Wireless Intrusion Prevention System (WIPS) Report

Rouge AP Scan

1st October’2019 – 31st December’2019

Contents

[Summary 3](#_Toc18638365)

[Approach 3](#_Toc18638366)

[Scope 3](#_Toc18638367)

[Findings 3](#_Toc18638368)

[Enumeration 3](#_Toc18638369)

[Conclusion 4](#_Toc18638370)

[References 4](#_Toc18638371)

# Summary

The purpose of this document is to outline the findings associated with the rogue access point scanning which is an ongoing process. This scanning and testing activities are carried out with the help of wireless technology developed by Aerohive, the detailed report about each task and our findings are described below.

The purpose of this scan was to determine if there were any non-sanctioned wireless access points connected to the network at the location tested. The scan was carried out passively and at no point was any device in danger of harm.

## Approach

* No packets of information were sent from the scanning machine.
* Any handshakes or other sensitive information caught were deleted immediately.

During the scan, the machine listened to all wireless traffic for at least 5 minutes. Access point SSIDs were recorded as well as the encryption on those networks.

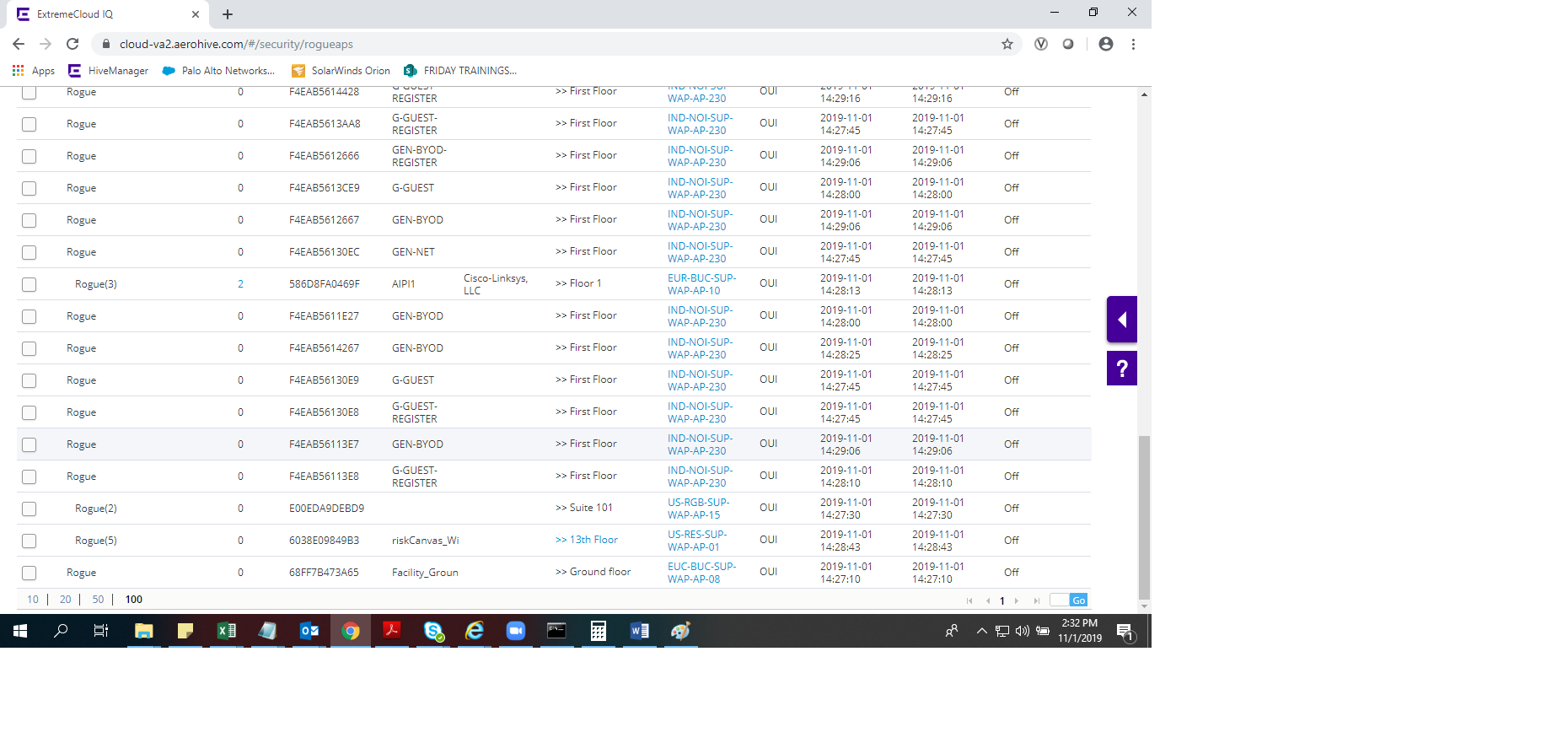
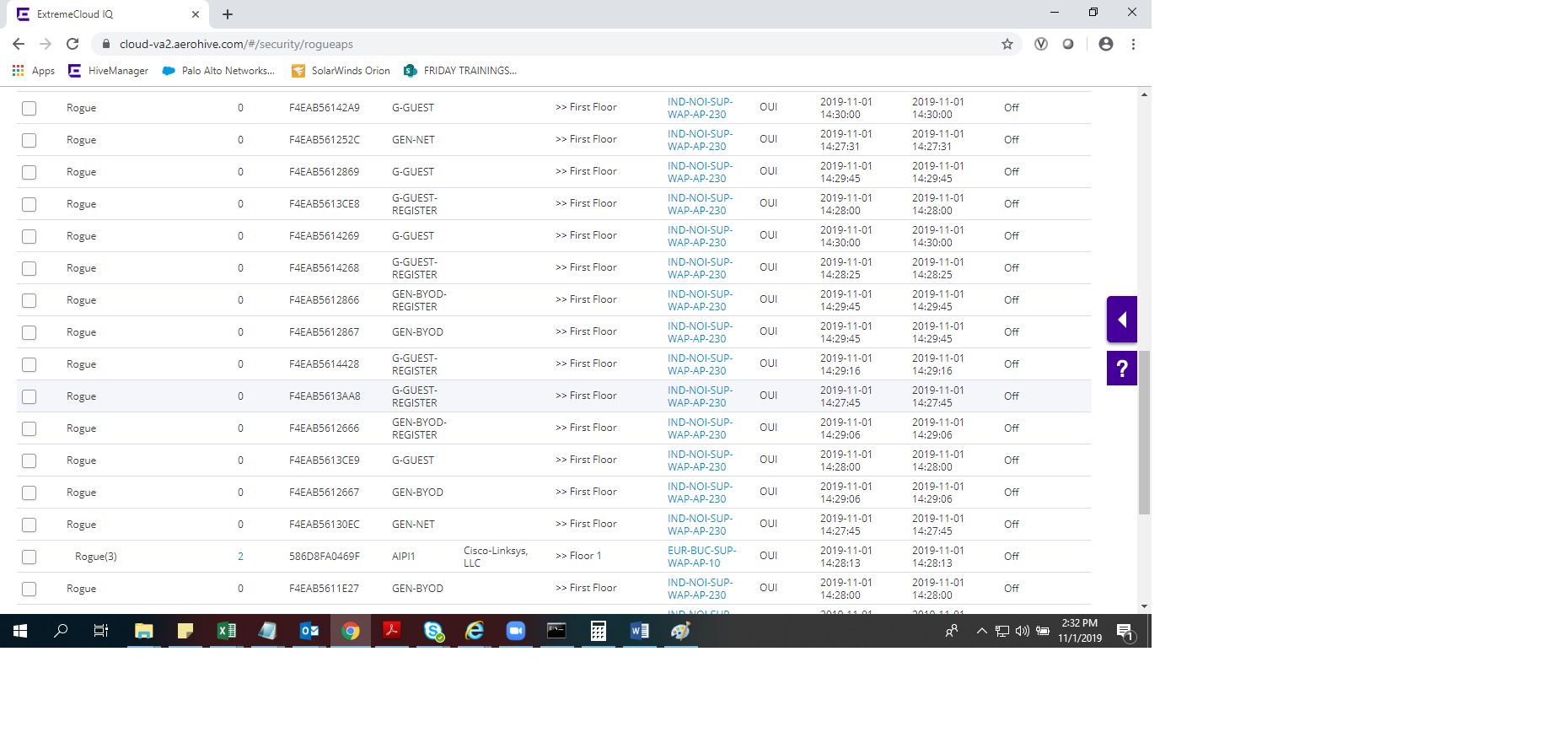
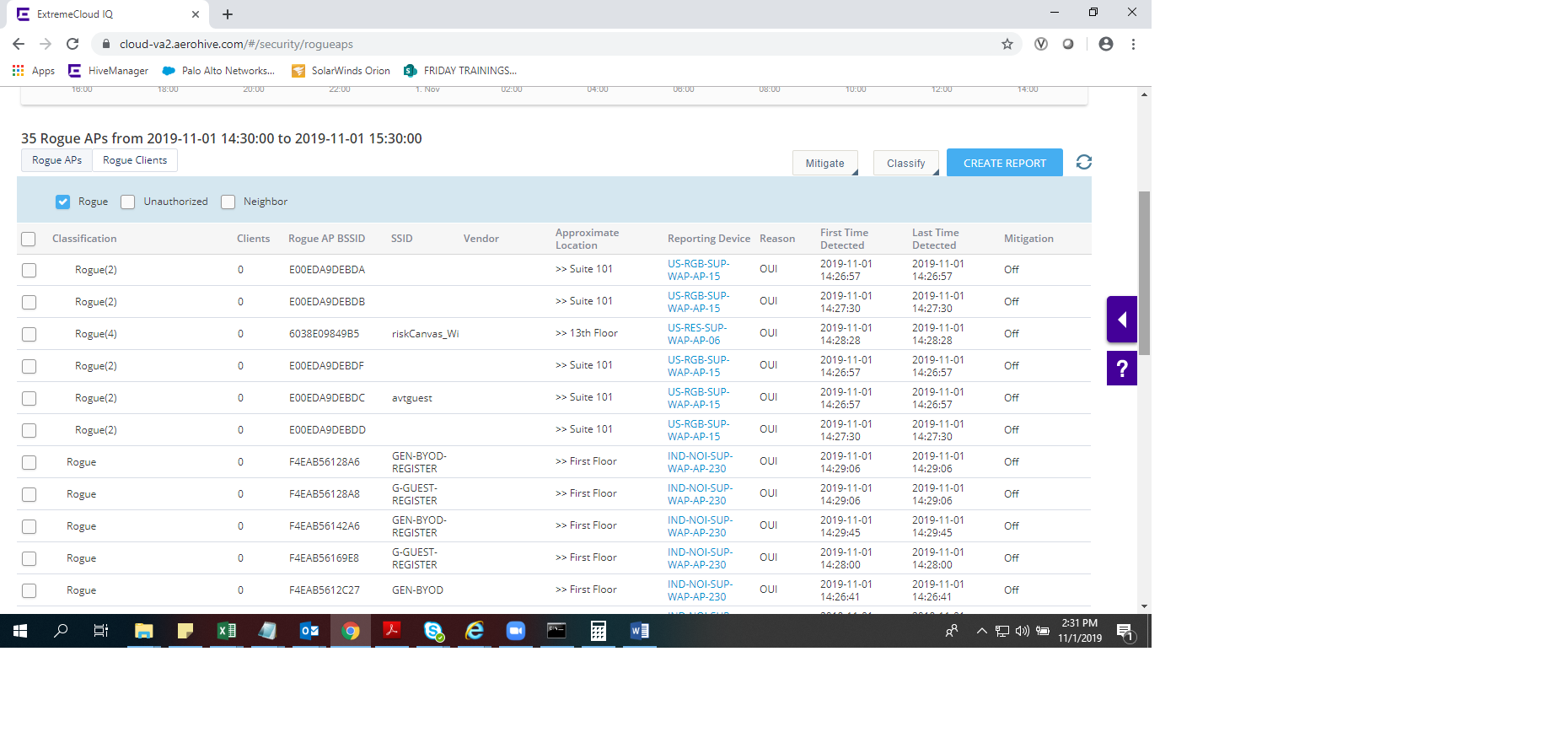
## Scope

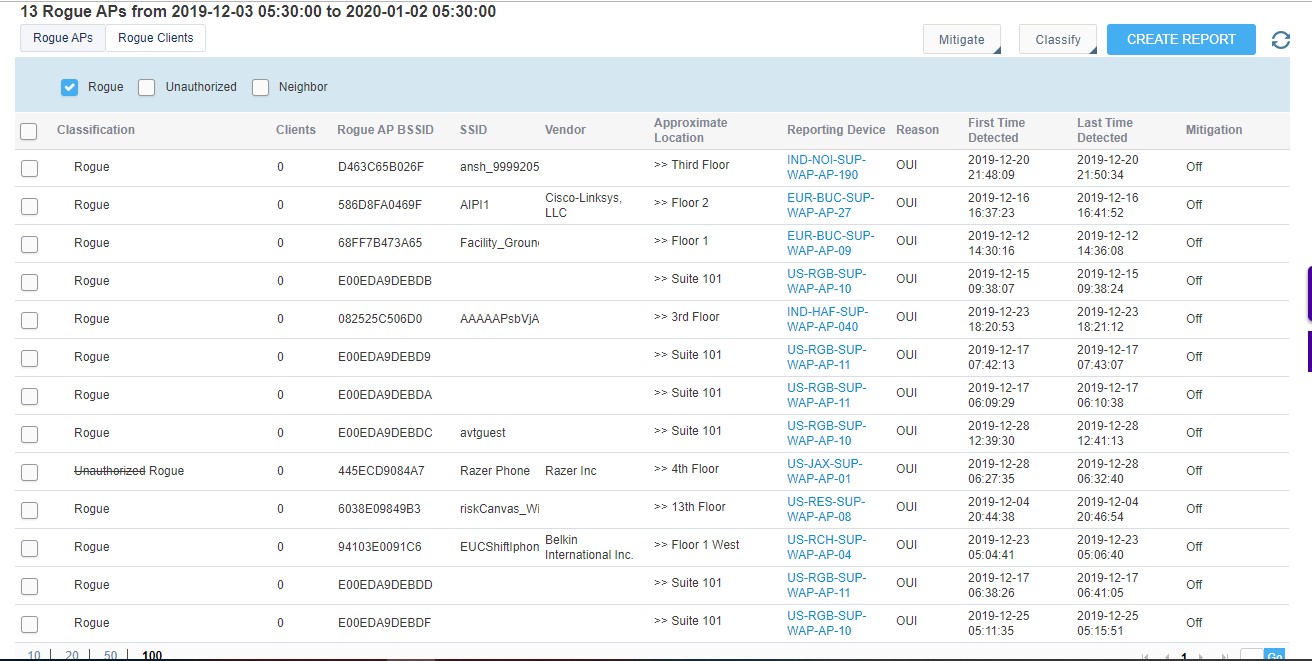
The scope of this test was limited to the traffic broadcast on all 14 2.4 GHz channels.

# Findings

## Enumeration

Below is the information we were able to extract from the network scans:





# Conclusion

Our testing found that there were no unauthorized wireless access points connected within Genpact environment where Aerohive is integrated...

# References