THREATQUOTIENT

sysdig

CUSTOMER SUCCESS STORY

Sysdig Selects ThreatQ to Scale Cloud Threat Detection and Response Solutions

Sysdig standardizes on the ThreatQ Platform for data-driven security operations, saving time and improving threat detection and research capabilities at scale.

Challenge

Over the past few years, the move to the cloud has accelerated dramatically and, with that transition, companies are turning to Sysdig to improve their cloud security posture. A cloud and container security leader, Sysdig detects threats in real-time using a combination of machine learning, curated rules, and Sysdig Threat Research Policies. Sysdig scans for hundreds of indicators of compromise (IoCs) from a variety of sources to enrich and provide context to their detections. Informed by this continuously evolving threat intelligence, the Sysdig Threat Research Team writes, tunes, and pushes rules out to customers via the Sysdig platform to detect threats in containers, cloud infrastructure, and the Kubernetes control plane, and implements response. The team, which includes computer security and machine learning experts from around the world, also creates threat reports, articles, and blogs to share their threat intelligence more broadly.

As Sysdig expands operations, Michael Clark, Director of Threat Research at Sysdig, knew the Threat Research Team had outgrown the standard database they were using to store indicator data. They needed a solution with capabilities to help aggregate, manage, and store multiple sources of intelligence, including OSINT, feeds from premium vendors, and threat intelligence developed internally by Sysdig, for example via their network of strategically placed honeypots.

Sysdig also needed a more efficient and effective way to provide more context with each rule, so analysts don't waste time trying to figure out why an indicator is bad. Instead of the Sysdig team having to gather

"With the ThreatQ Platform, we can scale our threat research capabilities now and in the future. Whether that's bringing in additional sources of intelligence, adding more and better rules, or the addition of ThreatQ Data Exchange to share data across different teams."

– Michael Clark, Director of Threat Research at Sysdig

OVERVIEW

INDUSTRY: Technology

CUSTOMER SINCE: 2022

EMPLOYEES: 700

TOTAL INCOME: Privately Held

LOCATION: San Francisco, CA

CHALLENGE

Gathering, tracking and reporting as the volume of threat data and number of sources grow. Enhancing the threat detection rules with data from detection feeds.

SOLUTION

The ThreatQ Platform with the DataLinq Engine meets Sysdig's key criteria for more efficient and effective threat intelligence management including support for different feeds, expiration of threat data, prioritization of indicators, API-based integration, ease of export, and flexibility to adapt to the unique requirements of the cloud.

OUTCOME

- ✔ Improves detection rules for customers
- ✔ Saves time for the Sysdig Threat Research Team
- ✔ Simplifies and enhances threat intelligence reporting

information from different sites and tools, they wanted one place to go for the context they need to enrich a rule and enable faster analysis and deeper understanding.

Solution

As a technology vendor, naturally Sysdig explored the option of build vs buy but dismissed the idea of building for a couple of reasons. Although Michael and several team members are skilled software developers, Michael didn't want to make being a programmer a requirement for the team.

Additionally, Michael explained that it isn't just about building something. Maintenance would be complex and time consuming, particularly considering Sysdig's extensive list of criteria which included:

- Support for different feeds
- Expiration of threat data
- Prioritization of indicators so customers receive only what matters to them
- API-based to integrate with data collection infrastructure
- Ease of exporting from the platform to the open-source Falco project for rule generation
- Flexibility to adapt to cloud architecture and different kinds of data

After reviewing the main platform providers, Sysdig determined the ThreatQ Platform met its key criteria and delivered additional valuable capabilities, including:

Flexibility: ThreatQ's very broad set of APIs and custom connectors can be written and deployed quickly to support bi-directional integration which allows the Sysdig Threat Research Team to make sense of and operationalize vast amounts of indicators and other threat data efficiently and effectively. It's easy to import data from a variety of sources including custom indicator types, enrich threat data with context, build and automate workflows, manage threat intelligence expiration, and export threat data to existing tools to generate rule sets. When writing reports and blogs, visualization through custom dashboards is also extremely valuable to measure and categorize data for analysis.

Outcome

Additional context-rich detection rules

The team can create rules faster with data from an expanded number of sources enriched with more context, resulting in better detections for customers. This is particularly important given the current geopolitical climate and rapidly evolving threat landscape.

Saves time for the Threat Research Team

The ThreatQ Platform automates tasks including data aggregation, deduplication, and normalization. Additionally, based on parameters set by the Sysdig Threat Research Team, the platform also automates enrichment, scoring, prioritization, and expiration, which saves time and reduces noise.

Simplifies and enhances threat intelligence reporting

Visualizations make it easier for the team to analyze and report on what they see and share their intelligence with the broader security community with compelling graphics.

Sales@ThreatQ.com • 703.574.9885

Architecture: ThreatQ's flexible and extensible architecture was important to Sysdig because it allows them to address specific use cases and provision separate instances to facilitate maximum control, efficiency, and speed.

Team: The expertise and responsiveness of the ThreatQuotient team came through during the evaluation period and beyond. Support for custom workflows and integrations is fast, often in just a few hours or less, so Sysdig can move at "cloud speed" and help their users get ahead of threats.

Working with ThreatQuotient, over the next few months Sysdig tackled their top use cases.

Export: With the ThreatQ exporting language, Sysdig's Threat Research Team can quickly generate Falco lists and automate rule creation without having to use Python or any other outside languages.

Containers: The ability to store container data in the ThreatQ Platform, along with context to understand why an indicator is malicious, allows them to create their own enriched feed that is continuously and automatically updated. Visualizations through custom dashboards also improve reporting.

Honeynet: When a Sysdig honeypot is compromised, the team creates a new incident and uses ThreatQ as the repository of that knowledge which enables them to quickly determine if they have seen an indicator before or not. If the indicator is new, they record the data and share it as a rule with customers, taking care to first eliminate any noise via whitelisting. Storage of this data is also useful for threat intelligence research and internal and public reporting.

> ***"Our use-case driven approach to the evaluation process clearly pointed us to the ThreatQ Platform to help us achieve our goals and demonstrate value back to the organization quickly."***
>
> – Michael Clark,
> Director of Threat Research at Sysdig

About ThreatQuotient

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC.

For more information, visit **www.threatquotient.com**.

Sales@ThreatQ.com • 703.574.9885