Polaris Sight – Industry Engagement

### Incident Response Team

**Q:** Hi Rachael, thank you for taking the time to answer a few questions I have about your team and your initial opinion on our product. To begin, on an average day what would be the most common incidents your team handles?

**A:** On average the most common incidents our team handles are:

* Phishing campaigns
* Brand spoofing
* Admin alerts

**Q:** Could you please elaborate on what these types of incidents are?

**A:** Sure, firstly phishing campaigns are spam emails we detect through our gateway either reported by our employees or detected by our email analysis tools. These spam emails are classified as phishing if they lure a user to provide sensitive information or are motivated to infect the user.

While efforts are made to ensure spam emails don’t make it past our firewall, a small percentage will find ways to bypass it.

The second type of incident is brand spoofing. In summary these are malicious actors attempting to imitate our apps and websites. This is monitored by our team and processes are in place to remove these occurrences of brand spoofing when they occur.

Finally, the third type of incident is admin alerts. We receive these alerts in our SIEM which monitors for unusual behaviour in relation to an admin account or the creation of a new admin account that cannot be verified.

**Q:** When these incidents occur, what is the process to resolve them?

**A:** When an incident occurs in response to either an employee reporting it or via an alert from our SIEM, we need to have a meeting and create an LOE (Line of Effort).

This will involve firstly determining the possibilities for this incident. Such as whether this incident has been caused by a malicious actor or whether it is a false positive caused by maintenance changes internally. Evidence is gathered to make this conclusion and resources are allocated in response to the severity of the incident.

When an LOE is created, the incident response team is divided into smaller teams assigned to a different possible source of the incident whether that is investigating the possibility of a malicious actor or a false positive. A team member is assigned throughout the investigation to create meeting minutes and record what had been discovered from the initial investigations. This is done to ensure that the next team to take over the investigation is informed what progress had been made so far. This is a precautionary action in case the incident goes all night requiring a second team to relieve the first one.

When the type and source of the incident has been determined then a variety of actions can be made to resolve it. For the common incidents mentioned before, there are templates that can be followed to resolve them. These would include for example in regards to a phishing campaign blocking the sender and ensuring the impacted users have their infected workstations cleaned, for brand spoofing raising a takedown order with the legal team or for admin alerts sending a request of information to the relevant team the alert is coming from.

**Q:** When investigating and resolving these incidents, what tools are used to assist this?

**A:** That’s a broad question as the tools we use can really vary depending on what kind of incident it is. At a basic level we will use PowerShell to collect hashes that might be required to determine whether a malicious actor has modified a resource owned by us or to determine whether say a fake app is indeed a fake and not officially issued by us.

We have email analysis tools that we can use to monitor what’s received in our gateway and to determine whether the email is malicious. If alerts are raised that an email might be suspicious we’ll load it in a virtual machine outside of our network to test what happens if the suspicious attachment or link in the email if it is opened. Free tools such as virustotal and Cisco Talos Intelligence we’ll be used to scan hashes that might be linked with viruses or to determine the reputation of a sender and their IP address. More advanced tools are kept in-house and will be used to create searches through our logs for particular indicators that might assist in our investigations.

As we are a large organisation, we have the advantage of being in contact with a variety of other IT teams such as infrastructure, app development, software as a service etc. We’ll usually contact these teams to gather information from the tools they have at their disposal.

**Q:** When performing your investigations, could there be anything that would improve your tools or the overall process of the investigation?

**A:** We do face an issue in regards to receiving too many logs in our SIEM which can cause backlogs if things are not calibrated carefully. This is a risk that’s monitored and faced by other incident response teams. When you have a variety of tools monitoring and collecting logs for multiple events, the database handling them can become bogged down and begin to struggle unless filters are put in place to only store the most relevant logs. This will only grow to become a more pressing issue in the future as legal requirements are in place to also require logs to be archived.

In an ideal world, it would be good to scan and store as many logs as we’d like. However this is not an ideal world and we face many limitations in regards to this. If we attempted to increase the amount of logs we had, we’d run the risk of delaying alerts we receive that would otherwise be received sooner if we didn’t have such a backlog. Additionally, we’ve found difficulties doing historical searches that go back multiple months as the database storing the logs struggles when it comes to these types of searches.

**Q:** Are there any solutions to this problem of backlogs and doing historical searches through logs?

**A:** There are alternative SIEM that don’t use a traditional database to index logs. Instead the logs are stored as compressed flat text files allowing a higher amount of logs to be stored. Importantly, this makes searches through the logs faster and it’s able to handle historical searches going back multiple months.

**Q:** From my explanation of our product, would you see it as a useful product for an incident response team?

**A:** I’d certainly agree that the product would have an important use for an incident response team. However from my understanding, the product is a mini SOC (Security Operations Centre) that has a friendly user interface. For a large organisation like mine, we’d probably not need it as we are already established and have the necessary tools for our security operations. The need for this product would be more found in small businesses and government departments who previously didn’t require an incident response team.

**Q:** Thank you for your time Rachael, this interview has been insightful in how an incident response team works and the challenges facing incident response. Before finishing up, are there any additional challenges your team faces that require a tool to resolve them?

**A:** Not so much as a challenge as rather a change in how cyber security is practiced. In the past, the main focus for cyber security was prevention either with applying the latest patches or ensuring cyber security rules are enforced. Today this has changed with a growing focus on detection as incidents such as Wannacry or Spectre have shown that prevention is only part of the solution. We need tools better geared for also detecting how many users are infected when prevention fails to assist in isolating the spread of the virus or movements of the malicious actor.