Matthew Development Plan to Senior Analyst

By: Matthew Riedle (Security Analyst)

Goal: Matthew promoted to Senior Analyst on August 1, 2018

Sponsor: Bill Billings

Action Items

1. ~~Matthew complete plan~~
2. ~~Confirm plan with Andrew~~
3. ~~Andrew confirm plan with Bill~~
4. ~~Andrew confirm plan with Paul S~~
5. Matthew track progress on improvement areas
6. Matthew chat with Bill on promotion

**Description:**

This plan proposes the business value of promoting Matthew to Senior Analyst on September 1, 2018, as well as improvements Matthew will make to meet or exceed the expectations of Senior Analyst at Castlight.

**Business Value of Promotion:**

1. Gives more weight to Matthew’s role, which is important with internal employees, as well as the IDC Security Monitoring team.
2. Empowers Matthew with a greater sense of responsibility, aligned with working more with other teams across Castlight, as well as the Security Vendors.
3. Can inspire and exemplify the reward for hard work to Security, and other Castlight employees.

Work Expected of a Castlight Senior Analyst

* **Being One Team** - While an Analyst will work on the tasks assigned to him, a Senior Analyst will look to how the things under his control benefits other teams at Castlight. By enabling communication, developing relationships, and establishing common goals, a Senior Analyst will demonstrate how accomplishing Security goals can be a benefit to the goals of other teams.
* **On a Mission** - While an analyst is able to work on the tasks assigned to them, a Senior Analyst knows the priorities across the company and is able to align the priority of his tasks with that of Castlight’s priorities.
* **Getting things Done** - A Senior Analyst is proactive in improving the overall Security posture of Castlight and manages the tools so that the Security team is able to have a more complete understanding of what happens within the Castlight environment.

Work Completed by Matthew consistent with Senior Analyst

* **Being One Team** - As an Analyst, Matthew had a goal of being able to work with other teams, and identify ways that his work can be a benefit to other teams across Castlight. Once such example was the implementation of the new File Change Monitoring tool (Tripwire) to assist with SOC2 reports. This cut down on the amount of logs the Resilience team needed to gather for the Security Compliance team to present to auditors. Matthew has kept his finger on the pulse of the greater security industry by checking in with others around the world and in different companies. This has allowed Matthew to become aware of new security issues around the world (such as WannaCry / NotPetya) as soon as others begin discussing and investigating them. Matthew has also written a few articles addressing such alerts in an effort to bring awareness to Castlight as a whole, as well as identified any susceptibility to them within Castlight’s network. Lastly, Matthew has developed a strong working relationship with the Resilience team allowing him to assist with overseeing some of their projects and point out how they assist with Security’s goals, such as patching servers across all of the environments for major vulnerabilities (like Meltdown and Spectre).
* **On a Mission** - As an analyst, Matthew has completed several major projects such as new tool implementations and more efficient configurations of existing tools. Consistent with being a Senior Analyst, Matthew was able to focus his work on projects that were the most beneficial to Castlight. As a first example, Matthew was able to complete a couple of pre-existing projects, Shape Security and Imperva Database Activity Monitoring, that were major milestones in trying to get a key customer (KPMG) signed on. Another example came about as part of the internal Ekko audit. As a result of one of the findings, Matthew oversaw log management to ensure logs are routed to the SIEM system from all primary servers. A last key priority was to oversee a WAF tool replacement to ensure all traffic with DiffieHelman ciphers are being monitored.
* **Getting things Done** - As an analyst, Matthew was diligent with the tasks assigned to him. One example was clearing out a major backlog of Security Monitoring tickets which had been building up before Matthew was hired. Consistent with a Senior Analyst, Matthew was able to take a proactive approach to some of the tasks in order to more efficiently align the workload of the IDC Security Monitoring team. As a first example, Matthew developed handling procedures for the different tickets in the Security Monitoring queue and trained a team in India to handle the alert tickets. This provided direction, while allowing Matthew to be hands off with the queue. Another example is that Matthew identified tool configurations that were generating false positives and minimized the amount of false positive alerts flowing into the Security Monitoring queue, reducing the amount of alerts that needed to be analyzed on a daily basis. As a final example, Matthew identified alert configurations that could be leveraged with additional alert sources to provide better correlation of events, yielding Security Monitoring alerts that are more fruitful.

List of Accomplishments

1. Monitored new security issues around the world (such as WannaCry / NotPetya) and write articles addressing the alerts, as well as identified any susceptibility to them.
2. Oversaw major vulnerability (Meltdown / Spectre) patching for servers.
3. Implemented new File Change Monitoring tool (Tripwire) to assist with SOC2 reports.
4. Oversaw WAF tool replacement to ensure all traffic with DiffieHelman ciphers are being monitored.
5. Finalized the Shape implementation under key customer (KPMG) deadline.
6. Finalized the Imperva Database Activity Monitoring under key customer (KPMG) deadline.
7. Oversaw log management to ensure logs are routed to the SIEM system from all primary servers.
8. Cleared out major backlog of Security Monitoring tickets.
9. Developed handling procedures for the different tickets in the Security Monitoring queue.
10. Assisted with leading and training the IDC Security Monitoring team.
11. Identified tool configurations that were generating false positives and minimized the amount of false positive alerts
12. Identified alert configurations that could be leveraged with additional alert sources to provide better correlation of events

Achievements Needed Before Senior Analyst

* **~~Improve Interdepartmental Communication~~** ~~- Matthew will need to lead a presentation, in order to demonstrate successful completion of a project, to key department leadership.~~ **~~Measured~~** ~~by completion and feedback.~~
* **Increase Security Infrastructure Transparency** - Matthew will document tool infrastructure, purpose, and tool maintenance for top 5 Security tools. **Measured** by completeness of articles and ability to implement feedback. (Shape, Signal, Tripwrire, Alertlogic)
* Andrew considering Secmon Maturity improvement based on - <https://docs.google.com/spreadsheets/d/1_gy_Q-B3YJ7-cWSGv94EJHoKZVBunMDbElZvbPiFies/edit#gid=900914334>