John Williamson

Vice President, CI Security

www.ci.security

GCI

Security Risk
is **Organizational Risk**

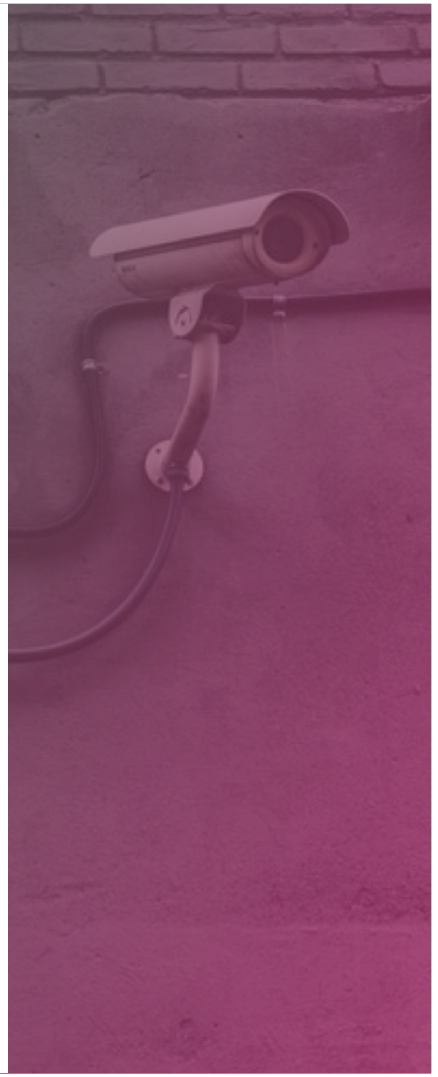
20th century

Prevent compromises & security events

21st century

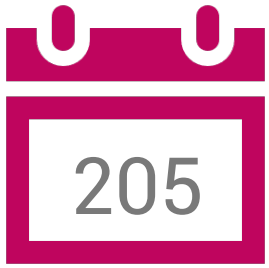
Manage & Respond
to the risk presented by compromised assets

CI Security

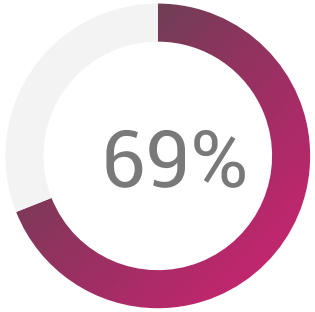


Impact Magnified

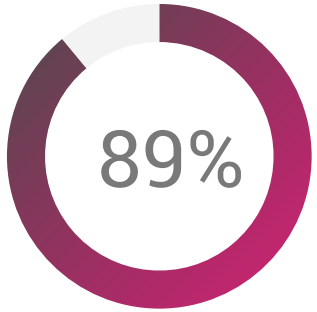
Detection & Response is a Critical Gap



average days until compromised asset detected



% victim organizations notified by 3rd party such as the FBI



% victim organizations **not** compliant with regulatory requirements

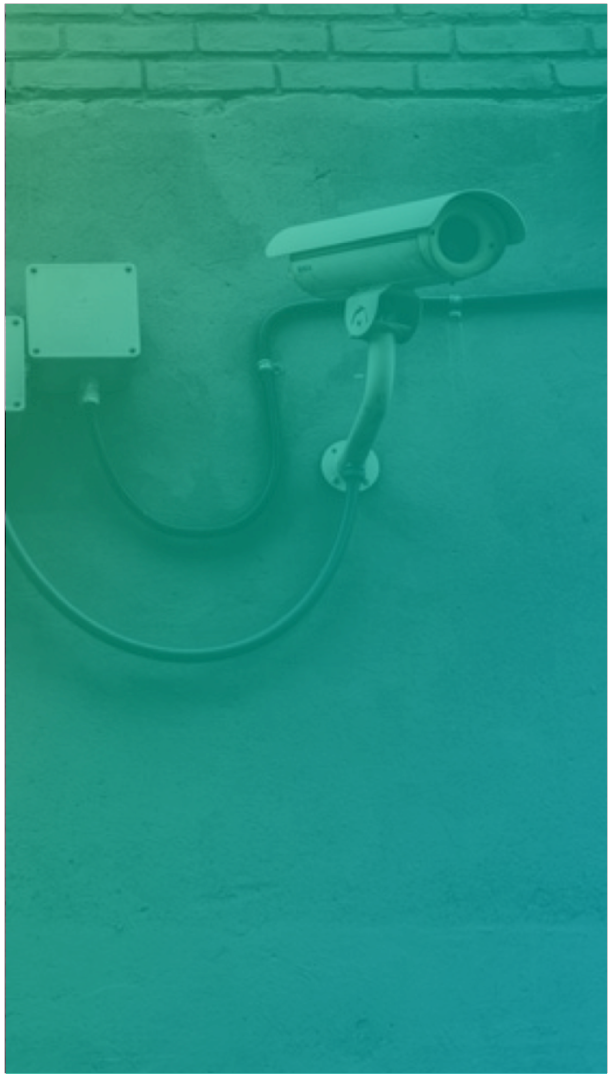
CI Security

Quantifying security risk

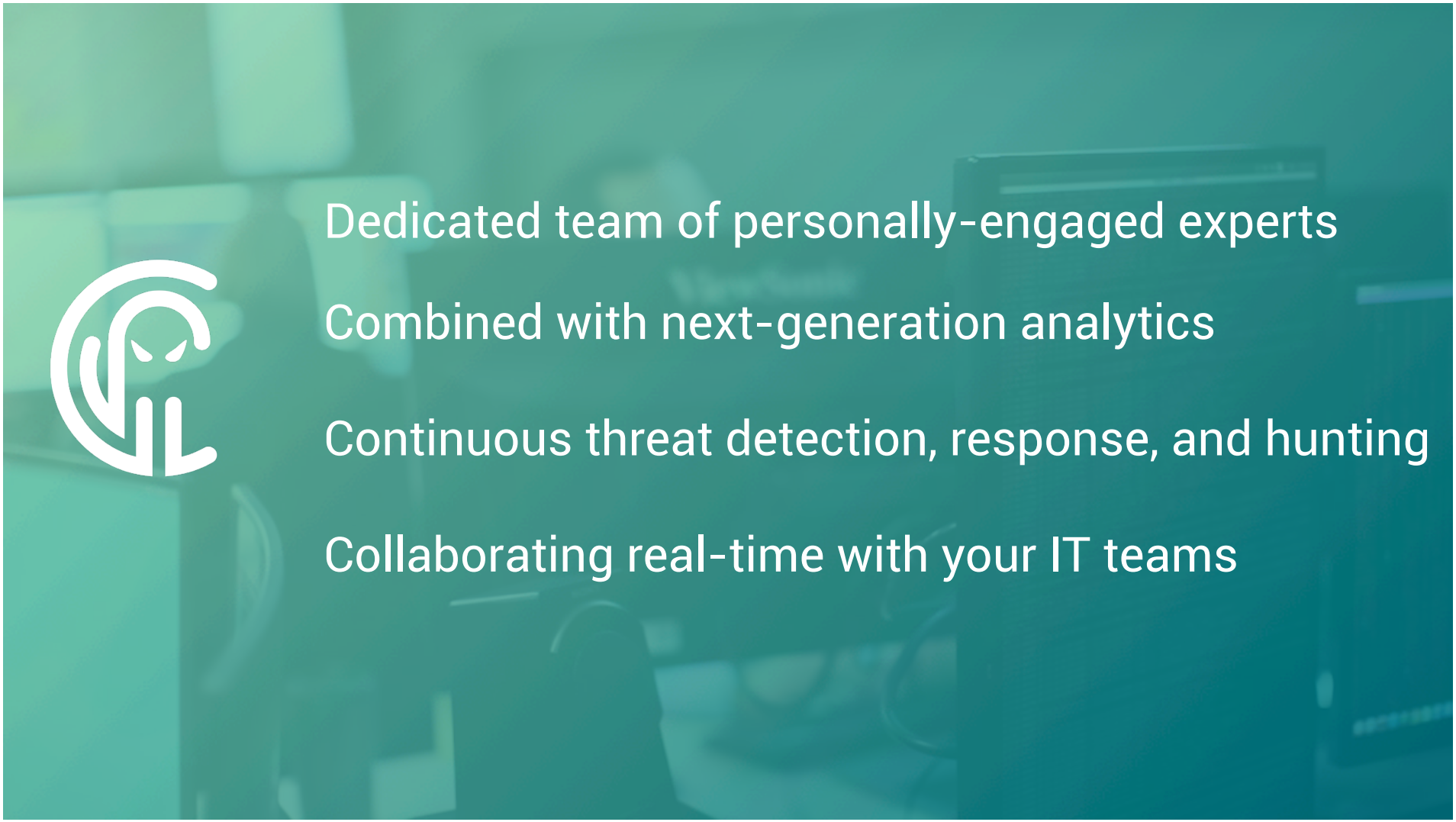
$$R = P(T_v) \times I$$

Options: **Solving for Impact Risk**

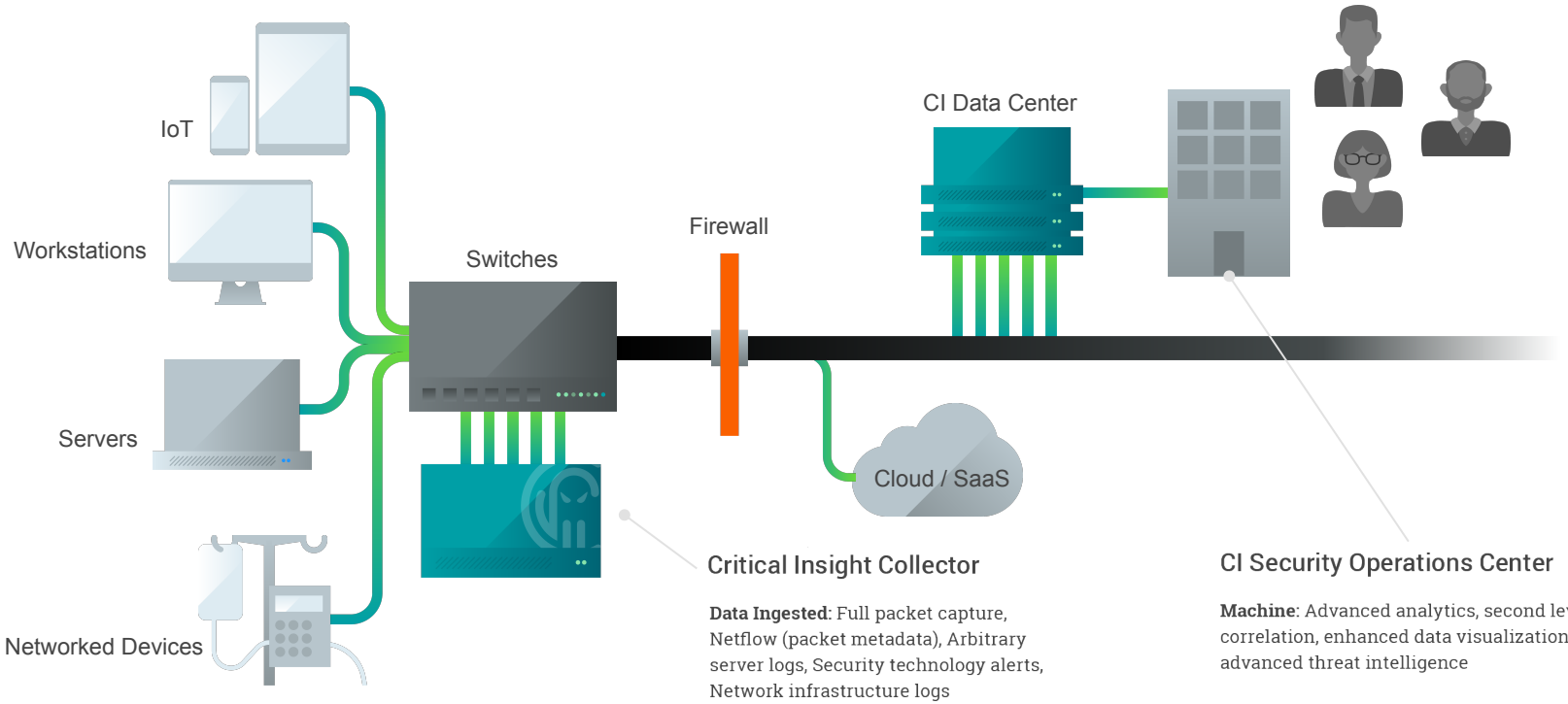
1. Accept the risk (‘71 Pinto method)
2. Repurpose IT (dilutes digital transformation projects)
3. Build your own SOC (8+ FTEs and must certify)
4. Leverage **managed detection & response services**




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

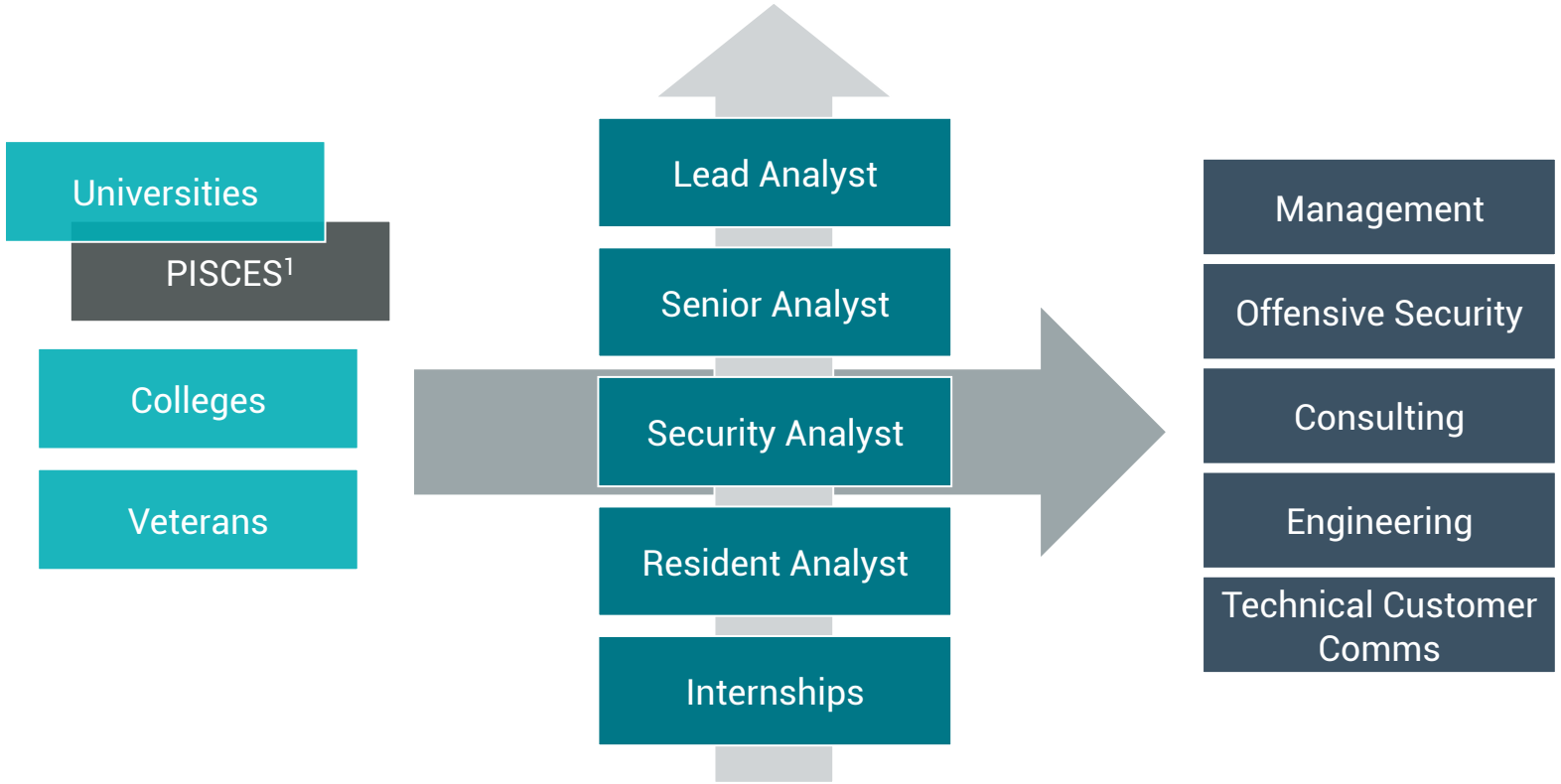
CI Security Operations Center

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

Human: Analyst event review, full investigation, Incident Action Plans & response planning

CI Security

PISCES



CI Security

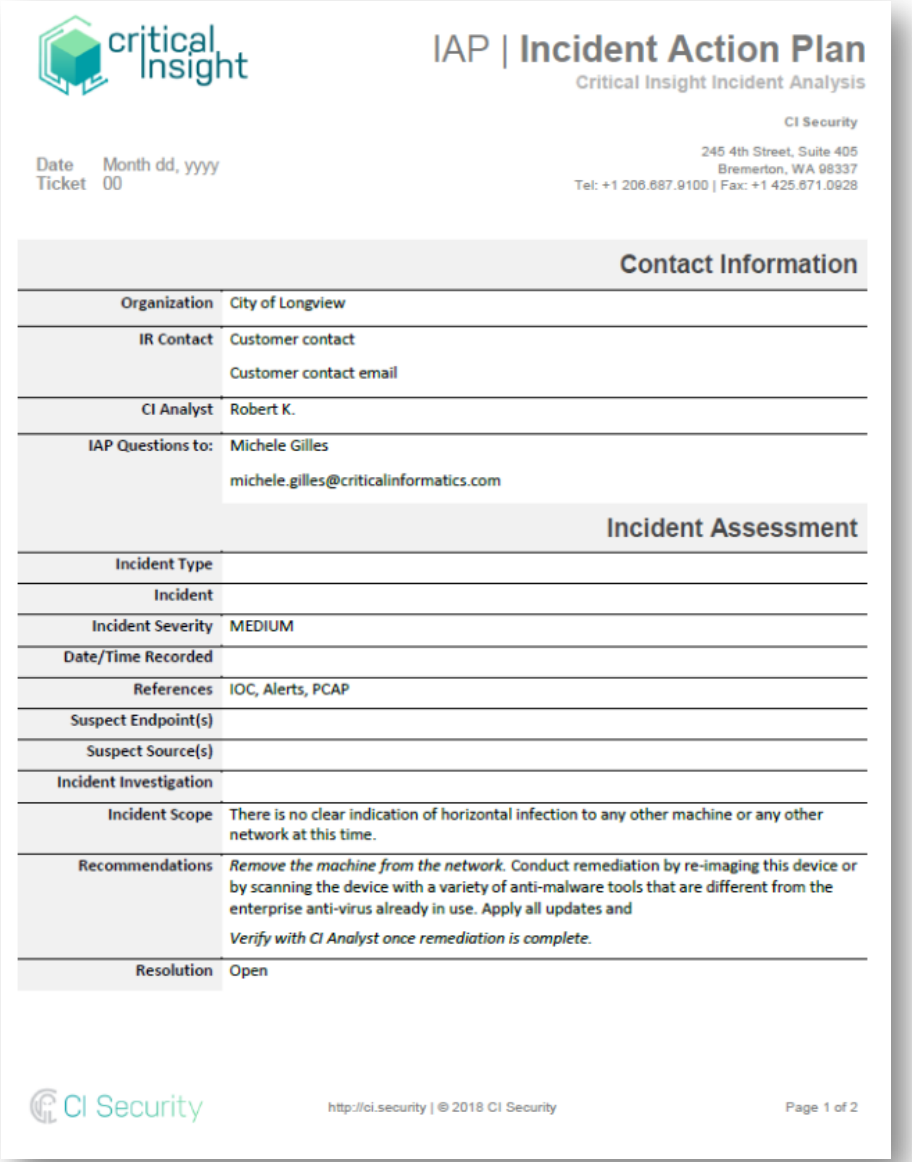
[1]PISCES: "Public Infrastructure Security Collaboration and Exchange System"

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

CI Security



critical insight

IAP | **Incident Action Plan**

Critical Insight Incident Analysis

CI Security

245 4th Street, Suite 405
Bremerton, WA 98337
Tel: +1 206.687.9100 | Fax: +1 425.671.0928

Date Month dd, yyyy
Ticket 00

Contact Information

Organization	City of Longview
IR Contact	Customer contact Customer contact email
CI Analyst	Robert K.
IAP Questions to:	Michele Gilles michele.gilles@criticalinformatics.com

Incident Assessment

Incident Type	
Incident	
Incident Severity	MEDIUM
Date/Time Recorded	
References	IOC, Alerts, PCAP
Suspect Endpoint(s)	
Suspect Source(s)	
Incident Investigation	
Incident Scope	There is no clear indication of horizontal infection to any other machine or any other network at this time.
Recommendations	*Remove the machine from the network.* Conduct remediation by re-imaging this device or by scanning the device with a variety of anti-malware tools that are different from the enterprise anti-virus already in use. Apply all updates and *Verify with CI Analyst once remediation is complete.*
Resolution	Open

CI Security http://ci.security | © 2018 CI Security Page 1 of 2

CI Security

GCI

john.williamson@ci.security