

# Cisco Identity Services Engine and User and Entity Behavior Analytics Integration

## Improve the analytics and mitigation of high-risk use

User and Entity Behavioral Analytics (UEBA) technologies help detect malicious and abusive user activities that may otherwise go unnoticed. Through [pxGrid](#) integration you can quickly map user activities to the wealth of user identity, endpoint, and network information generated by the [Cisco® Identity Services Engine \(ISE\)](#).

With all this data in one place your security analysts can quickly determine who is involved in a security event, whether it needs further investigation, and how urgent a threat it is. They can vastly shorten the time it takes to remediate network security threats.

## Benefits

- **Get answers faster** so you decrease the time it takes to classify and respond to events
- **Stop bad behaviors faster** through faster event responses to high-severity events
- **Protect critical data faster** by quarantining a user or redirecting traffic for deeper investigation

## Next steps

To learn more about the Cisco Identity Services Engine, visit:

<http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html>.

To learn more about Cisco pxGrid, visit:

<http://www.cisco.com/go/pxg>.

For additional information regarding the Identity Services Engine and other Security Information and Event Management system (SIEM) and threat-defense integrations, visit

<http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html>.

## How ISE and UEBA work together

Cisco ISE provides its user identity and device information to the UEBA system through pxGrid, which is associated with UEBA-detected events. When they're identified, you can use the network as an enforcer and mitigate a threat right from the UEBA product.

The information that ISE provides to UEBA products includes:

- User
- IP address
- Authentication status
- Location
- User class (authorization group, guest, quarantine status)
- Manufacturer, model, OS, OS version, MAC address, IP address, network connection method (wired or wireless)
- Posture and compliance status (antivirus installed, antivirus version, OS patch level, mobile device posture compliance status (through Cisco mobile device management partners))
- Location
- Threat level

## What is pxGrid?

The Cisco Platform Exchange Grid is a standards-compliant cross-platform network system. It allows many IT intelligence products to share contextual information. Security monitoring and detection systems, network policy platforms, asset and configuration management systems, and identity and access-management platforms from Cisco and Cisco pxGrid partners are among those that can share and correlate data for heightened security.