APRICOT 2026 Fellows Report

MasterClass 3: Practical Cybersecurity for Internet Operators

From 4–7 February 2026, I had the privilege of attending Master Class 3: *Practical Cybersecurity for Internet Operators* at APRICOT 2026. As a Security Analyst responsible for monitoring security events, analyzing threats, and supporting infrastructure protection, this Master Class was directly aligned with my professional responsibilities. The course provided not only technical knowledge but also valuable operational insight into how security mechanisms are implemented within real-world Internet environments, particularly for ISPs and organizations managing routing infrastructure.

Daily Learning Activities and Technical Experience

Day 1 – Building a Security Mindset

The first day focused on establishing a structured security mindset. The instructors emphasized that cybersecurity is not merely about deploying tools or reacting to incidents; it is about developing layered defenses, applying consistent operational discipline, and understanding the evolving threat landscape.

We explored foundational topics including physical security considerations, management plane protection, and Layer 2 security controls. Discussions around VLAN segmentation, access restrictions, and control-plane protection demonstrated how small configuration weaknesses can lead to large-scale vulnerabilities. For me, this reinforced the importance of secure baseline configurations as the first line of defense.

A key insight from the day was recognizing that many security incidents originate from operational oversight rather than sophisticated exploitation. Misconfigured management interfaces, weak authentication policies, and insufficient segmentation can all create significant exposure. As a Security Analyst, understanding these root causes improves my ability to identify systemic risks rather than focusing solely on surface-level symptoms.

Day 2 – Device Hardening and Routing Security

The second day shifted to device hardening and routing security fundamentals. We examined secure configurations for routers, including SSH best practices, access control lists, and management interface restrictions. These exercises provided practical reinforcement of defensive configurations that reduce unauthorized access risks.

From my professional perspective, this knowledge enhances my ability to correlate security alerts with infrastructure behavior. When investigating suspicious login attempts or anomalous

routing events, understanding how secure configurations should function allows me to detect deviations more accurately.

The afternoon sessions introduced BGP security concepts. We configured eBGP sessions, implemented prefix filtering, and applied routing policies to prevent route leaks and mis-origination. The lab environment simulated real inter-domain routing scenarios, demonstrating how insufficient filtering or validation can impact not only a single organization but also the wider Internet.

This practical exposure strengthened my appreciation of routing security as a foundational cybersecurity responsibility. It highlighted that prevention at the routing layer significantly reduces the likelihood of large-scale incidents.

Day 3 – Advanced Defensive Mechanisms

The final day concentrated on advanced routing security and mitigation techniques. One of the most impactful sessions covered Unicast Reverse Path Forwarding (uRPF). Through hands-on configuration, we observed how reverse-path validation mitigates IP spoofing by verifying that incoming packets have a valid return path. This mechanism demonstrated how infrastructure-level controls can block malicious traffic before it reaches monitoring systems.

We then explored Remotely Triggered Black Hole (RTBH) filtering. By simulating DDoS scenarios, we saw how routing policies can redirect malicious traffic into null routes to protect core infrastructure. This technique illustrated the importance of coordination between network engineers and security teams during active incidents.

Another critical component was Resource Public Key Infrastructure (RPKI) and Route Origin Validation (ROV). Configuring validator sessions and examining VRP tables clarified how cryptographic validation strengthens trust in BGP announcements. Before APRICOT, I understood RPKI conceptually; however, the lab transformed theoretical knowledge into operational capability.

In addition to routing security, sessions on DNS security, vulnerability management, and incident response reinforced a holistic approach to cybersecurity. The tabletop exercises emphasized structured communication, coordination, and decision-making during simulated incidents.

Professional Perspective as a Security Analyst

Participating in this Master Class significantly broadened my operational perspective. As a Security Analyst, my role typically focuses on detection, investigation, and response. However, this training reinforced the importance of preventive controls at the infrastructure layer.

Mechanisms such as uRPF, RTBH, and RPKI directly reduce the volume and severity of malicious traffic reaching detection systems. Understanding how these technologies function

allows me to better interpret anomalies, identify routing irregularities, and recommend proactive improvements.

The Master Class strengthened my belief that cybersecurity must be proactive rather than purely reactive. Monitoring tools and alerts are essential, but secure baseline configurations and routing validation mechanisms significantly reduce attack surfaces. This integrated approach improves resilience and enhances collaboration between security operations and network engineering teams.

Networking with Fellows and APRICOT Participants

Beyond technical learning, APRICOT 2026 offered valuable networking opportunities. Engaging with fellows from different countries allowed me to gain insight into diverse operational environments and regional challenges.

Discussions during breaks and social events, including the Gala Dinner, created meaningful opportunities to exchange ideas about routing security implementation, incident response coordination, and policy frameworks. These interactions broadened my understanding of how organizations with varying resources approach similar cybersecurity challenges.

The diversity of participants enriched the overall experience. Observing different analytical approaches and problem-solving methods encouraged me to evaluate security challenges from multiple perspectives. These connections also established a foundation for future collaboration within the regional Internet community.

Commitment to Knowledge Sharing and Return Service

Upon returning to my organization, I am committed to sharing the knowledge and experience gained from APRICOT 2026. We conduct regular internal knowledge-sharing sessions, and I plan to present key topics from the Master Class, including BGP hardening, uRPF deployment considerations, RTBH mitigation strategies, and the fundamentals of RPKI and Route Origin Validation.

My objective is not immediate deployment of every technology discussed, but rather structured evaluation and awareness-building. Technological improvements require careful planning and change management; however, exposure to best practices strengthens long-term resilience.

By sharing these insights internally, I hope to contribute to enhanced routing security awareness and improved collaboration between network operations and security teams.

Conclusion

I am sincerely grateful for the opportunity to attend APRICOT 2026 and participate in Master Class 3. The experience expanded my technical expertise, strengthened my operational awareness, and reinforced my commitment to continuous professional development.

As a Security Analyst, the knowledge gained from this Master Class will directly support my ability to analyze routing-related threats, recommend preventive controls, and contribute to a more secure and resilient network infrastructure. I look forward to remaining engaged with the APRICOT community and applying these lessons to strengthen cybersecurity practices within my organization and the broader regional Internet ecosystem.