CSA SINGAPORE | SG Passion Made Possible

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

ETHOS (Emerging THreat Open Sharing): An Introduction

Edgard Capdevielle, CEO
Nozomi Networks

ETHOS: Emerging THreat Open Sharing

The OT-centric open platform for anonymous threat sharing

Correlates security events across end users regardless of the security solutions they use

A benefit to critical infrastructure providers and governments

Leverages crowdsourced information in a community platform

Designed to reduce timelines for identifying novel threats targeting OT systems

Ethos
Intelligence Sharing Association

How ETHOS Discovers New and Novel Attacks

Continuous rapid exchange of emerging threat intelligence

- Defining Emerging Threat Intelligence: **Potentially** malicious events observed on production networks

Automated detection of new attack trends

- Analysis is performed via machine learning
- To maintain privacy, only affected contributors are notified
- The goal is to significantly reduce breach dwell time and stop lateral movement

Automatically receives and analyses data in real-time

- Data is submitted continuously and requires no user interaction
- Submitted data includes, but is not limited to, IOCs

Results processed into actionable threat intelligence

- Shared via STIX/TAXII

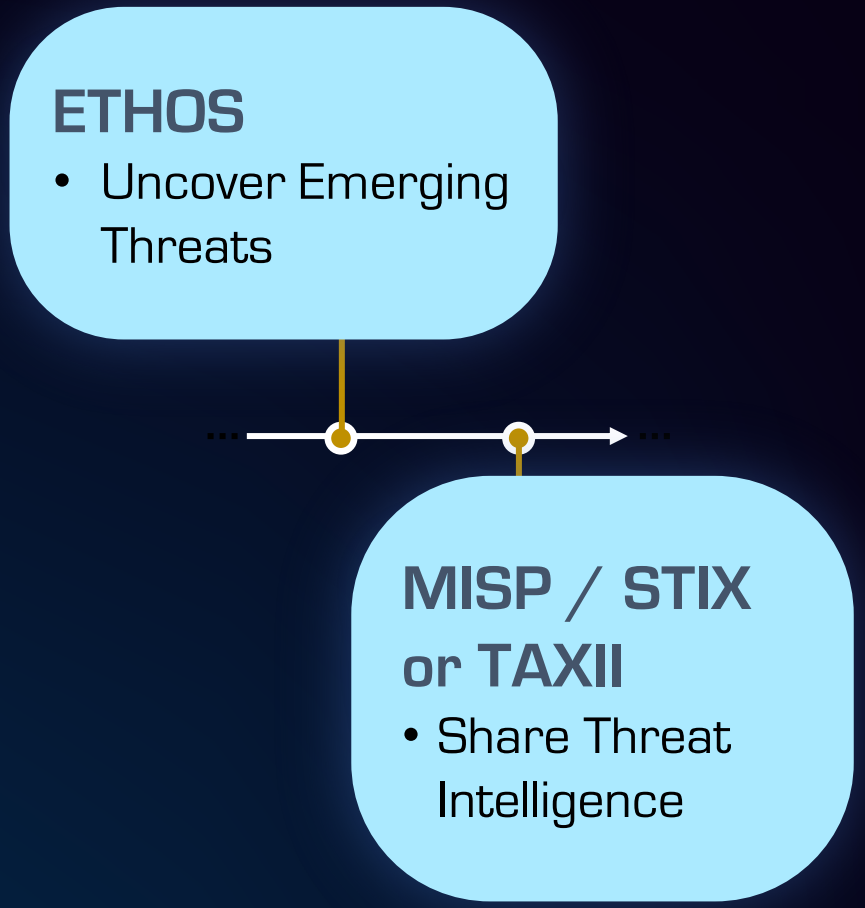
Ethos
Intelligence Sharing Association

What Makes ETHOS Unique

With ETHOS, our collective goal is to uncover emerging threats for which there is no threat intelligence available

How ETHOS integrates with STIX / TAXII or MISP

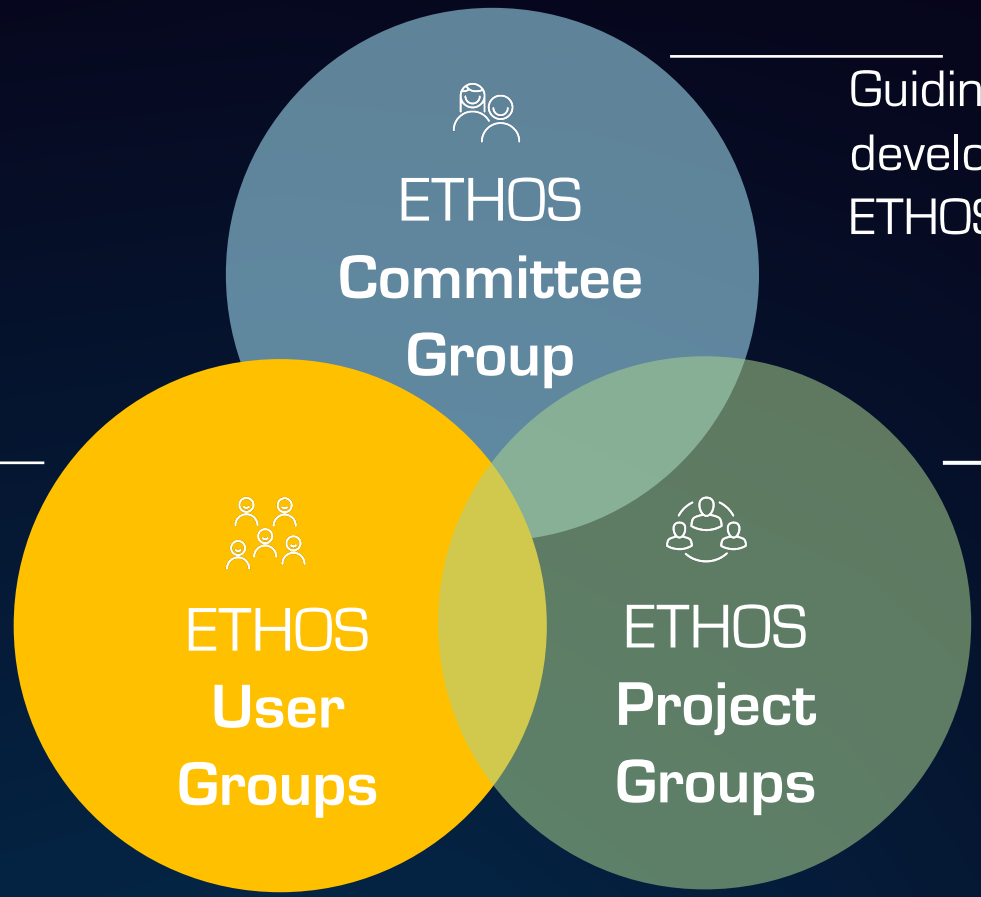
ETHOS uncovers patterns and trends which can then be expertly analysed and shared through STIX / TAXII or MISP—as well as the privacy-focused collaboration tools in ETHOS.



Ethos
Intelligence Sharing Association

ETHOS is a Community-driven Project

Modelled after the Kubernetes Community



Guiding the ongoing development of ETHOS

Articulating the needs of the user community to the ECG

Responsible for the development of assigned projects from the ECG

Ethos
Intelligence Sharing Association

Ethos
Intelligence Sharing Association

ETHOS Community Today

1898 & CO. PART OF BURNS MCDONNELL
ABS Group
WATERFALL Stronger Than Firewalls
CLAROTY
FORESCOUT Automated cybersecurity across your digital terrain
Ethos
NETRISE
Schneider Electric
tenable
NRECA America's Electric Cooperatives
NOZOMI NETWORKS
DRAGOS
np network perception

THANK YOU

Ethos
Intelligence Sharing Association