Watching the Internet of Things - The Convergence of Monitoring

Dale C. Rowe
Brigham Young University
dale_rowe@byu.edu

Sarah Cunha
Brigham Young University
scunha@byu.edu

Abstract

Today, the typical enterprise network provides infrastructure for applications, websites, servers, workstations, tablets and smartphones. Wearables, appliances and vehicles are rapidly being added to this list. Each device comes with unique requirements regarding connectivity, services, usability and security that much be addressed as organizations move forward. Many businesses must also work in multi-owner Bring-Your-Own-Device environments, where employees, contractors and guests may bring devices to the premises that require connectivity.

This proliferation of devices and diversity of platforms can present a variety challenges when providing a reliable and well-connected infrastructure. These challenges may include determining performance requirements and scalability, assessing application reliability, determining risk, and investigating suspicious incidents. Many larger organizations create teams to take responsibility for these challenges such as: network engineering, development operations, systems administration, risk management and incident response teams.
Each of these teams has a variety of tools at their disposal to help deliver necessary business capabilities. Notwithstanding the overlapping capabilities of many tools, ownership of a tool is often seen as a necessary pre-requisite to utilization. Yet progress is made towards infrastructure-as-a-service (IaaS) there is a growing trend to replace the need for ownership with operational needs. Tool capabilities are rapidly overcoming the need to own and fully manage.

In this paper we discuss how we have created a standardized platform for massive log analytics across multiple platforms, and used this to replace or supplement traditional tools for multiple types of information-technology teams. We introduce our case study which led to the development of this platform and next explain how the architecture has been adapted to cope with peak loads of over 100M events per minute. We explain design constraints and limitations of the system and conclude with a study of the sytems operational benefits to each team type.

We have found our approach to be both innovative and advantageous in its capability to present relevant data with key system indicators for a variety of different mission objectives.

Proceedings of the 2016 IAJC-ISAM Joint International Conference
ISBN 978-1-60643-379-9

Biographies

DALE C. ROWE is an assistant professor of Information Technology at Brigham Young University and Director of the Cyber Security Research Laboratory. He maintains a variety of security certification including a CISSP. Dr. Rowe's scholarly interests include most security topics and he enjoys keeping his technical skills up to date. In 2011, he created and maintains a student Red Team which frequently conducts penetration tests a service to the local community. In the past 4 years he has mentored 6 cyber defense (CCDC) student teams who have received 1st place 4 times over including the regionals in 2016. Prior to joining BYU in 2010, he worked as a systems security architect in the aerospace industry. Dr. Rowe may be reached at dale_rowe@byu.edu

SARAH CUNHA is a senior in the Brigham Young University Information Technology program and a Systems Administrator in the Cyber Security Research Laboratory. Sarah's interests include systems and network administration and systems security. Sarah was on the regional Cyber Defense Competition (CCDC) team in 2016 and with her team placed 1st in the contest. Sarah will pursue a Masters in Information Technology with an emphasis in Cybersecurity in 2016. She can be reached at snarsher1@gmail.com