Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXII, Issue 88, October-December 2016
Pages 11-16

Threat Intelligence Based Security Operations Centers

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

Abstract
With the advent of complex techniques, tactics and procedures used by the adversaries, Security Operations Center are starting to become obsolete. This paper changes the focal point to an advanced model that leverages intelligence to understand and anticipate threats targeting the organization. One of the most important aspects of this model is represented by this ability of anticipating threats before turning into incidents and moreover it highlights the proactive vs. reactive approach towards cybersecurity. Using this format, in the following pages the authors intended to build a comparison between a Security Operations Center and Security Intelligence Center by analyzing the impact of and steps needed for such a transition to both processes and people. Needless to say, it is critical to dedicate numerous and valuable resources to the automation aspect of such a migration. In this way management will enable the analysts and engineers to separate from routine activities, allowing them to focus on performing threat hunting against 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. Based on the authors' research one of the initial steps and perhaps one of the most effective projects on this matter would be the implementation of a honeypot environment for obtaining tailored IoCs.

Keywords: IT Security, Cyber-Security, 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.
[10] Mihai, I.C., Prună, Ş., 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.

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXII, Issue 88, October-December 2016
Pages 11-16

[11] An introduction to threat intelligence, CERT-UK – Reviewed July 2015.
[12] http://www.honeyd.org/concepts.php – Reviewed September 2015.