Request for Proposal (RFP)

Implementation of
Advanced Persistent Threat (APT)
Solution

VTB Bank Georgia

1. OVERVIEW

An Advanced Persistent Threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data other than to cause damage to the network or organization. To prevent the above mentioned type of attack, the Bank intends to purchase APT device, thereby to monitor the threat of both internal and external traffic. VTB Bank Georgia invites bids from the prospective bidders having proven past experience and competence in the field of Implementation of the Advanced Persistent Threat (APT) device.

1. DELIVERY AND INSTALLATION

Deliveries of the equipment, installation and operationalization of complete solution at all locations should be made within 4 weeks from the date of purchase order. If however, the delay is caused by any action pending from the Bank end, the corresponding period will not be considered while calculation of delay period.

The installation will be deemed to complete when all the Hardware products specified have been supplied, implemented and made operationalize as per the technical specifications and satisfactory acceptance given by the Bank. The Bidder has to resolve any hardware system software, etc. problems during successful installation and operationalization. All the equipment supplied by the Bidder shall be legal and Bidder shall give indemnity to that effect. Any license, if required, need to be provided by the successful bidder. The successful bidder is solely responsible for any legal obligation related to licenses during warranty period of three years for solution proposed as implemented by the bidder.

2. TECHNICAL REQUIREMENTS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Advanced Persistent Threat solution** |  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |  |  |  |
| 1 | Automated Malware Analysis |  |  |  |  |
| 2 | Real-Time Threat detection |  |  |  |  |
| 3 | Solution should be deployed on premise and along |  |  |  |
| with on premise sandboxing capability |  |  |  |
|  |  |  |  |  |
|  | Sandboxing capabilities of following Operating |  |  |  |
| 4 | Systems (32 and 64 bit) : Win XP, Win7, Win8.x, Win10.x, |  |  |  |
| Server 2008 R2, 2012 R2, Linux, Unix and MAC OS, all |  |  |
|  |  |  |  |
|  | industry standard OS |  |  |  |  |
|  | Solution should be able to detect the persistent |  |  |  |
| 5 | threats which come through executable files, PDF files, |  |  |  |
|  | Flash files, RTF files, any type of file |  |  |  |  |
| 6 | Inspect SMTP, POP3, IMAP traffic |  |  |  |  |
| 7 | Inspect UDP traffic |  |  |  |  |
| 8 | Domain Fluxing (Fast Flux / Dynamic | Reputation/ |  |  |  |
| Domain Generation Algorithms) |  |  |  |
|  |  |  |  |  |
| 9 | Ransom ware detection |  |  |  |  |
| 10 | Detection of C & C and Botnet that are carried by |  |  |  |
| Any protocol |  |  |  |
|  |  |  |  |  |
| 11 | Dormant threat detection capability |  |  |  |  |
|  | Suspected file collection and submission from Console |  |  |  |
| 12 | and also can do the uploading through a web page |  |  |  |
|  | as well. |  |  |  |  |
|  | Solution should be capable to integrate with devices |  |  |  |
| 13 | like Firewall/IPS to mitigate risk by blocking similar |  |  |  |
|  | session. (Cisco) |  |  |  |  |
| 14 | The solution should support discovery of infections via |  |  |  |
| Ipv4 and Ipv6 Traffic Analysis |  |  |  |
|  |  |  |  |  |
| 15 | Solution should integrate with SIEM technology (Arc |  |  |  |
| Sight) and other Log Co-relation systems. |  |  |  |
|  |  |  |  |  |
|  | Solution/appliance must have RAID redundancy (for |  |  |  |
| 16 | hard drives), network redundancy (for management |  |  |  |
| network interfaces), power Supply and Fan module |  |  |
|  |  |  |  |
|  | redundancy. |  |  |  |  |
|  | A solution must support minimum 4X1 GB supported to Copper Gigabit Ethernet (GBE). (4X1Gigabit Fiber (LC) interfaces optional). A solution should support VPC/LACP aggregation capabilities. |  |  |  |  |
| 17 |  |  |  |  |
|  |  |  |  |  |
|  | A solution should identify infections regardless of the |  |  |  |
| 18 | host‘s Operating System and devices used (OS- |  |  |  |
|  | agnosticism) |  |  |  |  |
| 19 | A solution should have Infections detection without |  |  |  |
| sandbox features as well. |  |  |  |
|  |  |  |  |  |
| 20 | Solution should track the infection or threat history for |  |  |  |
| a device, with the ability to access | all forensic |  |  |
|  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Advanced Persistent Threat solution** |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  | evidence for past infections. (6 months) |  |  |  |  |  |
|  |  | A solution should support hostname resolution through |  |  |  |  |
|  | **21** | either Net Bios Lookup or reverse DNS. (Asset |  |  |  |  |
|  |  | Identification) |  |  |  |  |  |  |
|  |  | The solution should be able to inspect and block all |  |  |  |  |
|  | **22** | network sessions regardless of protocols for suspicious |  |  |  |  |
|  | activities or files at various entry/exit sources to the |  |  |  |
|  |  |  |  |  |  |
|  |  | Bank's network. |  |  |  |  |  |  |
|  |  | The solution should be able to protect against |  |  |  |  |
|  | **23** | Advanced | Malware, zero-day | web exploits and |  |  |  |  |
|  | targeted threats without relying on signature |  |  |  |
|  |  |  |  |  |  |
|  |  | database. |  |  |  |  |  |  |  |
|  |  | The solution should be able to identify malware |  |  |  |  |
|  |  | present in network file shares and web objects (For |  |  |  |  |
|  |  | Eg:JPEG, doc, docx, exe, gif, | hip, htm, | pdf, png, |  |  |  |  |
|  | **24** | ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. |  |  |  |  |
|  |  | etc. and any new formats having vulnerabilities to |  |  |  |  |
|  |  | carry potential malware) and able to quarantine |  |  |  |  |
|  |  | them. |  |  |  |  |  |  |  |
|  | **25** | The | solution should be able | to block | malware |  |  |  |  |
|  | downloads over different protocols. |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  | The solution should be able to identify spear phishing |  |  |  |  |
|  | **26** | email containing malicious URLs and attachments |  |  |  |  |
|  |  | that bypass the anti-spam technologies. |  |  |  |  |  |
|  |  | The solution should support Sandbox test environment |  |  |  |  |
|  | **27** | which can analyze threats to various operating |  |  |  |  |
|  |  | systems, browsers, databases etc. |  |  |  |  |  |
|  | **28** | The solution should support both inline and out of the |  |  |  |  |
|  | band mode. |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | The solution should be able to detect and prevent bot |  |  |  |  |
|  | **29** | outbreaks including identification of infected |  |  |  |  |
|  |  | machines |  |  |  |  |  |  |  |
|  |  | The solution should be appliance based with |  |  |  |  |
|  | **30** | hardened OS. No information should be sent to third |  |  |  |  |
|  |  | party systems for analysis of malware automatically. |  |  |  |  |
|  | **31** | The solution should be able to block the call back |  |  |  |  |
|  | tunnel including fast flux connections. |  |  |  |  |
|  |  |  |  |  |  |  |
|  | **32** | The solution should be able to pinpoint the origin of |  |  |  |  |
|  | attack. |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | **33** | The | solution | should be able to conduct forensic |  |  |  |  |
|  | analysis on historical data. |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  | Dashboard should have the feature to report |  |  |  |  |
|  | **34** | Malware type, file type, CVE ID, Severity level, time of |  |  |  |  |
|  | attack, source and target IPs, IP protocol, Attacked |  |  |  |
|  |  |  |  |  |  |
|  |  | ports, Source hosts etc. |  |  |  |  |  |  |
|  |  | The solution should generate periodic reports on |  |  |  |  |
|  | **35** | attacked ports, malware types, types of vulnerabilities |  |  |  |  |
|  |  | exploited etc. |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Advanced Persistent Threat solution** |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |  |
|  |  | The solution should be able to export event data to |  |  |  |
| **36** | Bank‘s existing SIEM arc sight or Incident Management |  |  |  |
|  |  | Systems |  |  |  |  |
|  |  |  |  |  |  |
| **37** | Solution should be able to monitor encrypted traffic |  |  |  |
|  |  | The management console should be able to provide |  |  |  |
| **38** | information about the health of the appliance such as |  |  |  |
|  |  | CPU usage, traffic flow etc. |  |  |  |  |
|  |  | Sandboxing File type supports (.doc, .xls, .ppt, .pdf, |  |  |  |
|  |  | .exe, .zip, .rar, .tar, .gz, .tar.gz, .tgz, .zip, | .bz2, |  |  |  |
| **39** | .tar.bz2, .bz,.tar.Z, .cab, .rar, .arj, .exe, .dll, .avi, |  |  |  |
|  |  | .mpeg, .mp3/4, .jpg, java script, JavaArchive JAR, |  |  |  |
|  |  | LNK, .chm, .swf, .sys, .com, .hwp, etc.) |  |  |  |  |
| **40** | Zero Day Malware Discovery |  |  |  |  |
|  |  |  |  |  |  |  |
| **41** | Malicious P2P Discovery |  |  |  |  |
| **42** | Inspect Proxy/ http traffic |  |  |  |  |
| **43** | Inspect DNS traffic |  |  |  |  |
| **44** | Inspect https traffic (Full Deep Packet / Encrypted |  |  |  |
| Traffic Inspection) |  |  |  |
|  |  |  |  |  |  |
| **45** | Inspect Non-standard TCP port traffic |  |  |  |  |
|  |  | Solution should be capable to integrate with devices |  |  |  |
| **46** | like Web proxy to mitigate risk by blocking similar |  |  |  |
|  |  | session. |  |  |  |  |
|  |  | Solution should be able to support XFF (X- Forwarded- |  |  |  |
| **47** | For) to identify the IP Address of a host in a proxy/NAT |  |  |  |
|  |  | environment. |  |  |  |  |
|  |  | Solution should be able to Identify suspicious |  |  |  |
| **48** | embedded object in document file like OLE & Macro |  |  |  |
|  |  | extraction, Shell code& exploit matching |  |  |  |  |
|  |  |  |  |  |  |
|  |  | The solution should be able to integrate with |  |  |  |
| **49** | deployed appliances to share malware information/ |  |  |  |
|  |  | zero day attacks knowledge base. |  |  |  |  |
| **50** | The solution should be able to capture packets for |  |  |  |
| deep dive analysis. |  |  |  |
|  |  |  |  |  |  |
| **51** | The solution should display the geo-location | of the |  |  |  |
| remote command and control server. |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

3.TECHNICAL SPECIFICATIONS

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Feature** |  |  |  |  |  | **Description** |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **1** |  |  | Deployment | and |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Integration. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Any |  | deployed |  | solution |  |  |  |  |  |
|  |  |  | Centralized protection |  | should | provide | a | central |  |  |  |  |  |
| **2** |  | and Not client based |  | installation |  |  |  |  | and |  |  |  |  |  |
|  |  |  | software. |  |  |  | maintenance | of | client- |  |  |  |  |  |
|  |  |  |  |  |  |  |  | based. |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | A solution must possess an |  |  |  |  |  |  |
| **3** |  | Implementation | and |  | architecture | that | should |  |  |  |  |  |
|  | configuration |  |  |  | works in offline Mode/SPAN/ |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Mirror Traffic |  |  |  |  |  |  |  |  |  |  |
|  | **4** |  |  | Productivity |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | A solution | must | not | be a |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | ―point of failure‖ in network |  |  |  |  |  |
|  |  |  |  |  |  |  |  | traffic | flow; | the | failure of |  |  |  |  |  |
| **5** |  | Point-of-failure |  |  |  | one or more components of |  |  |  |  |  |
|  |  |  |  |  |  |  |  | the | solution | should | not |  |  |  |  |  |
|  |  |  |  |  |  |  |  | affect |  |  |  | organizational |  |  |  |  |  |
|  |  |  |  |  |  |  |  | network‘s functionality. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Solutions |  | must |  | improve |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | productivity | by | identifying |  |  |  |  |  |
|  |  |  |  |  |  |  |  | infections |  |  | automatically, |  |  |  |  |  |
|  |  |  |  |  |  |  |  | reducing |  |  |  |  | manual |  |  |  |  |  |
|  |  |  |  |  |  |  |  | investigations | of | logs | and |  |  |  |  |  |
| **6** |  | Automatic protection |  | alerts. Should be capable |  |  |  |  |  |
|  |  | to | integrate | with | other |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | security |  | controls |  | like |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Firewall/IPS |  | or | Enterprise |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Antivirus | Solution | or | Mail |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Gateways |  | or |  |  | Web |  |  |  |  |  |
|  |  |  |  |  |  |  |  | gateways. |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | A solution must be simple to |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | manage |  | and | maintain, |  |  |  |  |  |
| **7** |  | Simplicity |  |  |  | requiring | little | initial | training |  |  |  |  |  |
|  |  |  |  |  |  |  |  | or subsequent follow-up |  |  |  |  |  |
|  |  |  |  |  |  |  |  | training. |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **8** |  |  | Hardware |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | A solution must have RAID |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | redundancy | (for |  | hard |  |  |  |  |  |
| **9** |  | Hardware redundancy |  | drives), network redundancy |  |  |  |  |  |
|  |  | (for | management | network |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | interfaces), |  | Power-Supply |  |  |  |  |  |
|  |  |  |  |  |  |  |  | redundancy |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Feature** |  |  |  | **Description** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  | Interface flexibility |  | A solution must supportminimum ―4X1 GB‖supported to 1 GB CopperGigabit Ethernet (GBE). (4X1Gigabit Fibre (LC) interfacesoptional) |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A solution must be easily |  |  |  |  |  |
|  |  |  |  |  |  |  | scalable |  | to |  | support |  |  |  |  |  |
|  |  |  |  |  |  |  | monitoring a large number |  |  |  |  |  |
|  |  |  |  |  |  |  | of devices and bandwidth |  |  |  |  |  |
|  |  |  |  |  |  |  | with | throughput | support |  |  |  |  |  |
| **11** |  | Scalability |  |  | commensurate |  |  | with |  |  |  |  |  |
|  |  |  |  |  |  |  | corporate networks. As such |  |  |  |  |  |
|  |  |  |  |  |  |  | the solution should | handle |  |  |  |  |  |
|  |  |  |  |  |  |  | sustained | traffic | throughput |  |  |  |  |  |
|  |  |  |  |  |  |  | of |  | 1Gbps |  | network |  |  |  |  |  |
|  |  |  |  |  |  |  | throughput. |  |  |  |  |  |  |  |  |  |  |
|  | **12** |  |  | **Security** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Management | access | and |  |  |  |  |  |
|  |  |  |  |  |  |  | inter-system communication |  |  |  |  |  |
| **13** |  | Secure channels |  | must be handled in a secure |  |  |  |  |  |
|  |  |  |  |  |  |  | fashion (no http, no ftp, tftp, |  |  |  |  |  |
|  |  |  |  |  |  |  | etc.) |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A | security |  | solution | must |  |  |  |  |  |
| **14** |  | Permissions via Roles |  | provide |  |  | levels |  | of |  |  |  |  |  |
|  |  |  |  |  |  |  | administrative roles. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Device(s) |  | in | a | security |  |  |  |  |  |
| **15** |  | Secure | Operating |  | solution must be appliances |  |  |  |  |  |
|  | System (OS) |  | with | a | secure | operating |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | system installed. |  |  |  |  |  |  |  |  |
|  | **16** |  |  | Use |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Centralized |  | Management |  |  |  |  |  |
| **17** |  | Central Management |  | Console | with | customizable |  |  |  |  |  |
|  |  | dashboard and role-based |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | admin |  |  |  |  |  |  |  |  |  |  |  |
| **18** |  | Intuitive Interfaces |  | Must | have | an | intuitive |  |  |  |  |  |
|  |  | graphical User Interface (UI) |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A | solution | must | provide |  |  |  |  |  |
|  |  |  | Security | Information |  | outputs to, | and integrate |  |  |  |  |  |
| **19** |  | and | Event |  | seamlessly with | these | SIEM |  |  |  |  |  |
|  | Management (SIEM) |  | systems arc sight: RSA SA |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  | integration |  |  | and syslog and compatible |  |  |  |  |  |
|  |  |  |  |  |  |  | format. |  |  |  |  |  |  |  |  |  |  |  |
|  | **20** |  |  | Automated Infections |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Detection |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Network | behavioural |  | A | solution | should | identify |  |  |  |  |  |
| **21** |  | analysis |  |  | infections |  |  |  |  | through |  |  |  |  |  |
|  |  |  |  |  |  |  | corroboration | of | Suspicious |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sl.** | **Feature** |  |  | **Description** |  |  |  |  |  |
| **No.** |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  | Network | Communications |  |  |  |
|  |  |  | Identified |  |  | through |  |  |  |
|  |  |  | Behavioural, Content, | and |  |  |  |
|  |  |  | Source/Destination Analysis |  |  |  |
|  |  |  | A | solution | must | identify |  |  |  |
|  |  |  | infections | on | victim |  |  |  |
|  |  |  | machines |  |  | w i t h |  |  |  |
| **22** | Conviction in absence | corroborated evidence (not |  |  |  |
|  |  |  | just alerts), without needing |  |  |  |
|  |  |  | to interact directly with the |  |  |  |
|  |  |  | host (victim) device. |  |  |  |  |  |
|  |  |  | A solution should be able to |  |  |  |
|  |  |  | identify | infections | beyond |  |  |  |
|  | Detection of | threat | just | the initial dropper | and |  |  |  |
| **23** | propagation | and | be | able | to | identify |  |  |  |
| successful | communicated |  |  |  |
|  | escalation |  | to C & C server and |  |  |  |
|  |  |  |  |  |  |
|  |  |  | successful |  | malware |  |  |  |
|  |  |  | execution on Endpoint. |  |  |  |  |
|  |  |  | Solutions should be able to |  |  |  |
|  |  |  | identify | malicious | activity |  |  |  |
|  |  |  | and infections | for | devices |  |  |  |
|  |  |  | that are mobile (outside of |  |  |  |
|  |  |  | network |  |  | perimeter |  |  |  |
| **24** | Mobile VPN | threat | defences) | on | split-tunnel |  |  |  |
| detection |  | VPN |  | connections. |  |  |  |
|  |  |  |  |  |  |
|  |  |  | Identification of | Advanced |  |  |  |
|  |  |  | Threat Infections, Indifferent |  |  |  |
|  |  |  | of | Infection |  | Vector |  |  |  |
|  |  |  | Locations (in network or out |  |  |  |
|  |  |  | of network) |  |  |  |  |  |  |  |
|  |  |  | A solution must not be |  |  |  |
|  |  |  | dependent | upon | first |  |  |  |
|  |  |  | detecting | an | initial |  |  |  |
|  |  |  | malware |  | infection | (that |  |  |  |
|  |  |  | often happens outside of a |  |  |  |
| **25** | ―Infection order‖ non- | network) |  | to | identify | a |  |  |  |
| dependency |  | subsequent | or | related |  |  |  |
|  |  |  |  |  |
|  |  |  | infection. | Identification | of |  |  |  |
|  |  |  | Advanced Threat Infections, |  |  |  |
|  |  |  | Indifferent | of | Infection |  |  |  |
|  |  |  | Vector Locations (in network |  |  |  |
|  |  |  | or out of network) |  |  |  |  |  |
|  |  |  | A | solution | should | provide |  |  |  |
|  |  |  | administrators | with | the |  |  |  |
| **26** | Retroactive analysis | ability to view file download |  |  |  |
|  |  |  | activity | associated | with |  |  |  |
|  |  |  | infected | Endpoint | for a |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sl.** | **Feature** |  |  |  |  | **Description** |  |  |  |  |  |
| **No.** |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  | window of time prior to the |  |  |  |
|  |  |  |  | determination |  | of |  | the |  |  |  |
|  |  |  |  | endpoint‘s infected status. |  |  |  |
|  |  |  |  | A | solution | should | identify |  |  |  |
| **27** | OS-agnosticism |  | infections | regardless | of the |  |  |  |
|  | host‘s |  | Operating | System |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  | and devices used. |  |  |  |  |  |
|  |  |  |  | A solution should be able to |  |  |  |
|  |  |  |  | identify |  |  |  |  | infections |  |  |  |
|  |  |  |  | communicating | on | more |  |  |  |
|  |  |  |  | than just HTTP (Port 80), such |  |  |  |
| **28** | Malicious |  |  | as | HTTPS, | FTP, | P2P, | custom |  |  |  |
| communications |  | port. |  | Furthermore, | the |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  | solution |  |  | should |  | identify |  |  |  |
|  |  |  |  | communications | stemming |  |  |  |
|  |  |  |  | from proxy-server aware |  |  |  |
|  |  |  |  | malware. |  |  |  |  |  |  |  |  |  |
|  |  |  |  | A | solution | should | identify |  |  |  |
|  |  |  |  | infections |  |  | using |  | P2P |  |  |  |
|  | P2P | Malicious | Malicious |  | Communications |  |  |  |
| **29** | such as Zero Access, TDL4, |  |  |  |
| Communication |  | Zeus | V3, | and **Sality (The** |  |  |  |
|  | Identification |  |  |  |  |  |
|  |  |  | **solution should identify such** |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | **malicious** |  | **softwares** | **like** |  |  |  |
|  |  |  |  | **Sality, etc.)** |  |  |  |  |  |  |  |  |
|  |  |  |  | A | solution | should | identify |  |  |  |
| **30** | DGA/Domain | Flux | Domain |  |  |  | Generation |  |  |  |
| identification |  |  | Algorithm |  |  | (DGA)-based |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  | crime ware. |  |  |  |  |  |  |  |
|  | Suspicious | Traffic | A | solution | should | identify |  |  |  |
| **31** | TOR | or | DNS | Tunnelling | to |  |  |  |
| Behaviour |  |  | conceal |  |  |  |  |  | their |  |  |  |
|  | Identification |  |  |  |  |  |  |  |  |  |  |
|  |  |  | communications |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Malicious | Domain | A solution support detection |  |  |  |
| **32** | of | DNS | Query for malicious |  |  |  |
|  | detection |  |  | domains. |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | A |  | solution |  | support |  |  |  |
|  | Infections | detection | detection |  | of | infections |  |  |  |
|  | without | malware | without seeing the malware |  |  |  |
| **33** | samples | Infections | samples. |  |  |  |  |  |  |  |  |  |
| A |  | solution |  | support |  |  |  |
|  | detection | without | detection |  | of | infections |  |  |  |
|  | Sandbox features |  | without | any | file | analysis |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | features. |  |  |  |  |  |  |  |  |  |
|  |  |  |  | A | solution | should | correlate |  |  |  |
| **34** | Event assessment |  | events | and | differentiate |  |  |  |
|  | between a confirm infection |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | and | a |  | suspicious | event, |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Sl.** |  | **Feature** |  |  | **Description** |  |  |  |  |  |  |  |
|  | **No.** |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | thereby pinpointing infected |  |  |  |  |  |
|  |  |  |  |  |  |  | devices accurately. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A solution must have the |  |  |  |  |  |
|  |  |  |  |  |  |  | ability to track and trace all |  |  |  |  |  |
| **35** |  | Round-Trip-Tracking |  | C&C | communications |  |  |  |  |  |
|  |  | negotiated by a threat, not |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | only | the | initial | one-sided |  |  |  |  |  |
|  |  |  |  |  |  |  | ―call-back‖ of a dropper. |  |  |  |  |  |
|  |  |  |  |  |  |  | A | solution |  | support |  |  |  |  |  |
| **36** |  | Inspection | of |  | inspection | of | evidences |  |  |  |  |  |
|  | Evidences |  |  | both | per | threat and | per |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | asset. |  |  |  |  |  |  |  |  |  |  |
|  | **37** |  |  | Discovery and Analysis |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A | solution |  |  | must |  |  |  |  |  |
| **38** |  | C&C traffic detection |  | detect/monitor |  | inbound |  |  |  |  |  |
|  |  | and outbound command– |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | and–control (C&C) | traffic. |  |  |  |  |  |
| **39** |  | C&C | Domain |  | A solution should be able to |  |  |  |  |  |
|  | detection |  |  | discover suspicious | internet |  |  |  |  |  |
|  |  |  |  |  | domains. |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Secure |  |  | Solution should | be | able to |  |  |  |  |  |
| **40** |  | communication |  | detect | communication |  |  |  |  |  |
|  |  |  | detection |  |  | attempts over HTTPs / SSL. |  |  |  |  |  |
|  |  |  |  |  |  |  | A solution should provide a |  |  |  |  |  |
|  |  |  |  |  |  |  | conviction |  | engine | that |  |  |  |  |  |
| **41** |  | Local Intelligence |  | aggregates evidence | and |  |  |  |  |  |
|  |  |  |  |  |  |  | determines the presence of |  |  |  |  |  |
|  |  |  |  |  |  |  | a threat on a device. |  |  |  |  |  |  |
|  |  |  |  |  |  |  | The | solution | must | include |  |  |  |  |  |
|  |  |  |  |  |  |  | intelligence about malicious |  |  |  |  |  |
| **42** |  | Global Intelligence |  | files | seen | globally | and not |  |  |  |  |  |
|  |  |  |  |  |  |  | only | from within the | local |  |  |  |  |  |
|  |  |  |  |  |  |  | network |  |  |  |  |  |  |  |  |  |  |
| **43** |  | File Analysis |  |  | Sandbox features should be |  |  |  |  |  |
|  |  |  | allowed to |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A solution | should | perform |  |  |  |  |  |
|  |  |  |  |  |  |  | dynamic | analysis | of | files |  |  |  |  |  |
|  |  |  |  |  |  |  | outside of an organization‘s |  |  |  |  |  |
|  |  |  |  |  |  |  | network, in a ―space‖ where |  |  |  |  |  |
|  |  |  |  |  |  |  | malware files cannot evade |  |  |  |  |  |
|  |  |  |  |  |  |  | detection. |  |  | Specifically, |  |  |  |  |  |
| **44** |  | ―Battle-Simulation‖ |  | malware | files | should | be |  |  |  |  |  |
|  |  |  |  |  |  |  | processed | in | a | dedicated |  |  |  |  |  |
|  |  |  |  |  |  |  | ―dirty space‖, with full |  |  |  |  |  |
|  |  |  |  |  |  |  | Internet access | that allows |  |  |  |  |  |
|  |  |  |  |  |  |  | **bare metal analysis** of the |  |  |  |  |  |
|  |  |  |  |  |  |  | malware, | to | counter | VM |  |  |  |  |  |
|  |  |  |  |  |  |  | and | Internet | aware |  |  |  |  |  |



|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sl.** | **Feature** |  |  | **Description** |  |  |  |  |  |  |
| **No.** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | malware |  | as | well |  | as |  |  |  |
|  |  | implement | other | controls |  |  |  |
|  |  | (such as time dilation, key |  |  |  |
|  |  | stroke |  | counts, | varying |  |  |  |
|  |  | software configuration, etc.) |  |  |  |
|  |  | A solution should provide a |  |  |  |
|  |  | dynamic | analysis | option |  |  |  |
| **45** | Dynamic analysis | that does not allow for the |  |  |  |
|  |  | possibility |  | of | malware |  |  |  |
|  |  | attacks on other systems. |  |  |  |  |
|  |  | A | solution | should | identify |  |  |  |
|  |  | system |  | hooks, | network |  |  |  |
|  |  | communication, |  |  | file |  |  |  |
|  |  | accesses, file changes, etc. |  |  |  |
|  | Suspicious | used | by | suspicious | files |  |  |  |
| **46** | charged | with | infecting | a |  |  |  |
| file dismantlement |  |  |  |
|  | system. |  | These | malware- |  |  |  |
|  |  |  |  |  |  |
|  |  | related | traits | and | actions |  |  |  |
|  |  | should be decipherable via |  |  |  |
|  |  | the | dynamic |  | analysis | of |  |  |  |
|  |  | suspicious files. |  |  |  |  |  |  |  |  |
|  |  | The solution should indicate |  |  |  |
|  |  | the degree of certainty the |  |  |  |
|  |  | solution | has |  | of |  | threat |  |  |  |
| **47** | Conviction assertion | presence | on | a | device; | it |  |  |  |
|  |  | should not just alert in |  |  |  |
|  |  | discriminately |  | (Becoming |  |  |  |
|  |  | ―noise‖). |  |  |  |  |  |  |  |  |  |  |
| **48** | Threat information | The | solution support | local |  |  |  |
| threats. |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | The | solution | should | allow |  |  |  |
|  |  | administrator-level users to |  |  |  |
|  |  | include |  | custom | threats |  |  |  |
|  |  | (used for | testing purposes) |  |  |  |
|  |  | that can be **created and** |  |  |  |
|  |  | **tracked** | via |  | the | User |  |  |  |
| **49** | ―Custom‖ threats | Interface. |  | Custom |  | threat |  |  |  |
|  |  | can be created based on |  |  |  |
|  |  | domain, | IP | Address | and |  |  |  |
|  |  | MD5 Hash. |  |  |  |  |  |  |  |  |  |
|  |  | **Custom** | **threats** | **are** | **tried** |  |  |  |
|  |  | **only in test environment.** |  |  |  |  |
| **50** | Ipv4 Traffic Analysis | The | solution | should | support |  |  |  |
| discovery of infections |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **51** | Ipv6 Traffic Analysis | The | solution | should | support |  |  |  |
| discovery of infections |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Sl.** |  |  | **Feature** |  |  |  | **Description** |  |  |  |  |  |  |  |  |  |  |
|  | **No.** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **52** |  |  | Zero Day and Updates |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **53** |  | Zero-day analysis |  | A | solution | should | handle |  |  |  |  |  |  |  |
|  |  |  | Zero-Day Analysis based |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A | solution | should | detect |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | whether |  |  |  |  | malware |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | downloaded |  |  | by |  | an |  |  |  |  |  |  |  |
|  |  |  | File | execution |  | endpoint | was |  | effectively |  |  |  |  |  |  |  |
|  | **54** |  |  | installed (executed) on | the |  |  |  |  |  |  |  |
|  |  |  | detection |  |  | endpoint, | this | done | via |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | methodologies that do not |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | utilize | endpoint |  | agents. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Agentless approach |  |  |  |  |  |  |  |  |  |  |
|  | **55** |  | Real-time | Intelligence |  | A | solution | should | include |  |  |  |  |  |  |  |  |
|  |  | updates |  |  | automated | real |  | time |  |  |  |  |  |  |  |
|  |  |  |  |  | intelligence updates. |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **56** |  |  | Incident Response and |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Mitigation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Solutions | should | allow | for |  |  |  |  |  |  |  |  |
|  | **57** |  | Incident Tracking |  | incidents | to | be | marked, |  |  |  |  |  |  |  |
|  |  |  | tagged |  |  |  |  |  |  | and |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | acknowledged. |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Solutions should allow a user |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | to track investigation efforts |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | at an asset/device level by |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | supporting |  | tagging/notes, |  |  |  |  |  |  |  |
|  | **58** |  | Investigation Tracking |  | marking | assets | and | threats |  |  |  |  |  |  |  |
|  |  |  | as remediated, and support |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | auto-expiration if no further |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | evidence |  | has |  | been |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | collected for a period of |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | time. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Solution | should |  | track | the |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | infection or threat history for |  |  |  |  |  |  |  |
|  | **59** |  | Historical Investigation |  | a device, with the ability to |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | access all forensic evidence |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | for past infections. |  |  |  |  |  |  |  |  |  |  |  |
|  | **60** |  | Whitelisting |  |  | Solutions should be able to |  |  |  |  |  |  |  |  |
|  |  |  |  | mark assets/host |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A solution should provide risk |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | ranking of an infection to a |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | network, |  | based | on | the |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | activity of the threat locally |  |  |  |  |  |  |  |
|  | **61** |  | Risk Derivation |  | within |  | the |  | network |  |  |  |  |  |  |  |
|  |  |  | (frequently |  | of |  | malicious |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | communication |  | attempts, |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | data |  |  |  | transferred, |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | importance | of | infected |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | device). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Feature** |  |  |  |  | **Description** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | A solution should be able to |  |  |  |
|  |  |  | capture |  | and | display | all |  |  |  |
|  |  |  | events (either in | sequence |  |  |  |
| **62** | Event tracking |  | or | by | event | type) | in | a |  |  |  |
|  |  |  | simple, intuitive interface to |  |  |  |
|  |  |  | understand the contributing |  |  |  |
|  |  |  | events to an infection. |  |  |  |  |
|  |  |  | A solution should have the |  |  |  |
| **63** | Packet Captures |  | ability | to | capture, | publish |  |  |  |
|  |  |  | and download PCAP files. |  |  |  |
|  |  |  | A | solution | should | provide |  |  |  |
|  |  |  | information | on |  | the | threat |  |  |  |
|  |  |  | present | on | the | customer‘s |  |  |  |
|  |  |  | network |  |  | **(i.e.** |  |  | **Bank’s** |  |  |  |
| **64** | Threat details |  | **network)** |  | (threat |  | details, |  |  |  |
|  |  |  | threat |  | intent, |  | researcher |  |  |  |
|  |  |  | notes, |  | crime | ware | used, |  |  |  |
|  |  |  | local |  |  |  | communication |  |  |  |
|  |  |  | activity, etc.). |  |  |  |  |  |  |  |  |
|  |  |  | Solution should be able to |  |  |  |
|  |  |  | pick | up | and |  | reconstruct |  |  |  |
| **65** | Malicious | file | suspicious files via a passive |  |  |  |
| management |  | interface and make the files |  |  |  |
|  |  | accessible to administrators |  |  |  |
|  |  |  |  |  |  |
|  |  |  | with | rights | to |  | download |  |  |  |
|  |  |  | malicious files. |  |  |  |  |  |  |  |  |
|  |  |  | Solution |  |  | should |  | allow |  |  |  |
|  |  |  | customer |  | access |  | to |  |  |  |
|  |  |  | suspicious and malicious files |  |  |  |
| **66** | File access |  | so that they can download |  |  |  |
|  | them, |  |  | process |  | them |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  | themselves, | or |  | submit | to |  |  |  |
|  |  |  | their AV vendor for signature |  |  |  |
|  |  |  | creation. |  |  |  |  |  |  |  |  |  |  |
|  |  |  | A solution should allow for |  |  |  |
|  |  |  | categorization | of | devices |  |  |  |
|  |  |  | along |  | with |  | ‗level | of |  |  |  |
| **67** | Categorization |  | importance‘ | of |  | those |  |  |  |
|  | devices |  | should | they | be |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | infected, with the | following |  |  |  |
|  |  |  | priority:- |  |  | Critical, |  | High, |  |  |  |
|  |  |  | Medium, Low |  |  |  |  |  |  |  |  |
|  |  |  | A | solution | must | provide |  |  |  |
|  |  |  | infection forensics to enable |  |  |  |
| **68** | Validation |  | incident |  |  | responders | to |  |  |  |
|  | validate findings and adapt |  |  |  |
|  |  |  |  |  |  |
|  |  |  | security | policy | (connection |  |  |  |
|  |  |  | attempt counts, connection |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Feature** |  |  |  |  | **Description** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | attempt | success, | bytes | in, |  |  |  |  |  |
|  |  |  |  |  |  | bytes |  | out, | full | packet |  |  |  |  |  |
|  |  |  |  |  |  | captures, | suspicious | file |  |  |  |  |  |
|  |  |  |  |  |  | static and dynamic analysis, |  |  |  |  |  |
|  |  |  |  |  |  | Forensic | Metadata | and |  |  |  |  |  |
|  |  |  |  |  |  | Infection Forensics) |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | A solution should be able to |  |  |  |  |  |
|  |  |  |  |  |  | track | if | remediation | efforts |  |  |  |  |  |
|  |  |  |  |  |  | have | been effective | by |  |  |  |  |  |
| **69** |  | Remediation |  | continually | monitoring | the |  |  |  |  |  |
|  | effectiveness |  | network | behaviours | of | an |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | asset and keeping a threat |  |  |  |  |  |
|  |  |  |  |  |  | history |  |  | (including |  | all |  |  |  |  |  |
|  |  |  |  |  |  | evidence). |  |  |  |  |  |  |  |  |  |  |
| **70** |  | Asset identification |  | A | solution | should | support |  |  |  |  |  |
|  |  | hostname resolution |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | A | solution | should | facilitate |  |  |  |  |  |
|  |  |  |  |  |  | the analysis of the malware |  |  |  |  |  |
| **71** |  | Malware analysis |  | to | allow | for | quick | risk |  |  |  |  |  |
|  |  |  |  |  |  | identification | and |  | enable |  |  |  |  |  |
|  |  |  |  |  |  | remediation workflow. |  |  |  |  |  |  |
|  |  |  |  |  |  | A | solution | should | enable |  |  |  |  |  |
| **72** |  | Research validation |  | simple |  | investigation | / |  |  |  |  |  |
|  |  | research | to | validate |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | findings. |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | A | solution | should | provide |  |  |  |  |  |
|  |  |  |  |  |  | forensic information (such as |  |  |  |  |  |
|  |  |  |  |  |  | communication |  | profiles |  |  |  |  |  |
|  |  |  |  |  |  | seen locally in customer‘s |  |  |  |  |  |
| **73** |  | Third-party integration |  | network, | MD5s, | malware |  |  |  |  |  |
|  |  |  |  |  |  | details, etc.) that can be |  |  |  |  |  |
|  |  |  |  |  |  | promoted | to | prevention |  |  |  |  |  |
|  |  |  |  |  |  | systems | like | IPS/IDS/Web |  |  |  |  |  |
|  |  |  |  |  |  | Gateway. |  |  |  |  |  |  |  |  |  |  |
|  | **74** |  |  | Mitigation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | A solution should be able to |  |  |  |  |  |
|  |  |  |  |  |  | perform DNS redirection for |  |  |  |  |  |
| **75** |  | DNS Redirects |  | malicious DNS | queries, | to |  |  |  |  |  |
|  |  | prohibit |  | infections | from |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | communicating with | cyber |  |  |  |  |  |
|  |  |  |  |  |  | criminals. |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | A solution should be able to |  |  |  |  |  |
|  |  |  |  |  |  | perform |  | TCP | RSTs | for |  |  |  |  |  |
| **76** |  | Connection |  | individual | communication |  |  |  |  |  |
|  | termination |  | sessions | with | C&Cs | to |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | protect against the loss of |  |  |  |  |  |
|  |  |  |  |  |  | data. |  |  |  |  |  |  |  |  |  |  |  |  |
| **77** |  | Firewall integration |  | A | solution | should | integrate |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Feature** |  |  | **Description** |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | with | firewall | platform | for |  |  |  |
|  |  | asset quarantine | purpose |  |  |  |
|  |  | such as Check Point, Cisco |  |  |  |
|  |  | firewall. |  |  |  |  |  |  |  |  |  |  |
|  |  | Automated |  | and |  | Direct |  |  |  |
|  |  | Integration with Checkpoint |  |  |  |
|  |  | firewall | where |  | firewall |  |  |  |
|  |  | policies |  | can |  |  | be |  |  |  |
|  |  | implemented |  | based | on |  |  |  |
|  |  | device | state (suspected or |  |  |  |
| **78** | Firewall integration | infected) |  |  | information |  |  |  |
|  |  | discovered | by | the | solution. |  |  |  |
|  |  | (IE: | Block | infected | assets |  |  |  |
|  |  | from |  | communicating | to |  |  |  |
|  |  | internet and/or high-value |  |  |  |
|  |  | assets, enhance logging on |  |  |  |
|  |  | suspected assets) |  |  |  |  |  |  |
|  |  | Automated |  | and |  | Direct |  |  |  |
|  |  | Integration with Checkpoint |  |  |  |
|  |  | firewall | where |  | firewall |  |  |  |
| **79** | Firewall integration | policies |  | can |  |  | be |  |  |  |
| implemented | which | blocks |  |  |  |
|  |  |  |  |  |
|  |  | active | C&C |  | attempts |  |  |  |
|  |  | communication |  | attempts |  |  |  |
|  |  | identified by the solution. |  |  |  |
|  |  | Automated |  | and |  | Direct |  |  |  |
|  |  | Integration | with | web proxy |  |  |  |
|  |  | where web access policies |  |  |  |
|  |  | can be implemented based |  |  |  |
|  |  | on device state (suspected |  |  |  |
| **80** | Web Proxy Integration | or | infected) |  | information |  |  |  |
|  |  | discovered | by | the | solution. |  |  |  |
|  |  | (IE: | Block) | infected | assets |  |  |  |
|  |  | from |  | communicating | to |  |  |  |
|  |  | internet and/or high-value |  |  |  |
|  |  | assets) |  |  |  |  |  |  |  |  |  |  |
|  |  | Automated |  | and |  | Direct |  |  |  |
|  |  | Integration | with | web proxy |  |  |  |
|  |  | where ewb access policies |  |  |  |
| **81** | Web Proxy Integration | can be implemented which |  |  |  |
|  |  | blocks |  | active |  | C&C |  |  |  |
|  |  | communication |  | attempts |  |  |  |
|  |  | identified by the solution |  |  |  |  |
|  |  | Automated |  | and |  | Direct |  |  |  |
|  |  | Integration with Endpoint AV |  |  |  |
| **82** | AV Integration | solution | to | create | / | add |  |  |  |
|  |  | identified | threat‘s |  | file |  |  |  |
|  |  | integrity hash |  | value. | The |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Sl.** |  | **Feature** |  |  | **Description** |  |  |  |  |  |  |  |
|  | **No.** |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Solution |  | can | work | in |  |  |  |  |  |
|  |  |  |  |  |  |  | conjunction with | ANTIVIRUS |  |  |  |  |  |
|  |  |  |  |  |  |  | but it should not be |  |  |  |  |  |
|  |  |  |  |  |  |  | dependent on it |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A solution should have built |  |  |  |  |  |
|  |  |  |  |  |  |  | in reports such as: |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | - Executive | Reports |  |  |  |  |  |  |  |
| **83** |  | Integrated reporting |  | - Incident Response Reports |  |  |  |  |  |
|  |  |  |  |  |  |  | - Infection Life Cycle Reports |  |  |  |  |  |
|  |  |  |  |  |  |  | - Malware in Motion Reports |  |  |  |  |  |
|  |  |  |  |  |  |  | - System Health Reports |  |  |  |  |  |  |
| **84** |  | Event logging |  | A solution | should | support |  |  |  |  |  |
|  |  | the ability to forward logs |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | The solution should integrate |  |  |  |  |  |
| **85** |  | SIEM integration |  | with Enterprise | level | Arc |  |  |  |  |  |
|  |  | sight Solution and other Log |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Co relation systems. |  |  |  |  |  |  |  |
|  | **86** |  |  | Alerts |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Solution |  | should | report |  |  |  |  |  |
| **87** |  | Administrator alerts |  | infection | alerts | on | a | real |  |  |  |  |  |
|  |  |  |  |  |  |  | time basis via email. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | A solution | should | support |  |  |  |  |  |
|  |  |  |  |  |  |  | device | alerting | for | the |  |  |  |  |  |
|  |  |  |  |  |  |  | health of | the solution | via |  |  |  |  |  |
| **88** |  | SNMP integration |  | the industry-standard simple |  |  |  |  |  |
|  |  |  |  |  |  |  | network |  | Management |  |  |  |  |  |
|  |  |  |  |  |  |  | protocol | (SNMP | v2) traps |  |  |  |  |  |
|  |  |  |  |  |  |  | and alerts. |  |  |  |  |  |  |  |  |  |

+