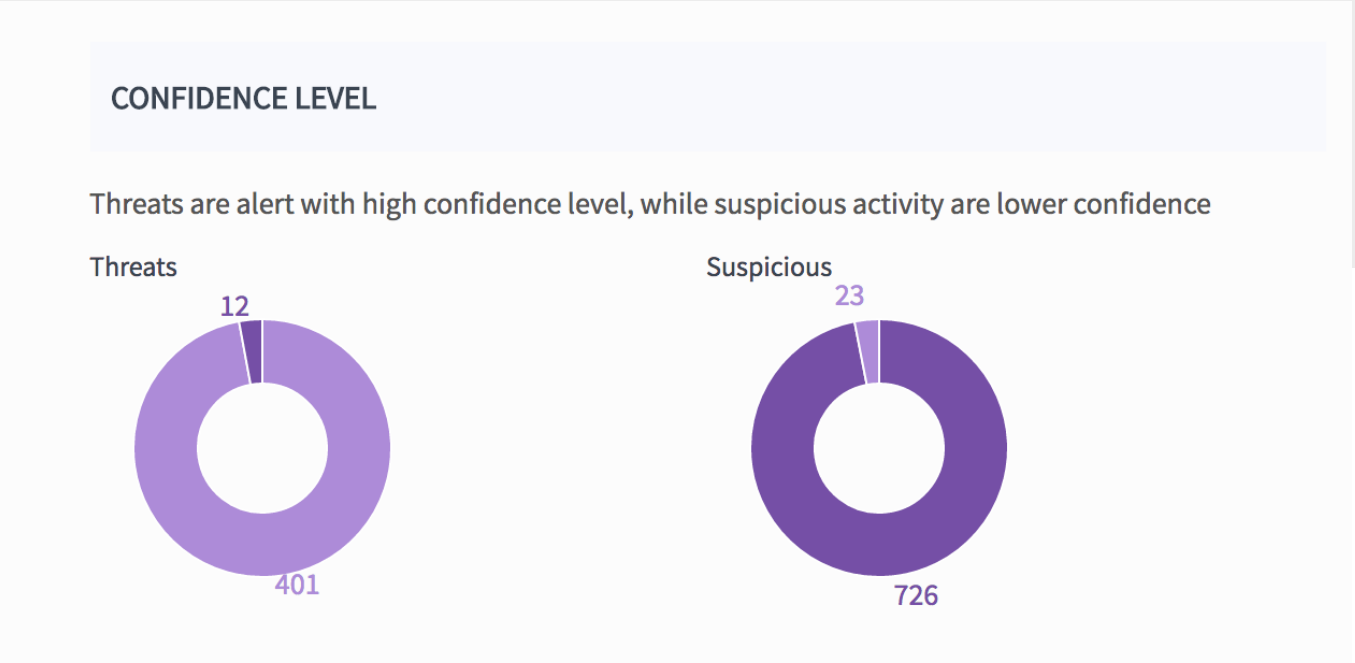


Insight Reporting – Feature Spotlight

January 9, 2018
by Migo Kedem

We are thrilled to announce our new *Insight* reports!

This feature is available to all customers with the Bahamas release of the Management Console.

The Why

Different customers want to see different items in their reports. But everyone wants information to be easy to digest and actionable. Insight Reports let you make data-driven decisions to improve your team's security and performance. We also added the option to create new Insight reports without the need for a release, so if you want us to build a custom report for you, just ask!

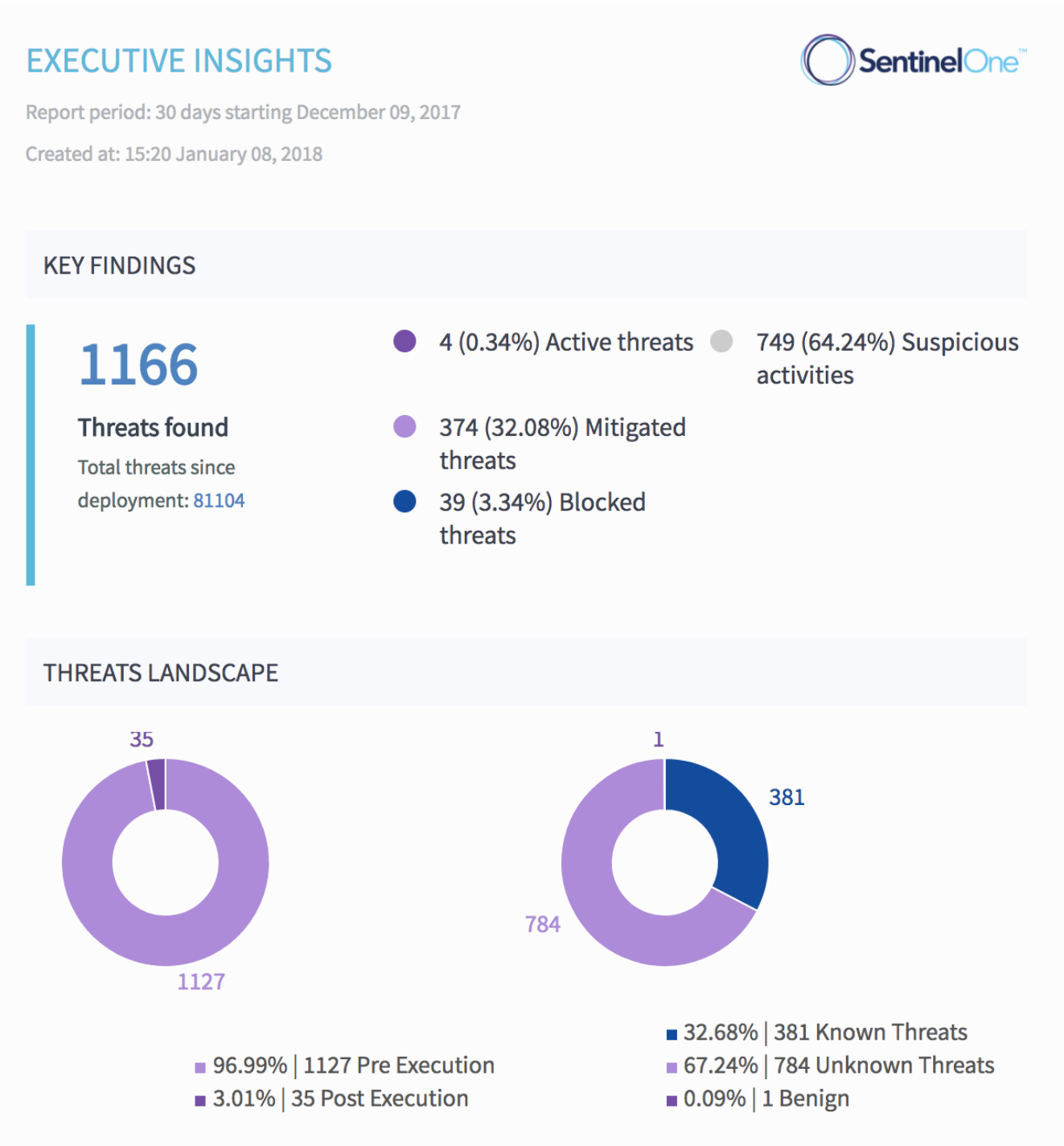
These Insight Reports are already available:

- Executive Insights
- Executive Insights by Group
- Threat Insights
- Mitigation and Response Insights
- Application Insights

Let's look at some of the content of Insight reports and see how they can help you.

Executive Insights

Executives are busy people who need to know what is going on in their network, so the Executive Insights report includes graphic details about threats seen on the network, including trends, the most at risk users, devices, and groups, and information about the deployment. Each status is explained. Altogether, it lets you see the status of your endpoint security and the value that SentinelOne products provide. Here is an example:



The Threat landscape section shows you how many threats were detected *pre-execution*, before they had a chance to execute, as opposed to *post-execution*, where they started running before the SentinelOne Agent detected them. On the right side, you can see the real value of the Agents – how many of the threats detected were *known threats*, known to reputation services, compared to threats that only a solution like SentinelOne can detect – *unknown threats*, which have never been seen before.

We also acknowledge if we detected benign activity as malicious.

Most at Risk

Often, when you look at the quantity of threats, you don't see the details behind the numbers. Adversaries might attempt to compromise specific users, devices, or groups and you should know about it so you can take action accordingly. Is your finance group exposed to the most threats? Maybe your CEO? Or your sysadmin?

In the Threats Insight report, you'll find more information about those who are at risk.

Deployment

To make a security product fully effective, it must be deployed across your network. For attackers, even a single weak entry point can be enough to cause damage. Seeing the deployment trends lets you understand where do you stand, how your teams are executing, and how much coverage you have. The trend measurement also shows you the velocity of the deployment.

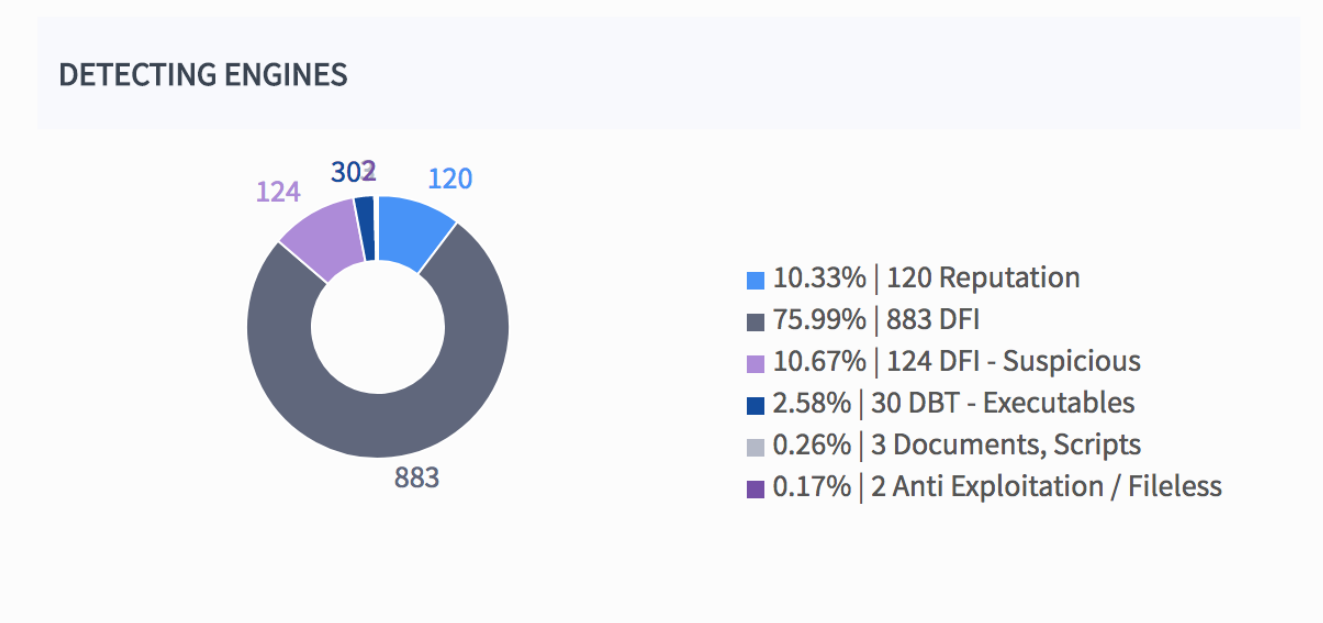
DEPLOYMENT TRENDS

METRIC	REPORT PERIOD	PREVIOUS PERIOD	TREND
Total Agents	295	271	+8.86%
Windows	117	106	+10.38%
macOS	159	150	+6.00%
Linux	19	15	+26.67%
New Agents	24	12	+100.00%
Scanned	53	42	+26.19%

Report period is 30 days

Threat Insights

Get more details on the security aspects of your network. In addition to the number of threats and their status, you can see which SentinelOne engines were effective in your environment. Just remember, the pre-execution engines get the first chance to detect. Then come the post-execution engines. File-less attacks are mostly detected by the Documents, Scripts, Exploits and Fileless engines. These attacks are most likely to bypass other security products. SentinelOne engines protect you from all types of attacks.



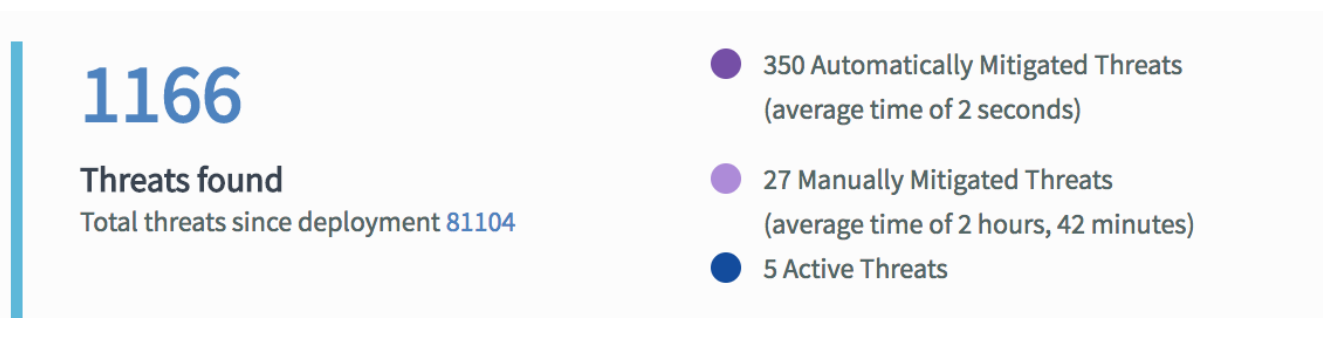
Another interesting metric is threat indicators. Although threats detected by SentinelOne Agents provide context information, you can also see these short and descriptive indicators to allow sysadmins to figure out why an item was detected. See what is common in your network so you know what changes to make in your security procedures.

TOP INDICATORS

Indicator	Occurrences	Most seen Agent
This binary contains abnormal section names which could be an indication that it was created with non-standard development tools	151	garym-surfacepro
This binary may contain encrypted/compressed info as measured by high entropy of the sections (>6.8)	153	garym-surfacepro
The majority of sections in this PE have high entropy which is a sign of obfuscation/packing.	196	garym-surfacepro
This binary imports debugger functions	137	garym-surfacepro
This binary has an RWX section. It might contain self-modifying code.	122	garym-surfacepro

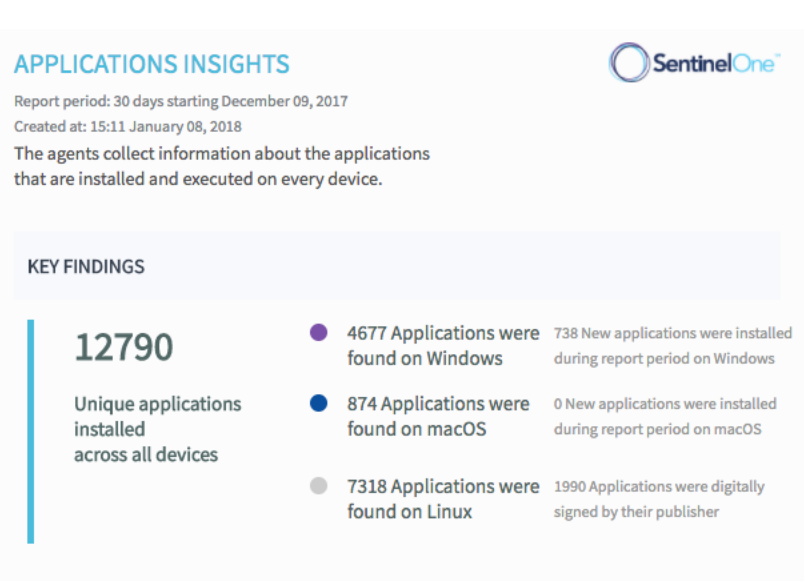
Mitigation And Response Insights

How much time passed from detection to automated mitigation? How long did the sysadmin take to act when necessary? What is still active?



Application Insights

SentinelOne Agents are aware of all installations on the endpoints. So, we can give you insights into your applications, and what was installed recently, by OS. You can check for application updates and security alerts for vulnerabilities.



Bottom Line

With SentinelOne new Insight reports, you get a wide variety of methods to analyze and present custom data visualizations. This gives you a wide variety of ways to analyze and present custom data visualizations.

Insight reports are accessible in the Bahamas console version, which is now available to all our customers.

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

Read more about Cyber Security

- Announcing 2.5/Bahamas Release
- PowerQuery Brings New Data Analytics Capabilities to Singularity XDR
- Mobile Threat Defense | Bringing AI-Powered Endpoint Security To Your Mobile Devices
- Rapid Response with XDR One-Click Remediations
- Feature Spotlight | Introducing Singularity Dark Mode
- Introducing the New Singularity XDR Process Graph