Proceedings of the 15th International Conference on Quality and Dependability
Sinaia, Romania, September 14th-16th, 2016
ISSN 1842-3566
Pages 150-155

Migration of a SOC to SIC Security Operations Center vs. Security Intelligence Center The use of Honeypots for Threat Intelligence

Ionuţ-Daniel BARBU, Cristian PASCARIU, Ioan C. BACIVAROV
EUROQUALROM - ETTI, University "Politehnica" of Bucharest, Romania
barbu.ionutdaniel@gmail.com, crpascariu@gmail.com, bacivaro@euroqual.pub.ro

Abstract
The purpose of this paper is to emphasize the advantages of transitioning from the classic Security Operations Centers into an advanced model that leverages intelligence to understand and anticipate threats targeting the organization. By tackling the proactive vs. reactive approach towards cybersecurity it is intended to present a comparison between the two models. Initially it focuses on the ability to anticipate threats before they become incidents and also on the drawbacks of the classical SOC including the reactive security posture and monitoring. Furthermore, the article analyzes the impact of such a transition to both processes and people. It is worth mentioning the automation aspect of the migration which enables the human to separate from routine activities, allowing them to focus on the intelligence gathered. As the enterprise oriented tools from various vendors are intended to work for everyone but are optimized for no one, the authors highlight the importance of deploying custom tools supported by knowledgeable engineering teams. On that matter, the final part of the paper is dedicated to honeypot deployment by underlining their benefits from a Threat Intelligence perspective.

Keywords: SOC, SIC, Threat Intelligence, APT, HoneyPots

References:

[1] SOC vs. SIC: The Difference of an Intelligence Driven Defense Solution, Lockheed Martin Corporation - Reviewed 2nd of March 2016
[2] The Six Stages of Incident Response, Dark Reading, 2007 - Reviewed 14 of May 2015
[3] http://www.lockheedmartin.com - Reviewed 28 of March 2016
[4] https://en.wikipedia.org/wiki/Advanced_persistent_threat - Reviewed 2nd of May 2016
[5] https://technet.microsoft.com/dynimg/IC78017.jpg
[6] https://en.wikipedia.org/wiki/Honeypot_(computing) - Reviewed 3rd of June 2016
[7] Naveen, Sharanya. "Honeypot" - Reviewed 1st of June 2016.
[8] Lance Spitzner (2002). Honeypots tracking hackers. Addison- Wesley. pp. 68-70. ISBN 0-321-10895-7. - Reviewed August 2014
[9] BARBU, I.D., PETRICĂ, G. (2015). Defense in Depth Principle to Ensure Information Security. International Journal of Information Security and Cybercrime, 4(1), 41-46. Retrieve from http://www.ijisc.com

Proceedings of the 15th International Conference on Quality and Dependability
Sinaia, Romania, September 14th-16th, 2016
ISSN 1842-3566
Pages 150-155
[10] MIHAI, I.C., PRUNĂ, Ș., BARBU, I.D. (2014). Cyber Kill Chain Analysis. International Journal of Information Security and Cybercrime, 3(2), 37-42. Retrieve from http://www.ijisc.com
[11] An introduction to threat intelligence, CERT-UK - Reviewed July 2015
[12] http://www.honeyd.org/concepts.php - Reviewed September 2015