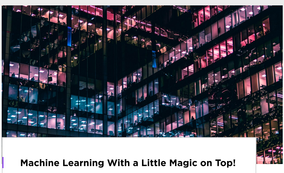


Machine Learning With a Little Magic on Top!

August 27, 2018
by SentinelOne

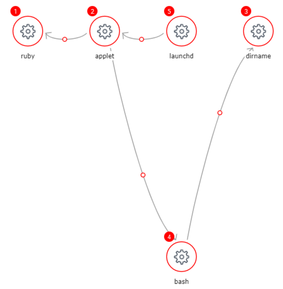
As part of our intro pitch, we explain how the SentinelOne agent uses multiple engines. The primary ones are –

Static AI

SentinelOne Static AI engine detects and prevents threats from executing using static ML models. Static ML models are now used by many vendors and are trained to detect threats by looking at various static attributes that can be extracted from binaries/executables. This is a true signature-less technology which is very good at detecting file-based threats. The biggest difference between Static models of vendors is the way they are tuned. The more aggressive models are great at stopping threats, but may also have a higher False Positive rate.

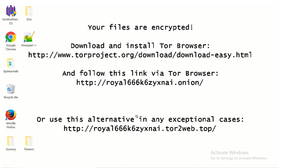
Dynamic Behavioral Tracking (DBT)

SentinelOne **Dynamic Behavioral Tracking** (DBT) tracks all activities on the system including file/registry changes, service start/stop, interprocess communication, network activity. This information is fed into a dynamic ML model which detects and kills threats not caught by Static AI. Since it models the behavior of all processes, we are able to identify threats that are very hard to catch with static models. For e.g. your excel spreadsheet could have a macro that runs PowerShell with a network payload that never touches the disk. We have even found script-based attacks on macOS using our dynamic model.



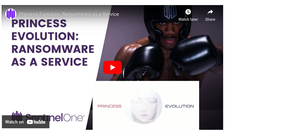
Orchestration Engine

Our orchestration engine is able to isolate infected computers from the network or rollback threats automatically. The rollback is especially useful during the first few days of a Proof of Concept or initial deployment when our agent is being used alongside the customer's AV that they are trying to replace. Typically, the SentinelOne agent is installed in Alert mode to see what else it is able to catch. If there is an infection that was not blocked, we can save customers a lot of time by just rolling back to an earlier version of the snapshot as shown in the gif here –



This is a jaw-dropping experience and normally seals the deal in our favor. Are you ready to try ML with some magic on top?

In this video, you can see it in action. You can see how each layer is detecting the ransomware and finally, how the malware is rolled back, so the user can continue working without spending time on the malicious attempt.



Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Can Whitelisting Win over Advanced Persistent Threats?
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- 24 Cybersecurity Twitter Accounts You Should Follow in 2022
- 6 Real-World Threats to Chromebooks and ChromeOS
- More Evil Markets | How It's Never Been Easier To Buy Initial Access To Compromised Networks
- 4 Steps Toward Successfully Measuring the Effectiveness of Your Security Controls