Key use cases

Am I under attack?

- **Advanced detection** – based on machine learning, including cloud sandboxing – automatically detects threats.
- **Download and scan IoC**s from securelist.com or other sources to find advanced threats.

Can I neutralize it?

- **Utilize multiple response options** – isolate host, prevent file execution or remove it.
- **Scan other hosts** for signs of the analyzed threat.
- **Apply an automatic response** across hosts on discovering a threat (IoC).

How do I get some skills training?

- **Check out the response guidance** in the alert card.
- **Access the Threat Intelligence Portal** and the latest TI.
- **Develop your expertise** as you analyze and respond to threats.

How did it happen?

- Analyze the threat in a **visual process tree.**
- Track its actions in a **drill-down graph.**
- **Understand its root cause and entry point** into the infrastructure.

How do I stop it ever happening again?

- **Put learnt information to use –** knowing which IPs and websites to block, policies to modify and employees to train.
- **Create rules for preventing** such threats in the future, e.g. prevent file execution.

What about all the commodity threats?

- **Next-gen endpoint security** is on board to stop most threats right away.
- **Step up your patching** with Vulnerability and Patch Management.
- **Automate your attack surface reduction** and policy adjustment with endpoint controls.

How it works