


ENDPOINT THREAT DETECTION & RESPONSE

DETECTING ATTACKS TO MICROSOFT SYSTEMS





To increase the security of the Microsoft systems, SGBox provides a number of specific out-of-the-box correlation rules and dashboards to detect threats and generate automated responses to mitigate the risk of a data breach.

The Scenario

To identify a targeted attack within your MS computer systems, you need to have visibility of possible indicators of compromise (IOC), collecting qualified information from endpoints, where most of the targeted attacks are concentrated. Endpoints are targeted for various reasons: they are the user's access point to business information, they can be used to identify privileged credentials (credential dumping techniques), they are often used by non-experienced users with access to personal data (increasingly sophisticated phishing techniques are accompanied by software vulnerabilities). Furthermore, by exploiting web browser vulnerabilities or the lack of advanced prevention tools, some techniques may help circumvent perimeter controls (i.e. spear phishing via service attacks).

Endpoint protection tools (belonging to the preventive control sphere) can be ineffective in identifying modern attacks. For this reason, most vendors have introduced more sophisticated tools that use behavioral analysis and machine learning platforms to process the telemetry of endpoint and generate alarms automatically. Endpoint Detection and Response (EDR) solutions have been created but, while offering many advantages, represent an additional cost to the company. Most EDRs also require IT personnel to operate through a new console, to highlight the anomalies reported by the instrument. Why not use the SIEM platform already adopted to centralize compromise and attack indicators and highlight risk scenarios? Why not use a free tool to get telemetry from Microsoft Windows endpoints?

The SGBox Security Package for Microsoft Security

As a supplier of a SIEM solution, SGBox decided to respond to these needs by collecting and integrating specific information generated by Microsoft systems.

System Monitor (Sysmon) is a free Microsoft software component that, installed as a Windows service, allows you to monitor and track system activities by saving them in the Windows event log. The data collected by the service significantly increases Windows audit capabilities, allowing you to gather detailed information about processes, but also about network traffic (such as DNS queries sent by an application).

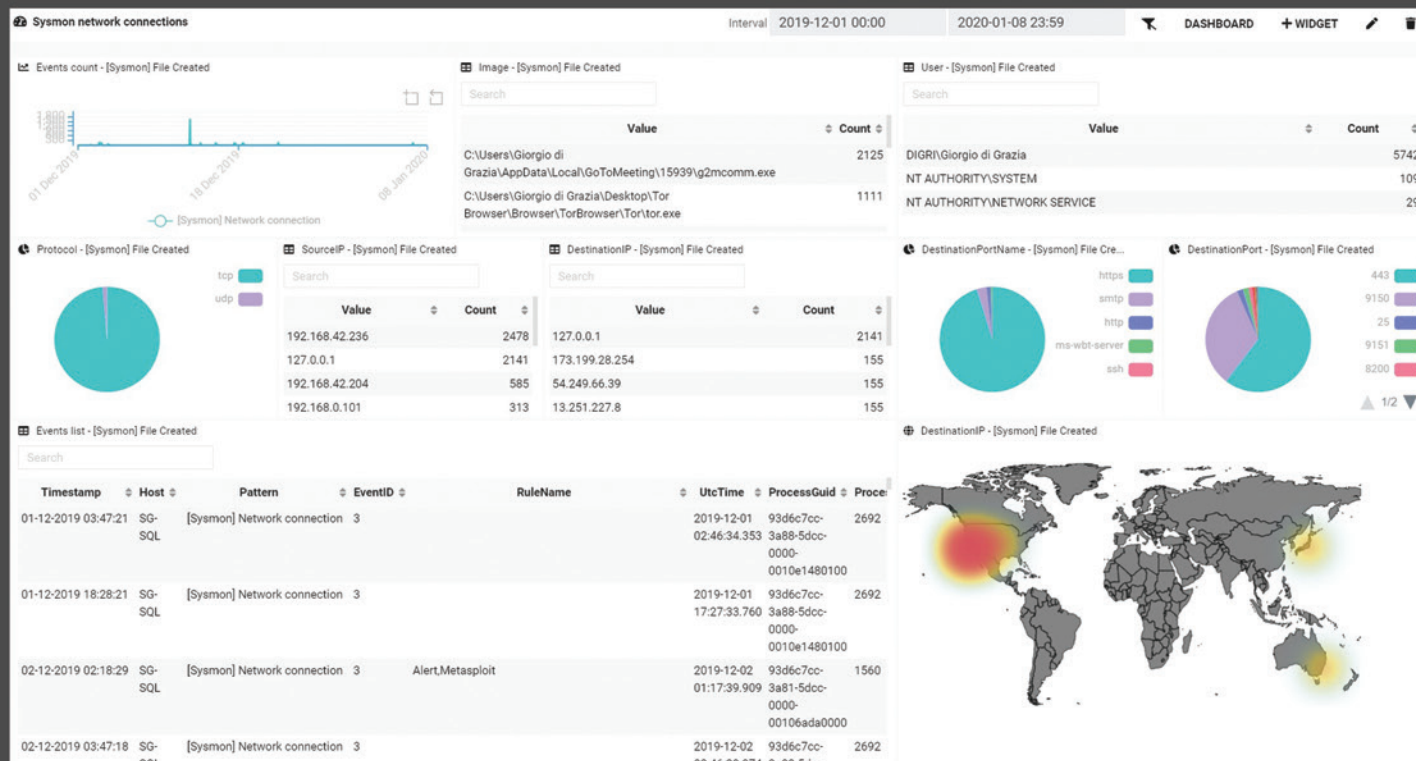
Process information is enriched by other details such as a hash (SHA1), the Globally Unique Identifier (GUID) of the process, the session GUID and other related processes. The collection of this data in the fully configurable SGBox SIEM allows both the visualization of anomalies within dedicated dashboards and the creation of automatic rules to generate different type of alarms (from email to Telegram message, up to possible interaction via API with a third-party solution).

Sysmon can be configured with an XML file that allows you to determine which items to monitor. There are a number of freely usable models on GitHub (the most popular is probably the one from SwiftonSecurity: <https://github.com/SwiftOnSecurity/sysmon-config>).

SGBox maps possible attack techniques with Tactics, Techniques and Procedures (TTP) of the MITRE ATT&CK framework (<https://attack.mitre.org>). ATT&CK catalogues the modus operandi of attackers (pre and post-compromise phases) starting from real cases, defines common terminology and is widespread in many security products (including EDRs).

After installing the SGBox agent on endpoints, data is collected in the log management platform in a dedicated class ("Windows Security") and interpreted through patterns that allow recognition of event categories produced by the Microsoft device driver.

Examples are DNS query, driver loaded, file created, process creation, registry modification, WMI event etc. In addition to event recognition, SGBox allows the identification of commands normally used by fileless techniques.



Blacklists can be updated with programs and processes used by the customer, in order to improve process monitoring and reduce false positives. Statistics are represented in two dashboards: the first one with the details of the processes detected and the MITRE ATT&CK techniques; the second one with the information regarding network connections (DNS traffic and related processes). Of course, it is possible to associate automatic correlation rules to generate alarms of various types.

By integrating detailed endpoint information and MITRE ATT&CK techniques, SGBox offers to his customers a convenient way to identify possible risk scenarios related to Microsoft platforms, reducing false positives, the complexity of the IT infrastructure and the cost of a dedicated security product license.

Value	Count
technique_id=T1047,technique_name=Windows Management Instrumentation	40
technique_id=T1036,technique_name=Masquerading	13
technique_id=T1059,technique_name=Command-Line Interface	2
technique_id=T1031,technique_name=Modify Existing Service	2
technique_id=T1086,technique_name=PowerShell	1