CASE STUDY

Bricata Scales Up Network Detection and Response

The Threat and Response Management team at PwC provides cybersecurity threat hunting and incident response services. The group wanted to scale up its network monitoring and detection capabilities beyond the tools it was developing in house.

PwC was looking for a product that could match their existing knowledge and the way the team was already performing its job. They also wanted technology that added more value, enabled engineers to work more effectively, and scaled their capabilities to allow them to work with larger networks and multiple customers.

"When we started having discussions with Bricata, we found their product was built to fit exactly with our recent thinking about network threat hunting. Bricata's advanced network detection and response (NDR) platform uses Suricata and Zeek, the open-source technologies we were already using, which made our learning curve fast and easy. Plus, **Bricata is scalable and optimized to monitor large enterprises that have consistent amounts of network traffic, which wasn't possible with the existing infrastructure we were using."**

Network visibility has always been critical for the PwC team because it allows them to provide faster, more efficient incident response and threat hunting, and help ensure customers' operational policies are enforced.

"Most security teams today aren't focused on the network as much as they should be. That's unfortunate because, when you don't have network visibility, you lose out on a lot of important security and operational information. **Everything generates some level of network noise. If you can quickly pick up on that noise, you can respond much more rapidly."**

Why PwC Chose Bricata

- Advanced network detection and response platform
- Leverages Suricata and Zeek open-source technologies
- Delivers complete visibility of heterogeneous networks
- Immediately identifies compromised systems
- Flexible customization to optimize for specific networks
- Easily integrates with SIEM, SOAR, EDR and other systems
- Dedicated team of passionate and responsive security experts

Rapid Response with Bricata

The Bricata NDR platform allows the PwC team to quickly gain complete visibility into the heterogeneous networks most enterprise customers have today.

"When you're doing incident response, your network is already compromised, and you need to respond rapidly. **If you don't have network visibility, containment is extremely challenging. With Bricata NDR, you can put one device on the network and, within minutes, get an immediate image of an entire infrastructure, without deploying any agents."**

PwC needed better and more efficient ways to dig into data and telemetry information and correlate information between events. The PwC team brings Bricata in during an incident to help them immediately identify which systems are infected, quickly partition them into a closed network and monitor their traffic to better identify the type of infection and how it operates.

"Most security teams today aren't focused on the network as much as they should be."

"If you don't have network visibility, containment is extremely challenging."

"Bricata is more open, gives us more control, and allows my team to more effectively monitor, customize and optimize a customer's environment."

What Bricata Delivers

"Bricata is more open, gives us more control, and allows my team to more effectively monitor, customize and optimize a customer's environment. We can go much deeper, even write our own detection levels, and the Bricata platform can be easily integrated with SOAR, EDR and other technologies. Finally, the Bricata team is dedicated, passionate and extremely responsive to our needs."

FOR MORE INFORMATION

BRICATA.COM | INFO@BRICATA.COM | 888.468.0610

BRICATA pwc