Dollar Tree

Through the partnership with SOC Prime, Dollar Tree managed to accelerate the cloud SIEM migration process, cutting down detection content translation time by several months while boosting resource efficiency. SOC Prime also helped the industry-leading retailer strengthen its defenses against challenging threats to minimize the risk of breaches. Applying verified hunting queries for Microsoft Sentinel and Crowdstrike Falcon LogScale, backed by actionable threat intelligence, SOC Prime Platform enabled Dollar Tree to increase the productivity of its engineering team while saving time & effort on regular threat detection and hunting tasks.

Industry	Region	Company Size	SIEM & XDR in Use
Retail	**USA**	**10,000+ employees**	**IBM QRadar, Microsoft Sentinel, Crowdstrike Falcon LogScale, CrowdStrike EDR**

Kyle W.
Cyber Security Analyst at Dollar Tree

“Rules conversion with Uncoder has been a major help for us as part of our transition to the cloud. Without SOC Prime, it would have taken at least a couple of extra months of work on top of what we have already spent on the migration process. Apart from that, we rely on SOC Prime Platform as a primary source for our threat intel reporting to search for the latest threats in the industry, specific threat actors, CVEs, and zero-days. This helps us save at least several analyst hours daily on threat research”

Highlights

- Streamlining detection content translation as part of the company’s transition to the cloud
- Simplifying threat research with access to SOC Prime’s global feed of security news and tailored threat intelligence
- Enhancing hunting velocity and accuracy with an extensive collection of verified hunting queries
- Accelerating the engineering team’s productivity by saving hours on manual repetitive tasks

Challenges

Increased Sophistication & Numbers of Cyber Attacks Targeting the Retail Industry

According to Verizon’s 2023 Data Breach Investigations Report, 88% of the cyber attacks against retailers stem from system intrusion, social engineering, or basic web application attacks, with nearly 100% of them being financially motivated. Dollar Tree, as a Fortune 500 Company in the retail sector, underscores the need for proactive detection against intrusions for financial gain, including skimming and ransomware attacks that can lead to serious data breaches and are continuously evolving in volumes and sophistication. The company also raises concerns about risks of intrusions involving B2B vendors and third parties as potential attack vectors for internal threats.

Growing Volumes of Data Sources, Complex Infrastructure & Rising Costs of Legacy SIEM Maintenance

Managing complex on-premise SIEMs requires extensive training and high maintenance costs which, coupled with productivity and performance hurdles, encourages progressive enterprises to consider a cloud transition.

Dollar Tree was looking for a next-scale cloud SIEM adoption as part of its digital transformation priority to simplify integration and onboarding of the company's diverse product stack and keep up with the latest cybersecurity trends. The company was looking for a cost-efficient third-party solution that would help accelerate the transition to Microsoft Sentinel, with a primary focus on assistance in the content translation part of cloud SIEM migration.

Threat Intelligence Integration & Prioritization Hurdles

With increasing volumes of data coming from diverse threat intelligence feeds, large-scale organizations, like Dollar Tree, are continuously under pressure to ensure that threat intelligence collection is effective and actionable. To address this challenge, Dollar Tree was in search of a feasible product suite that would facilitate threat intel reporting and reduce the manual burden on the in-house engineering team of operationalizing CTI to tailor it to the unique threat profile and organization-specific needs.

Solution

Before the partnership with SOC Prime, Dollar Tree was investing a great deal of time and effort into building detections to address emerging threats using their internal team's resources while striving to continuously evolve the organization's cybersecurity maturity. The company has chosen SOC Prime's expertise and technology to accelerate the resource-intensive migration process to Microsoft Sentinel spanning over 3 years. Relying on **SOC Prime's product suite** enables automated rule conversion to the cloud-native language format, saving the need for manual routine and extensive fine-tuning, which coupled with enhanced capabilities for threat intel prioritization and simplified hunting, allows Dollar Tree to increase SOC team capacity and productivity.

Achievements

2X Faster Detection Content Translation

Dollar Tree has been planning the cloud migration from the IBM QRadar SIEM to Microsoft Sentinel for over 3 years mostly due to the complex infrastructure and product update challenges of the legacy on-prem solution. Dollar Tree chose SOC Prime's product suite over another MDR provider's services that would take twice as many man-hours on rule conversion coupled with double expenses. Relying on SOC Prime's **Uncoder AI**, Dollar Tree saved a couple of months of the team's effort, eliminating the burden of manual content translation and customization.

Threat Intelligence Accelerator

Dollar Tree relies on SOC Prime's global feed of detection algorithms to explore relevant context on the latest TTPs, specific threats, and threat actors, including APTs targeting the retail sector, like **Lazarus** or **FIN7**, ransomware operators like **Black Basta**, trending CVEs, exploits, and zero-days. Leveraging SOC Prime Platform as a core source of threat intelligence enables SOC and CTI analysts to save at least 60 hours each month on threat research instead of drowning in overwhelming data from diverse open-source threat intel feeds struggling to prioritize what matters most.

Simplified Threat Hunting Experience

Dollar Tree takes advantage of SOC Prime's extensive library of detection and hunting ideas to apply them as code templates, adjust to current security needs, and instantly convert the queries to Microsoft Sentinel ready to run in the cloud instance. This facilitates increased threat hunting accuracy and velocity while saving time on building queries from scratch and automatically converting them to the native SIEM or EDR language format.

Adoption of Next-Gen Cybersecurity Strategy

As a forward-looking and industry-leading retailer, Dollar Tree proactively allocates resources and prioritizes initiatives that align with the company's future-proof cybersecurity strategy. Leveraging SOC Prime's cutting-edge technologies backed by AI fits with the innovation-driven strategy, enabling Dollar Tree to continuously elevate its cybersecurity maturity and facilitate the adoption of next-gen SOC.

About Dollar Tree

Dollar Tree, is a Fortune 500 company and one of the nation's leading value retailers, which operates more than 16,000 stores and 25 distribution centers across 48 contiguous U.S. states and five Canadian provinces. From party supplies and home décor to health & beauty, seasonal items, food & snacks, the company offers a huge selection of products and services to millions of customers from across the globe. For over 30 years, Dollar Tree's philosophy and mission have not changed, yet the company focuses its strategy on constantly adapting to an ever-changing marketplace with innovative and creative ideas. Dollar Tree connects over 10,000 talented people who contribute to the company's growth and continue its success with genuine drive, imagination, and intelligence.