise. Automated response requires actionable TI in SOAR

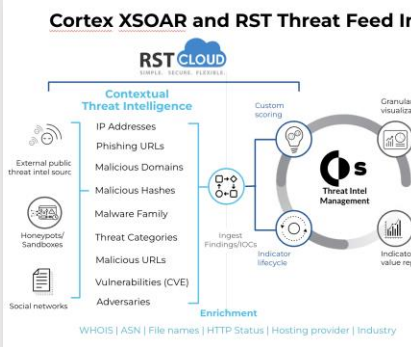
Threat actors often utilize dynamic infrastructure, causing an indicator that appears malicious one week to become benign the next. The lack of comprehensive indicator information necessitates manual enrichment by cybersecurity analysts, a resource-intensive process that hinders automation

# Integration with CTI

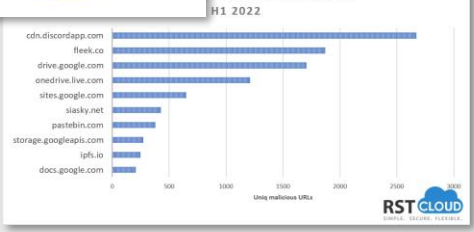


To address this challenge, organizations rely on having reliable and high-confidence threat intelligence data at their disposal

RST IoC Lookup API helps with enrichment of the known bad indicators. RST NoiseControl allows to filter out false positives and enable SOAR to interpret data and proceed with appropriate response



ID	Tags	#Hits	#Certs	Date	Last modified at	Published at	Info	Distribution	Actions
180	rstcloud-threat-namecontrol	875	1	2023-05-23	2023-05-23 13:38:49	2023-05-23 13:40:06	RST Cloud	Organization	🔍 🔄 🗑️
181	rstcloud-threat-namecontrol	614	8	2023-05-23	2023-05-23 13:38:35	2023-05-23 13:38:51	RST Cloud	Organization	🔍 🔄 🗑️
182	rstcloud-threat-namecontrol	3819	10	2023-05-23	2023-05-23 13:38:24	2023-05-23 13:38:36	RST Cloud	Organization	🔍 🔄 🗑️
183	rstcloud-threat-namecontrol	29	2	2023-05-23	2023-05-23 13:38:15	2023-05-23 13:38:20	RST Cloud	Organization	🔍 🔄 🗑️



```
function RSTCloudEnrichment() {
  // Script configuration
}
```

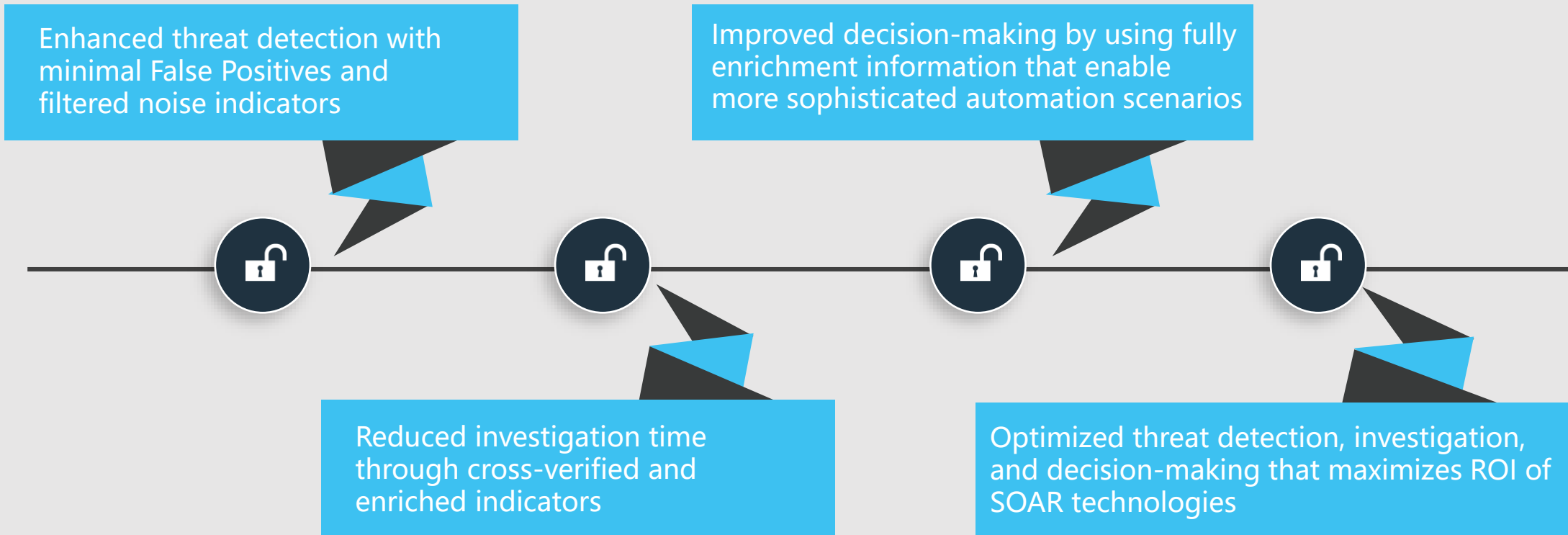
Triage

Enrichment

Interpretation

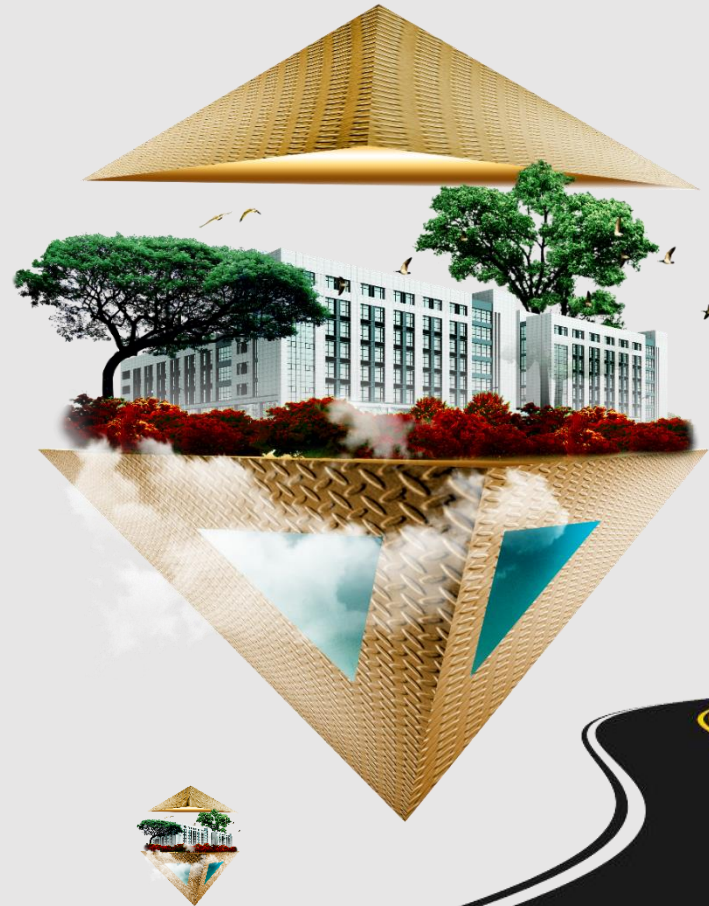
Response

# Benefits of SOAR technology combined with CTI from RST Cloud



# Securing Web Services with RST Cloud CTI

4



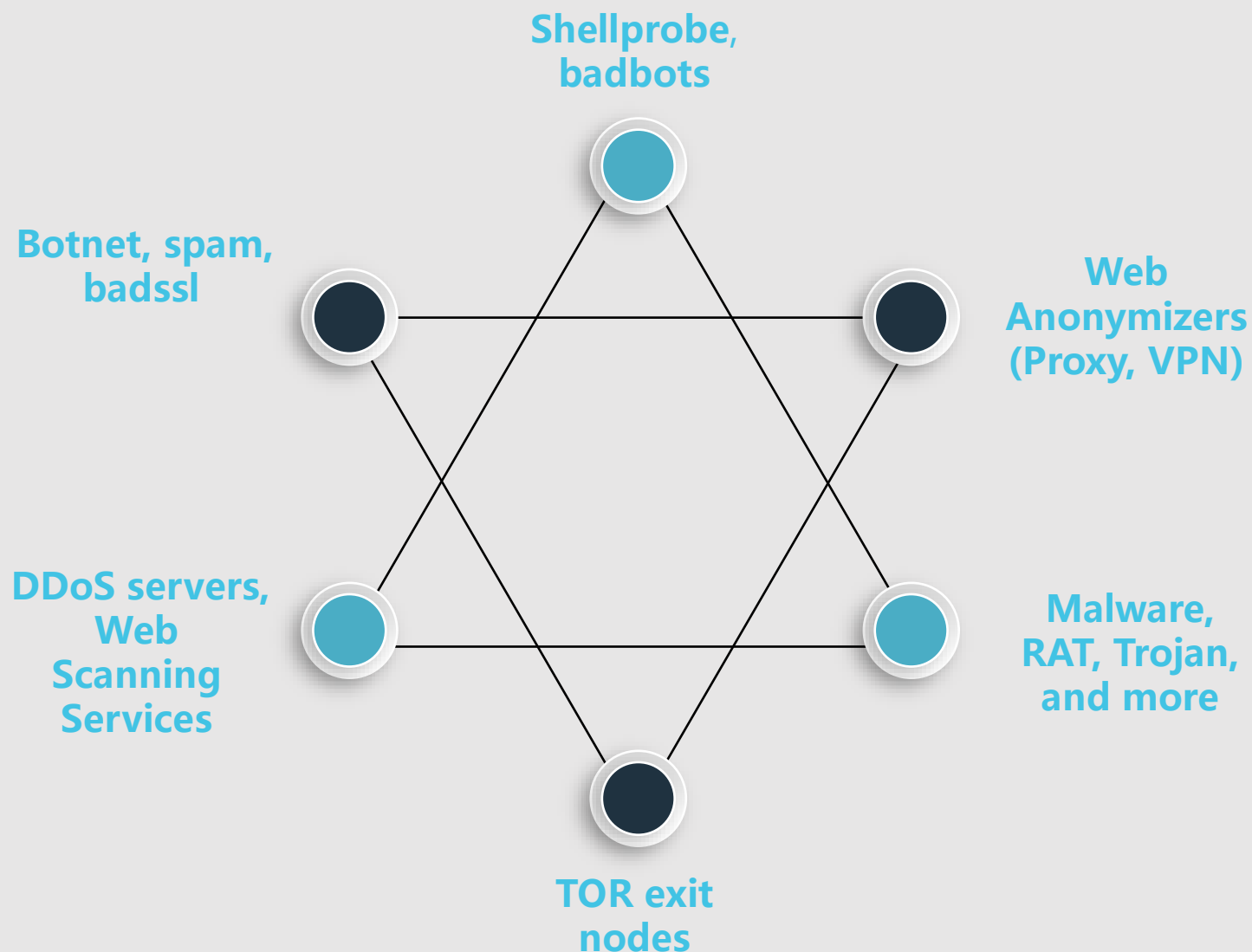
In the realm of business-critical online web services, ensuring uninterrupted service delivery to clients is an absolute necessity. Web services are under constant threat from a myriad of cyber adversaries. Protecting against these threats and maintaining service integrity is a significant challenge



# Attribution and categorization

RST Cloud steps in to help to protect web services, offering the knowledge of the most relevant cyber threats in this realm.

With RST Threat Feed, you stay one step ahead of cyber adversaries. Our platform provides detailed indicators of compromise (IoCs) for a wide range of malicious resources, including:



This integration empowers you to proactively block malicious connections, fortify your web defences, and prevent incidents from happening

Our platform gives you precise control over connections associated with IP addresses linked to fraud and misuse cases.

By blocking connections from known bad resources and thwarting web attacks using data from RST Cloud, your infrastructure remains resilient against threats

What sets RST Cloud apart is its seamless integration with leading Next-Generation Firewall (NGFW) and Web Application Firewall (WAF) solutions through a simple API



# Implementation of CTI in accordance with industry standards

## More standards mandate implementation of Cyber Threat Intelligence (ISO 27001, NIS2, SAMA, etc.)

A

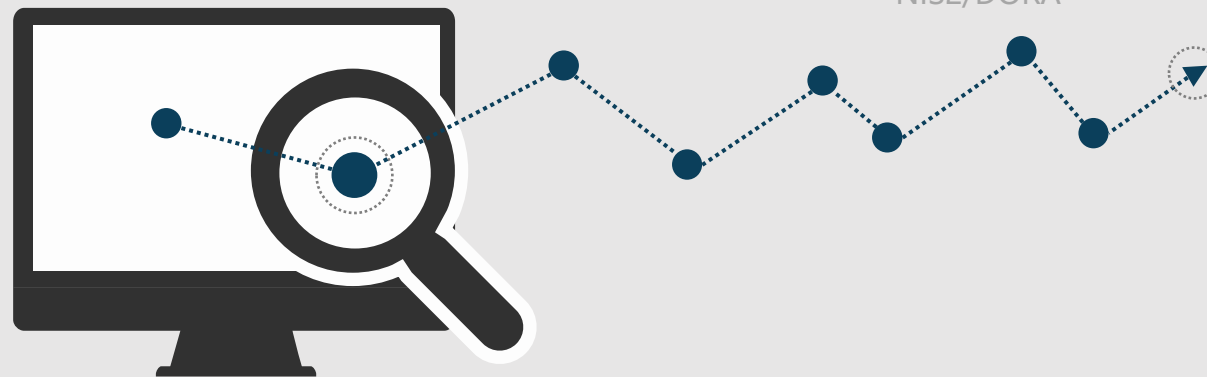
In the ever-evolving landscape of cybersecurity threats, it's crucial to have a clear understanding of the threat landscape. Without a comprehensive view of potential risks, security measures can become fragmented, leading to increased budgetary expenses for information protection. The absence of a focused approach towards current threats can hinder the ability to model real-world threats effectively, ultimately affecting the level of security and requiring endless investments in cybersecurity. The need for implementing cyber threat intelligence is emphasized by the most reputable industry standards, such as ISO 27001, SAMA CTI Principles, CIS Controls v8, and more.

B



# Benefits of leveraging CTI from RST Cloud

- ISO 27001
- SAMA
- CIS Controls v8
- NIS2/DORA



Gain a comprehensive view of the threat landscape. Prioritize security measures based on current and relevant threats



Enhance threat detection and response capabilities. Improve overall security posture through a deeper understanding of real-world risks



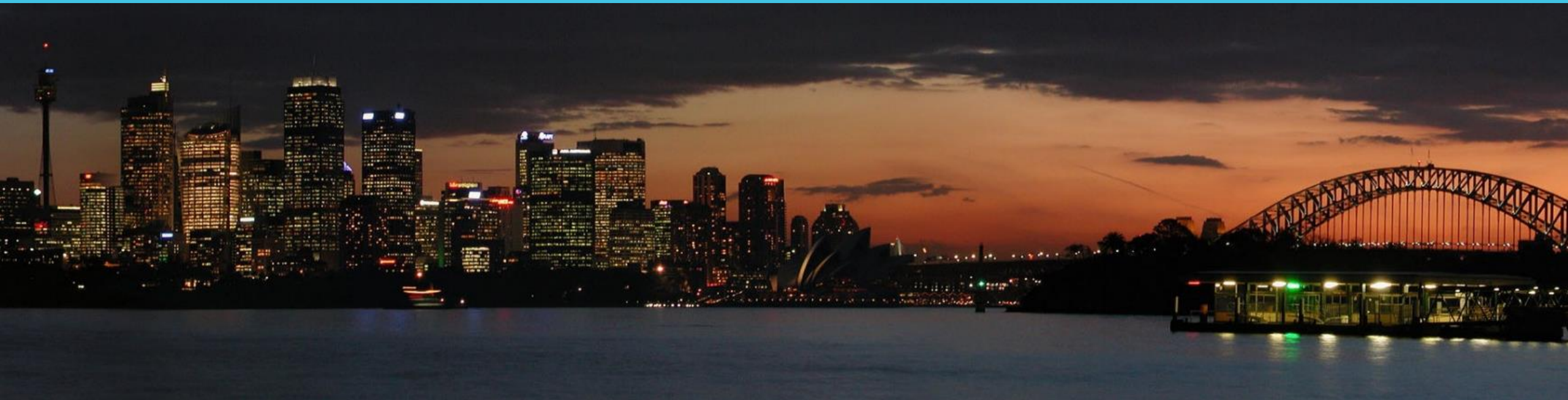
Reduce the overall costs of cybersecurity by optimizing resource allocation, streamlining incident response, and minimizing the impact of cyberattacks

Cyber Threat Intelligence emerges as the solution to this challenge. CTI empowers organizations and security vendors with a targeted approach to threat assessment, providing a deeper understanding of adversary behavior. By focusing on relevant and up-to-date threats, CTI helps organizations model threats accurately and improve their security posture without the need for endless investments in cybersecurity.



# Elevating Telecom Provider Services with RST Cloud CTI Solutions

In today's rapidly evolving digital landscape, cybersecurity has become a paramount concern, even for Small and Medium-sized Businesses (SMBs). Internet Service Providers (ISPs) are facing the challenge of meeting the growing demand for robust security solutions alongside their core telecom services. They also want to grow their revenue via value-add services such as "Secure Internet Access" option for their clients. Traditional customer edge routers or modems often have limited memory and CPU capacity, posing limitations in providing comprehensive cybersecurity services



# RST Cloud empowers ISPs to enhance their service

RST Cloud empowers ISPs to enhance their service offerings by seamlessly integrating advanced cybersecurity solutions into their portfolio. These solutions are designed to fortify the businesses of ISPs, providing top-notch security services tailored to SMBs. By leveraging RST Cloud feeds and their scoring mechanism, ISPs can optimize their budget-friendly devices, which are typically constrained in terms of memory and CPU resources. This optimization allows ISPs to focus solely on the most current indicators, effectively thwarting a majority of major threats.



MikroTik

Fortinet Fortigate

Cisco Firepower

Check Point NGFW

Palo Alto NGFW

## RST Cloud solutions enable ISPs to offer their SMB clients robust and cost-effective security services

**This integration not only enhances the ISPs' service portfolio but also ensures that their clients experience secure connectivity and peace of mind in an increasingly digital world. By efficiently utilizing RST Cloud data, ISPs can deliver cutting-edge security alongside telecommunications, meeting the cybersecurity demands of SMBs without the need for expensive network equipment**




- No need for costly centralized infrastructure: Telecom providers can implement RST Threat Feed without significant capital investments.
- Unlock additional revenue sources: This innovative approach allows telecom providers to tap into an additional revenue source within their existing client base.
- Optimize budget-friendly devices for effective threat mitigation, and unlock additional revenue streams within their existing client base.
- Turn existing resources into profit centers: By embracing RST Threat Feed, ISPs can transform their existing resources into profit centers.
- Efficiency meets profitability: Elevate security, bolster revenue, and embrace a future where efficiency meets profitability with RST Cloud CTI Solutions.

# Contact us




 [rstcloud.com](http://rstcloud.com)



 +441143608085



 +38268226732

