Quzara Cybertorch™

SOC Prime partners with Quzara Cybertorch™ to provide curated content to drive more streamlined and accurate detections based on a variety of threats, including zero-days and bounty hunting content.

Industry
Computer & Network Security (MDR)

Region
USA

Company Size
50+ employees

SIEM & XDR in Use
Microsoft Sentinel, M365 Defender, MDE, Microsoft IoT

Parvez Nadaf
Security Engineer at Quzara Cybertorch™

“Leveraging SOC Prime, we can now reach rules to detect the latest exploits and instantly deploy them to our customers’ workspace. SOC Prime genuinely enhances our real-time monitoring offerings, which is the biggest advantage any service-based cybersecurity company would want.”

Highlights

- Increased visibility into the emerging threats to ensure real-time monitoring of the in-house infrastructure and customers’ environments
- Streamlined Microsoft-based log source coverage tailored to the company’s security needs
- TTP-based threat detection based on the MITRE ATT&CK® framework v.10
- Automated streaming of the curated Azure-centric analytics rules directly into the customers environment

Challenges

Lack of Content Based on SIEM-Native Log Sources. As a cloud-focused Microsoft Intelligent Security Association (MISA) MDR provider, Quzara Cybertorch™ was looking for ways to stay updated on the latest detection content based on the Microsoft-native log sources to ensure full-stack coverage of their customers' environment. Apart from the Microsoft-tailored content, Quzara Cybertorch™ needed additional custom detections to add to its own curated Threat Intel databases, including data sources, like firewalls, matching the customers’ threat profiles.

Need for Custom SOC Use Cases with Minimum Fine-Tuning. Quzara Cybertorch™ has been striving to infuse their MDR Services and Technical Support with streamlined delivery of detection content that needed minor customization after its deployment to the customers’ cloud environment. Quzara Cybertorch™ was looking for a cost-efficient solution enabling access to curated use cases that could be seamlessly deployed to the customers’ instance with minimum SOC team time and effort needed for their fine-tuning.

Insufficient Visibility into Organization-Specific Threats. To help the company’s customers enhance their cybersecurity posture, Quzara Cybertorch™ was driven to enrich their MDR Services with proper threat modelling. One of the ways to reach this goal was obtaining detection content aligned with the MITRE ATT&CK framework that would ensure proper data source coverage against adversary TTPs.

Solution

Addressing the challenge of developing Microsoft-centric custom SOC use cases, Quzara Cybertorch™ leverages SOC Prime's Detection as Code platform offering the world's largest collection of SIEM & XDR algorithms. SOC Prime has become a highly anticipated solution enabling the automated delivery of Microsoft Sentinel analytics rules to the customers' environment, continuous threat coverage with a focus on the company-specific log sources and ATT&CK parameters, as well as reduced SOC team effort on content development and its further customization.

Achievements

Direct Access to Curated Microsoft-Native Content

By choosing SOC Prime as the industry-leading content provider, Quzara Cybertorch™ has gained direct access to detection content based on the data sources perfectly tailored to the company's threat profile and environment. Having the primary focus on Microsoft-centric content, Quzara Cybertorch™ has fulfilled their content needs with 5,000+ Azure Sentinel detections available in the extensive SOC content repository of the Threat Detection Marketplace. Reaching a wealth of analytics rules based on the Microsoft log sources, like Azure Active Directory logs, Microsoft Defender ATP, and Sysmon, enabled Quzara Cybertorch™ to boost detection coverage across the entire company's infrastructure.

Saved SOC Team Hours Through Continuous Content Streaming

With the Continuous Content Management (CCM) module powered by the SOC Prime's platform, Quzara Cybertorch™ can stream the latest analytics rules directly into the customers Microsoft Sentinel environment enabling protection against the constantly emerging threats. Leveraging the automated deployment capabilities of the CCM module, Quzara Cybertorch™ can now boost the content delivery potential with roughly 150 rules per quarter, which allows saving up to 600 SOC team hours.

Reduced SOC Team Effort on Content Customization

With access to 130,000+ detection and response algorithms available in the Threat Detection Marketplace content repository, Quzara Cybertorch™ can easily reach SOC use cases that are ready for deployment without substantial customization. The highly scalable capabilities of the Custom Field Mapping tool help overcome data complexity by adopting custom data schemas to different types of content and smooth out deployments of rules, queries, and functions to Azure Sentinel.

Proactive Defense Against the Most Anticipated Threats

SOC Prime's accelerated speed to market based on the ability to deliver critical detections within 48 hours after threat discovery has enabled Quzara Cybertorch™ to stay always vigilant against digital risks. The advanced content search capabilities of the SOC Prime's Detection as Code platform make threat detection even faster and simpler. Leveraging the Lucene-powered search based on CTI, the latest CVE, and exploits, Quzara Cybertorch™ can continuously track the most recently released rules within the scope of the organization-specific log sources.

This way, the company has instantly reached detection content related to the Kaseya VSA ransomware attack and SolarWinds RCE vulnerability (CVE-2021-35211) having all means to protect their customers right at their fingertips. By applying the threat-centric selection of SOC content based on the MITRE ATT&CK matrix, Quzara Cybertorch™ has empowered their threat discovery and detection capabilities with the TTP-based approach.

About Quzara Cybertorch™

Quzara Cybertorch™ is a Woman-Owned Small Business (WOSB), US Government (SBA) certified 8(a), General Services Administration (GSA) Multiple Award Schedule holder for Highly Adaptive Cybersecurity services (HACs) in every category. As a Microsoft Intelligent Security Association (MISA) member, cybersecurity services delivered by Quzara Cybertorch™ are primarily focused on the Microsoft Sentinel SIEM enabling the company's customers to proactively defend against the sophisticated attack vectors by means of Microsoft's cloud-based stack in use. Quzara Cybertorch™ provides MDR Services to Federal and Commercial customers. The company delivers cloud services, security analytics, enterprise security services, as well as helps organizations meet security control requirements and compliance with the government-wide Federal Risk and Authorization Management Program (FedRAMP) and such compliance frameworks as CMMC, NIST FISMA, NERC-CIP, HIPAA, and others. Learn more about Quzara Cybertorch™ at www.cybertorch.com