A new source of information: User programs.

System Information and Event Management (SIEM) solutions have become a necessity to manage the security of both large and mid-sized IT infrastructures. Their capabilities to collect and correlate the status of IT systems allow organizations to turn massive volumes of data into useful information for decision making.

Integrate a new source of critical information into the security intelligence collected and correlated by your SIEM: all processes and programs run on your devices and continuously monitored by Panda Adaptive Defense.

A new security status.

IT Departments require high levels of visibility and control to be able to anticipate the security problems caused by next-generation malware.

Panda Adaptive Defense helps administrators filter the huge volumes of data handled by SIEM systems and focus on what really matters:

› What new programs are being run and are yet to be classified as goodware or malware?

› How did those programs reach the network?

› What suspicious activities are they performing on user devices (registry editing, hooks, driver installation, etc.)?

› What legitimate software with known and exploitable vulnerabilities is being used?

› What processes are accessing user documents and sending information out?

› What is the network usage of each process run on the IT network?

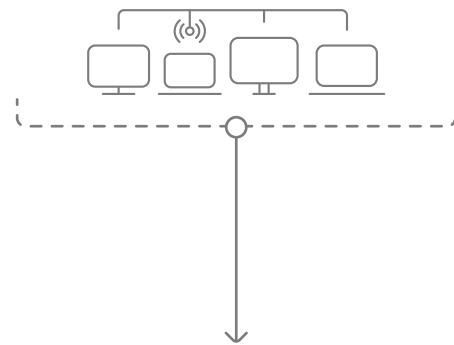## Seamless integration and operation.

Panda Adaptive Defense seamlessly integrates with existing corporate SIEM solutions without additional deployments on users' devices. Monitored events are sent securely using the LEEF/CEF formats compatible with most SIEM systems on the market either directly or indirectly via plugins.

Panda Adaptive Defense

Panel SIEM

Supported Platforms and System Requirements for SIEM Feeder:

http://go.pandasecurity.com/siem-feeder/requirements

This module is available in:

◎ Panda Adaptive Defense

◎ Panda Adaptive Defense 360

Compatible with:

ALIEN VAULT   ArcSight An HP Company   QRadar   bitacora   lookwise   **Compatible with LEEF and CEF formats too**