snare
A PROPHECY SOLUTION

The Workstation Monitoring Imperative

Whitepaper

If you aren't monitoring workstations, you are opening yourself up to a world of hurt

You've just discovered a breach and are hunting down the forensic chain of events of an APT when the trail goes cold. Like most breaches today, they don't start on the servers, they start on your workstations - and you haven't been monitoring your workstations. Maybe it was resource prohibitive. Maybe it was deemed unnecessary. Maybe it was both, but now it's a painful lesson, not to be repeated, which can derail your career.

Why not keep an eye on the new process created events? Especially when the process name doesn't match up with an approved list or the process name looks suspicious. Wouldn't you also want to know whether an employee or contractor was trying to, or successfully, accessed sensitive files, saving them to a USB drive or emailing them to a personal domain? Or what if an OS exe was replaced overnight while they were off the network? Trying to trace a breach and not knowing what programs were running makes for a lot of guesswork and leaves you vulnerable and susceptible.

Close to 25% of corporate data is saved on workstations and inadvertently shared or misplaced on USB drives.[i] Off-network activities on mobile devices can tell you a lot about what's happening to your corporate data, though it's all moot if you can't see it.

I hear you say, *"But my SIEM is already overloaded, my network congested, and I pay through the nose by the byte"*. This may be true for some, but not for most. There are proven and effective approaches such as an output-driven strategy to reduce the noise by as much as 90% using lightweight standalone logging agents with real-time objective-based filtering.2[ii] You can also truncate non-forensic data from event logs further reducing the data by up to 70%. Ultimately, there are no valid excuses for neglecting to monitor your workstations.

In addition to the constant threats posed to your organization, compliance standards need to be met at all times. Too many companies find themselves scrambling in the face of an audit they will undoubtedly come up short on. Remaining compliant can often feel like a moving target, but the more thorough your organization, the more likely you are to stay in front the ever-evolving compliance landscape. There are several fundamental compliance standards to keep in mind.

PCI DSS compliance all systems in scope need to have logging and auditing in place. This means all servers, desktops, databases, web servers, applications, routers, firewalls, switches, etc. Any device that is involved with storing, processing, transmitting or accessing cardholder data is in

SOX and FISMA require assurance of the integrity of financial systems. To achieve this end-to-end logging is needed, from the desktop to the server to the database where the information may reside. Such processes facilitate the management team to prove and attest, in writing, that their technical controls prove the financial systems are true and correct.

HIPAA requires any company who deals with protected health information to ensure that physical, network, and process security measures are in place and followed. For example, when patient data has been accessed from the servers there must be a record of what data was accessed, and what was done with it. *Was it copied or moved to another system?* To track this requires agents to be deployed on desktops and laptops.

NISPOM and other USA government standards also cover the need for all computers to be in scope and this includes workstations. All systems that have access to the corporate network or security zones need to have logging and auditing to know what state that system is in. In general, it is no different to customers that have antivirus and apply security patches to these systems as they are essential. If the system is important enough to have antivirus software it is important enough for logging. Not just for compliance but also because numerous critical activities can only be tracked on the workstations themselves.

MONITORING LOGIN ACTIVITY

Domain logins will cause a log to be generated on the domain controller while the system is connected to the LAN. When it's off the LAN, no logs will be generated even for accounts hosted by the Domain, as the authentication will be via cached credentials. Login event logs will be generated locally. These events will not be sent to the Domain controller and may be overwritten locally. Additionally, when local user authentication is performed it will not send the logs to the Domain Controller but only the local event logs.

PROCESS MONITORING

Commands that run on a workstation are not logged to the Domain Controllers. Thus, there is no way for the security team to know what the end users are executing or if some unknown new malicious software is running. To track these movements, they must have local auditing and logging processes in place.

FILE MONITORING

Most workstations will have locations where sensitive data is stored. This data can be copied data or data moved to unauthorized locations. By combining information on commands that are run locally, and events relating to sensitive files, such activity can be monitored.

LOCALLY LOGGED EVENTS

A workstation can be changed; sensitive data can be copied to it, or accessed from it. Such modifications can be an issue, as not all changes are recorded on the domain controllers - with many of the details only logged locally. For example, when a user logs onto a workstation with a local login (a non-active directory account), the information is only recorded locally and is not be passed to the domain controller. This is also the case when users access a

local USB or CD-ROM drive. Thus, the only way to capture this local information is to deploy a log monitoring agent on the workstation.

CONCLUSION

It's critical to collect and analyze the logs from your workstations, desktops, PC's, laptops and BYOD's. This is where the action is, it's easy street, and where the threats and breaches originate. So much time and money is spent on last century's 'best practices' that we forget that people use workstations. No matter how often you tell them not to click on links, not to visit questionable sites, not to leave their workstations logged on, and not to connect to a public WiFi - they do. It is in err that we think of threats as real-time hacks against the perimeter that we must vigorously defend. As more often than not the perimeter has been breached months, if not years, ago. With malicious actors lying dormant waiting to act.

It only takes a handful of Google searches to see companies across the globe facing crises and realizing the importance of workstation logging. Workstation logs are critical and no organization can afford to lose them to oblivion. Whether piecing together how a breach occurred or preventing threats from prevailing in the future, knowledge, as they say, is power.

Knowing what to do and understanding how to execute, can be two completely different things and how your organization chooses to go forward can be the unheralded difference between "business as usual" and having a breach that gets splashed across the headlines. Intersect Alliance is here to help you address all of your SIEM and log monitoring needs.

manage it and protect it. The integration of an effective collection, analysis and reporting platform in Snare, can provide you with the capacity to meet the GDPR requirements.

ADDITIONAL RESOURCES:

To learn how Snare can help you optimize the management of your workstations, visit

https://www.snaresolutions.com

---

[i] Gartner statistic retrieved November 6th, 2015 from https://twitter.com/gartner_inc/status/481528221054169088

[ii] Anthony, Russ “Detecting Security Incidents Using Windows Workstation Event Logs.” Advisor. Robert Vandenbrink. SANS Institute. 2012. Page 7.