

"Businesses must apply in-country insight and intelligence to determine all potential vulnerabilities, threats and risks to their most valuable assets."

John Watters,
CEO of iSIGHT Partners

EC⁴ – Electronic Crime Command and Coordination Center™

What is EC⁴?

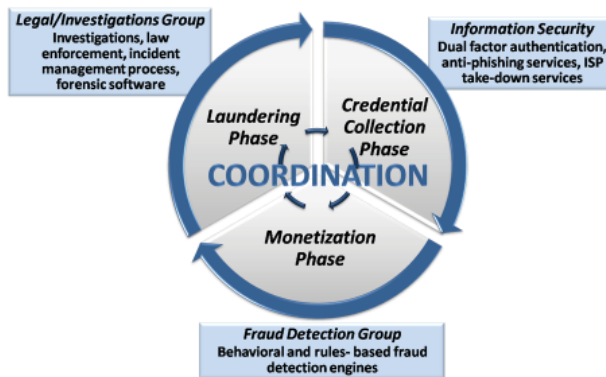
iSIGHT Partners' Electronic Crime Command & Coordination Center™ (EC⁴) is a patent-pending combination of technology and processes that leverages information about the electronic crime ecosystem to help customers prevent, detect and manage electronic crime losses. For example, we obtain the identity of fraudsters, which tools and tactics they are using and then disrupt their process.

iSIGHT Partners' products, solution sets and global intelligence experts ensure an integrated approach to risk identification and mitigation across cyber and physical assets, managing real-world risk beyond the edge of our customers' resources and physical boundaries.

Electronic Crime Ecosystem

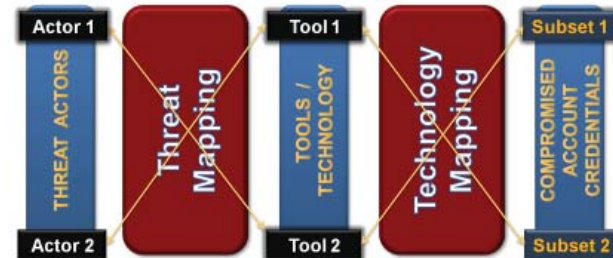
The Electronic Crime Ecosystem has three phases, each of which is countered by our EC⁴ strategies.

- **Credential Collection Phase** – iSIGHT Partners helps Information Security Teams monitor the trafficking of customer credentials in the underground.
- **Monetization Phase** – iSIGHT Partners helps Fraud Detection teams better understand the tools, techniques and processes used by cyber criminals to defeat fraud controls.
- **Laundering Phase** – iSIGHT Partners helps Legal and Investigation Teams understand the dynamic nature of the laundering techniques used to "clean" money.



Threat Mapping

Threat mapping is the process of identifying and matching the threat actors with the specific tools and tactics they use to compromise accounts, as illustrated in the following graphic.



EC⁴ Process

In order to map threats created by account compromises, iSIGHT Partners takes the following steps:

- **Account Data Analysis:** Determine characteristics about compromised accounts to set baselines and determine trends
- **Process Reversing:** Reverse engineer both the manual and automated methods attackers use to monetize accounts
- **Attack Signature Generation:** Augment current fraud detection capabilities
- **EC⁴ Stand-Up:** Leverage technology to aggregate threat and vulnerability scoring from all groups

EC⁴ provides a set of actionable mitigation strategies to:

- Reduce False Positives
- Disrupt the Marketplace
- Reduce Fraud Loss
- Attack the eCrime Business Model

Attacking the Adversary's Business Model

Since criminals need money to make money, EC⁴ works to define and subvert their business model, making it too expensive and difficult for them to target our clients' assets. *We increase their pain and decrease their gain.*

Our core objective is to reduce your adversary's revenue (your losses), drive up their cost of executing fraud strategies by tightening controls; and through creative investigative support, we increase the risks associated with attacking our clients.

In other words, we **define and attack the bad guy's business model**, which will eventually make it too expensive and difficult for the adversary to attack our clients.

Contact iSIGHT Partners today to learn more about EC⁴ and our other products and strategies.



| www.isightpartners.com |