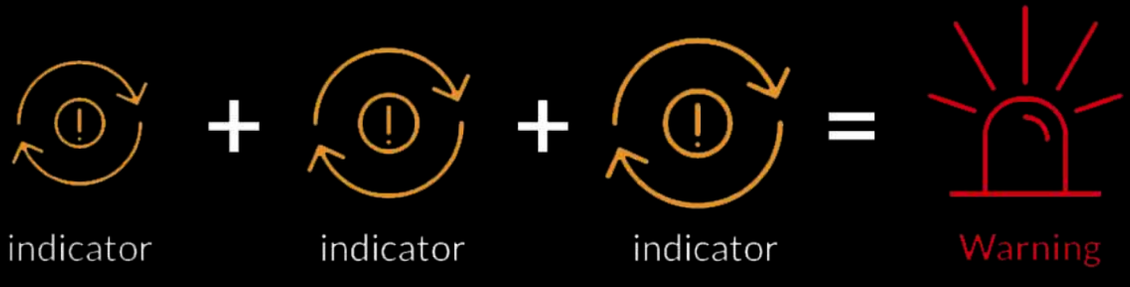
coordinates°

cor. Security Operations Center

SECURITY INCIDENT REPORT

Prepared for: ATOMZ
Recurrence: Monthly
Version: Sample Report
Date: 02-JAN-2019



coordinates

cor. Reporting

REPORT INFORMATION

Report # COR-IR-9210

Date / Time 02 JAN 2019 08:00PM

Prepared for ATOMZ

Threat Level

04 / 10

INCIDENT SUMMARY

Incident ID
Enter unique incident identifier

Breach Type
Enter breach type (Standard, Phishing, Malware etc.)

Incident Severity
Enter severity (Low, Medium, High etc.)

Occurrence Date
Enter occurrence date

Closure Date
Enter closure date

Time to Resolution
Enter resolution time

Reason for Closure
Enter reason for closure (resolved, duplicate incident, false positive etc.)

Earliest Flagged Evidence
Describe first piece of evidence flagged

Most Recent Flagged Evidence
Describe most recent piece of evidence flagged

Incident Owner
Enter owner's name

Closure Notes
Enter any custom notes relevant to the incident

Custom Data
Describe any custom data sets used for the incident

INVESTIGATION TIMELINE

EVENT ID 3332
DATE 02 JAN 2019
TIME 08:00PM
OWNER <Enter Name>

Task Type
Task Details
Task Owner
Indicators used in the task
Indicators that the task threw up as results
Change / Modification to incident
Other task specific criteria

Incident Name
Occurrence
Type
Severity
Area of impact

INVESTIGATION INDICATORS

Value	Reputation	Type	Source	First Seen	Last Seen
8738GH383738ATW21	Bad	File MD5	Email	Timestamp	Timestamp
...	...	...	...	...	...
...	...	...	...	...	...

COLLABORATION NOTES

Analyst-specific notes relevant for posterity. For example:
- *Specific actions taken by the analyst and underlying reasons.*
- *Chats between analysts to highlight how they arrived at a certain decision.*
- *Thought process behind identifying key evidence pieces.*
- *Product integrations used and underlying reasons.*
- *Learnings for similar incidents in the future.*

EVIDENCE TIMELINE

Evidence ID
Enter unique evidence identifier

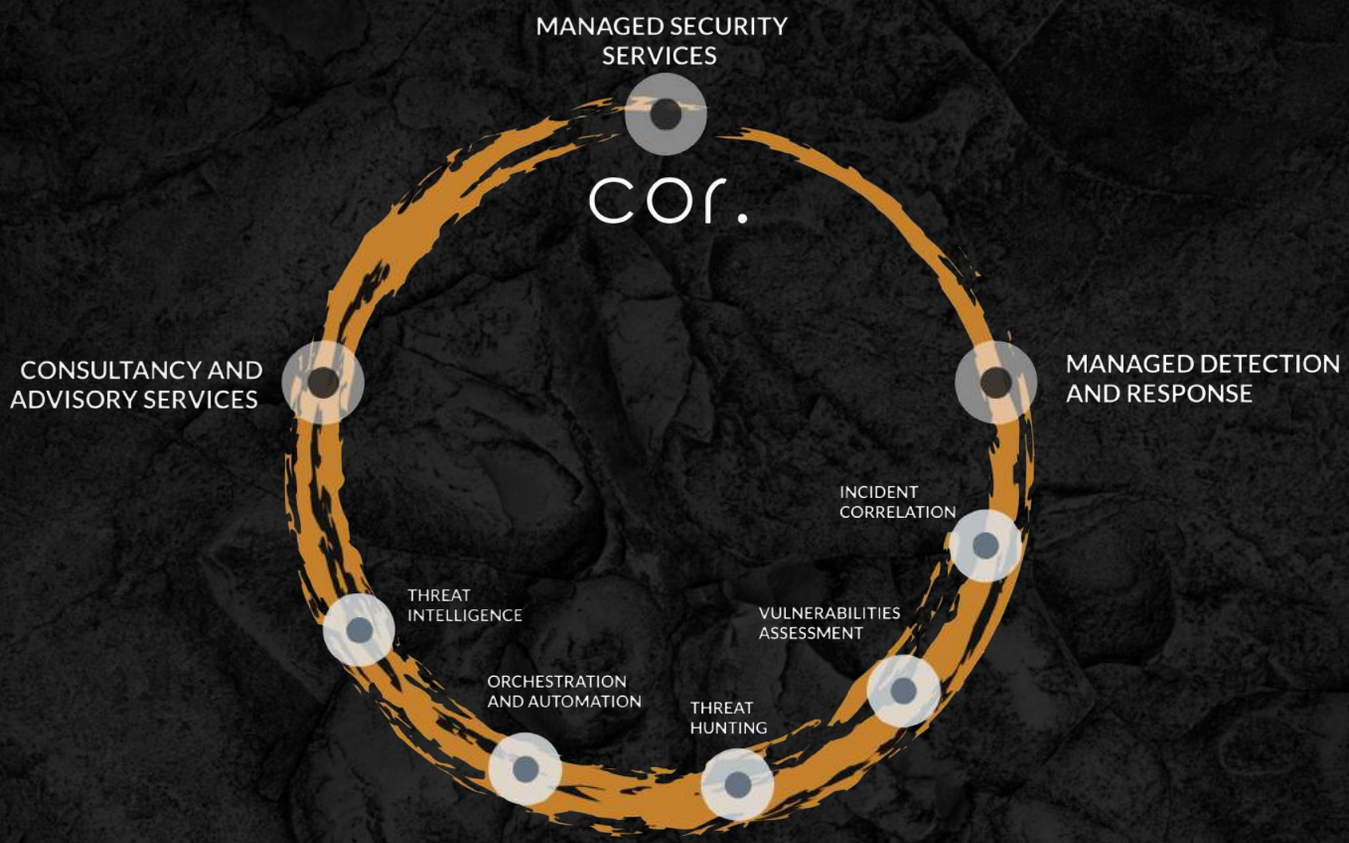
Evidence Header
Enter evidence title/short description

Date/Time Occurred
Enter occurrence timestamp

Evidence Details
Enter all salient details of the evidence that are useful for future reference, for example:

CbID	00000006-0000-0870-01d3-5ecdf2636840-00000001
CbSegmentID	1
CommandLine	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2472 CR
Hostname	WIN-6OR88OJLK5U
MD5	41c5d70956a565f7ae1979c9c165ea84
Name	iexplore.exe
PID	2160
Parent Name	iexplore.exe
Parent PID	2472
Path	c:\program files (x86)\internet explorer\iexplore.exe

* * *



coordinates

CLOSING THE GAP IN THE FIGHT AGAINT CYBER THREATS