# Monitoring Abnormal Process Behavior with Python



Sean Wilkins
Network Engineer & Author

swilkins@infodispersion.com

www.infodispersion.com

### Module Introduction

Move on from IP Tracking

Moved into monitoring processes



### Overview



- Reviewing Processes for Abnormal Behavior
- Concepts Demonstration Abnormal Process Behavior

# Abnormal Process Monitoring

Discuss the process of process monitoring

Split into two goals:

How to use the psutil module

Filtering data to show resource usage



# Abnormal Process Monitoring



#### Multiple python modules will be used

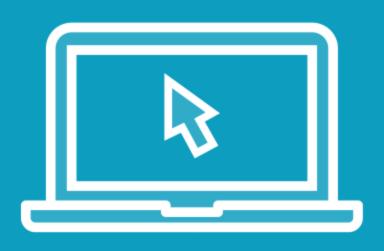
#### Including:

- psutil
- time and sys
- pprint
- os

# Let's move into our demonstration environment!



## Demo



How to display system processes

Creating a process resource monitor

## Summary



- Reviewing Processes for Abnormal Behavior
- Concepts Demonstration Abnormal Process Behavior

