Security Risk is Organizational Risk

20th century
Prevent compromises & security events

21st century
Manage & Respond to the risk presented by compromised assets
Impact Magnified

Detection & Response is a Critical Gap

- Average days until compromised asset detected: 205
- % victim organizations notified by 3rd party such as the FBI: 69%
- % victim organizations not compliant with regulatory requirements: 89%

CI Security
Quantifying security risk

\[ R = P(T_v) \times I \]
Options: Solving for Impact Risk

1. Accept the risk (‘71 Pinto method)
2. Repurpose IT (dilutes digital transformation projects)
3. Build your own SOC (8+ FTEs and must certify)
4. Leverage managed detection & response services

https://ci.security
Managed Detection & Response
Dedicated team of personally-engaged experts

Combined with next-generation analytics

Continuous threat detection, response, and hunting

Collaborating real-time with your IT teams
How does it work?

**Critical Insight Collector**

- **Data Ingested**: Full packet capture, Netflow (packet metadata), Arbitrary server logs, Security technology alerts, Network infrastructure logs

- **Transmits**: metadata and alerts sent to the Security Operations Center

**CI Security Operations Center**

- **Machine**: Advanced analytics, second level correlation, enhanced data visualization & advanced threat intelligence

- **Human**: Analyst event review, full investigation, Incident Action Plans & response planning
PISCES: "Public Infrastructure Security Collaboration and Exchange System"
Incident Action Plan
Within an hour of the threat detection

• Analyst investigation confirmed real threat
• Presents specifics of the threat
• Lists key actions to respond to & recover from the threat
• Includes instructions for preservation of evidence