

# SOC Prime Inc Case Study

Use Case - Kubernetes Cost and Capacity Optimization



## Case Study

# CloudNatix helps SOC Prime optimize Kubernetes spend

**CASE STUDY** 

### **Executive Summary**

SOC Prime's operates the world's largest and most advanced platform for collective cyber defense enabling security teams to address the challenges of building context-enriched and threat-specific detections, organize and execute around strategic detection objectives, and manage the deployment of content at scale across 25+ SIEM, EDR, and XDR platforms.

"Being a tech-forward company, SOC Prime runs the significant part of their applications and services on Kubernetes," says the Head of DevOps Eugene Samborskyi. As SOC Prime grows and delivers more products to its customers across different industry verticals and diverse levels of cybersecurity maturity, it becomes a priority to gain a more granular view of workloads to better manage efficiency, allocate resources, and forecast capacity.

### Solution

SOC Prime was looking for a feasible solution to manage Kubernetes environments more efficiently, as well as provide a real-time view and historical drilldown of resource allocation and usage. While their existing cloud providers – AWS and Azure – deliver what Eugene Samborskyi calls "a helicopter view of spend" the team required a more granular look at their environment to accurately manage workload resources and breakdown costs to better serve internal teams and end-customers.



### **About SOC Prime**

SOC Prime cultivates collaboration from a global cybersecurity community and curates the most up-to-date Sigma rules compatible with over 25 SIEM, EDR, and XDR platforms.

SOC Prime's innovation, a community-driven approach based on Detection-as-Code principles and cutting-edge technology leveraging Sigma language and MITRE ATT&CK® as core pillars are recognized by the independent research companies, credited by the leading SIEM, XDR & MDR vendors, and trusted by 8,000+ organizations, including 42% of Fortune 100 and 21% of Forbes Global 2000.

"SOC Prime estimates a 25% reduction in overall cloud spend on Kubernetes using CloudNatix"

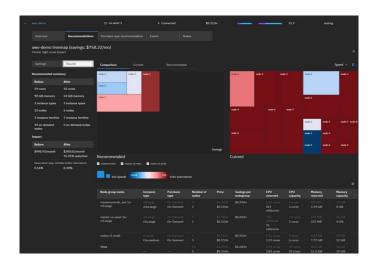
- Eugene S, Head of DevOps, SOC Prime



### **Detailed Capabilities**

#### **Benefits**

Since implementing CloudNatix, SOC Prime has gained a solid overview of applications and services resource consumption within different Kubernetes environments, including the production, stage, test and development. Having this data at hand, the team now easily spins up resources for a new application or workload and supports other business lines even more efficiently. Deploying CloudNatix allowed SOC Prime to address the emerging challenges within multiple environments enabling the DevOps team to proactively mitigate any issue while shaving seconds off environment management.business.



CloudNatix Cluster Rightsizing Simulator

By consistently monitoring workload behaviors and implementing CloudNatix's real-time recommendations, the company can now easily provide resources to spin up new application workloads for different lines of

### Results

#### **ELIMINATE WASTE**

By leveraging CloudNatix, SOC Prime reports easily doing more with less. With CloudNatix cluster rightsizing, the team better optimizes resources in terms of CPU and memory to ensure their environments are running as efficiently as possible.

#### SAVE COSTS

The team at SOC Prime estimates a 25% reduction in overall cloud spend with CloudNatix's cluster rightsizing recommendations. Additionally, CloudNatix helps SOC Prime's DevSecOpsteam accurately forecast future requirements and optimize financial investment in cloud resources.

### **About SOC Prime**

SOC Prime cultivates collaboration from a global cybersecurity community and curates the most up-to-date Sigma rules compatible with over 25 SIEM, EDR, and XDR platforms. SOC Prime's innovation, a community-driven approach based on Detection-as-Code principles and cutting-edge technology leveraging Sigma language and MITRE ATT&CK® as core pillars are recognized by the independent research companies, credited by the leading SIEM, XDR & MDR vendors, and trusted by 8,000+ organizations, including 42% of Fortune 100 and 21% of Forbes Global 2000.





To learn more about about how CloudNatix can be your partner in the journey to Cloud, Cloud Native and beyond, go to <a href="https://www.cloudnatix.com">www.cloudnatix.com</a>.

contact@cloudnatix.com | www.cloudnatix.com | @cloudnatix