IT Data Collection Summary

Topics

- Types of Data Captured
- Examples of Data
- How Data is Used

IT Data Collection Summary

Types of Data Captured

Data Source: Technology used are devices themselves such as servers, workstations, network appliances and most network attached devices. Data collected is consolidated into tables using excel and charts.

1. Syslog
2. Microsoft Windows
3. Network Security
4. Application

IT Data Collection Summary

Types of Data Captured Example: Syslog

All logs created by network devices such as firewalls, routers, switches, etc., which are used for monitoring and trending computer network traffic patterns and/or detecting unauthorized network traffic.

o *May 11 10:40:48 scrooge disk-health-nurse[26783]: [ID 702911 user.error] m:SY-mon-full-500 c:H : partition health measures for /var did not suffice - <u>still using 96% of partition space</u>*

IT Data Collection Summary

Types of Data Captured Example: Windows

These logs are used to monitor activity on city network servers/workstations including successful/unsuccessful login attempts, file system access, hardware performance, etc. These logs provide detailed information about city network account ID's, file system structure, and hardware profiles.

o

```
03/26/2018 01:49:40 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4625 EventType=0 Type=Information computerName=NAME.cityofmadison.com TaskCategory=Logon OpCode=Info RecordNumber=4681591341 Keywords=Audit Failure Message=An account failed to log on.
```

IT Data Collection Summary

Types of Data Captured Example: Network Security

All logs created by network security devices such as the anti-virus appliance, anti-SPAM appliance, content filtering appliance, etc., which are used to monitor specific types of unauthorized or malicious traffic on the city network. These logs identify specific network traffic patterns and/or protocols that are allowed or disallowed on the city network.

```
Mar 26 16:14:00 servername Server:  Message: 1016955, servername / workstation name 00001, 2018-03-26 11:11:08 , domain\xxxxx, Real-time file system protection, Warning, file, C:\Users\xxxxxx\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE0\HLUFPUHB\flashplayer_34.9.1_plugin[1].js, JS/TrojanDownloader.Agent.QJG trojan, deleted, Event occurred on a new file created by the application: C:\Program Files (x86)\Internet Explorer\iexplore.exe
```

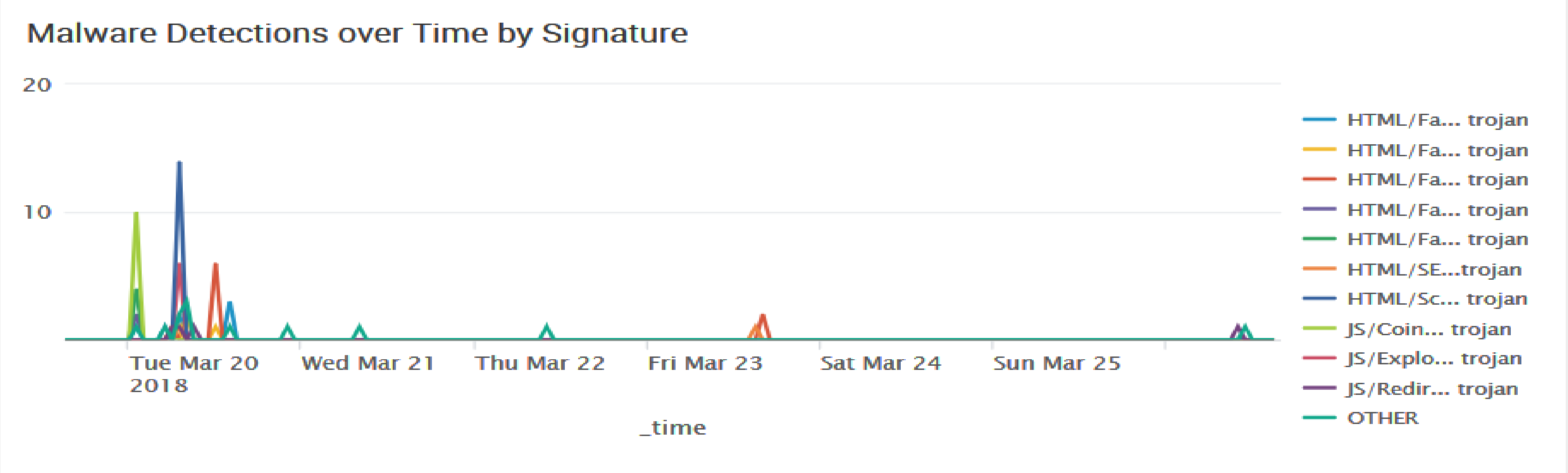
IT Data Collection Summary

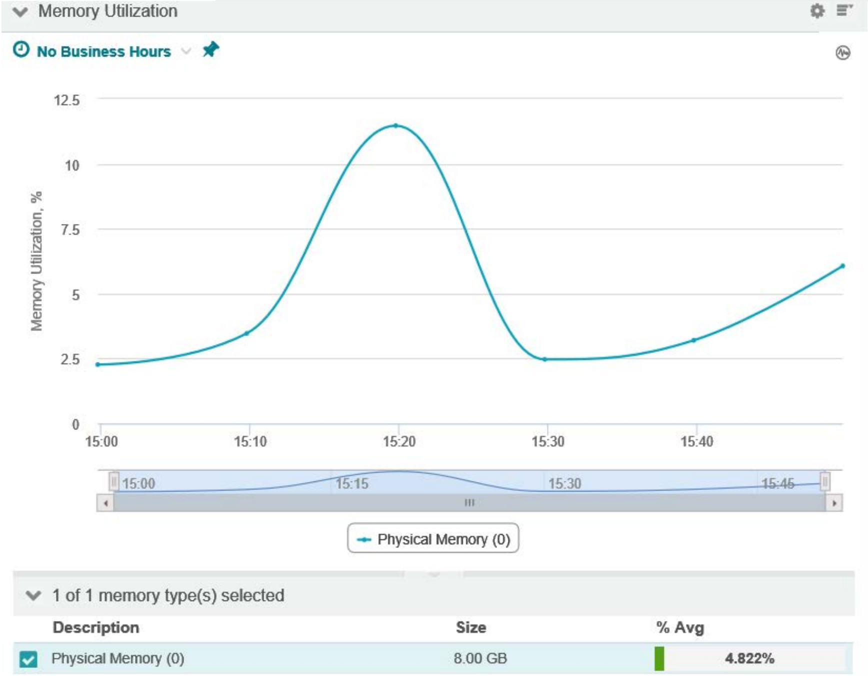
Types of Data Captured Example: Application logs

These logs are used to monitor activity on various database applications, but do not contain specific audits of database transactions. These logs can contain version information, program variables, and programming logic.

```
03/26/2018 03:12:51: LogName=Application, SourceName=MSSQLSERVER,
EventCode=28796, EventType=0, Type=Information,
ComputerName=XXXXXX, User=XXXXX, TaskCategory=Logon,
Keywords=Audit Failure, Classic, Message=Login failed for user
'servername\username'. Reason: Token-based server access validation failed
with an infrastructure error. Check for previous errors. [CLIENT: n.n.n.n]
```

IT Data Collection Summary: Dashboards

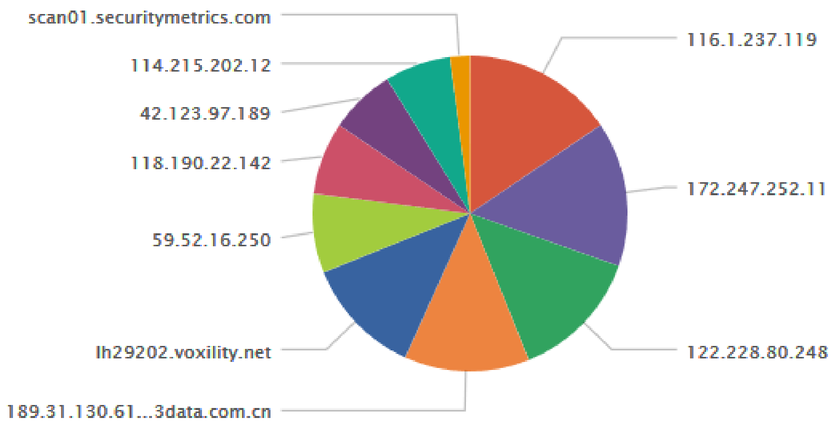




1 of 1 memory type(s) selected

Description	Size	% Avg
☑ Physical Memory (0)	8.00 GB	4.822%

Potential malware activity


scan01.securitymetrics.com
lh29202.voxility.net
189.31.130.61...3data.com.cn