Priority Intel Requirements

When Everything everywhere all at once comes together

- Inventory
- Modeling
- Landscaping
- Profiling

What are they?

Requirements provide direction for an intelligence analyst to gather and collect information.

Requirements define the required resources and also gaps in capabilities for collection management purposes.

Requirements determine the end product that will be produced and whether the end-user will be satisfied with the results.

Where to start?

- What team can you augment
- Biggest risks
- Biggest impact on business

Teams to Augment

- Executive management
- Security operations
- Incident response
- Risk management
- Vulnerability Management
- Privacy
- Legal
- Forensics

Types of PIRs

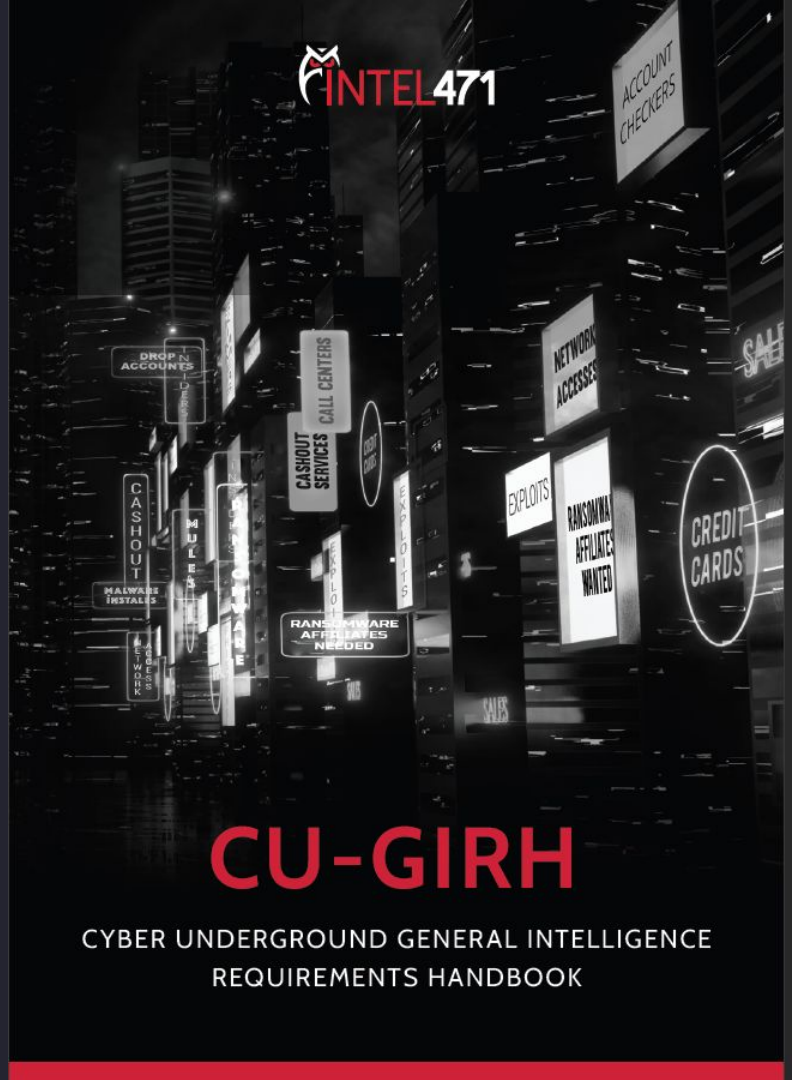
- Brand impairment (reputational risk)
- Legal or compliance failure
- Financial fraud
- Operational disruption
- Competitive disadvantage

Some Examples

SecOps 1.0		
1.01	Threat List	Providing Threat list of IPs, Hashes, Domains, ULs, and Emails to search against organizations data lakes.
1.02	TTP	News on latest trends in TTPs used by threat actors.
1.03	Threat Profiles	Detailed description of Threat actors, their TTPs, and their targets.
1.04	Hunting Packages	Reports on threat actors, what they are doing, and how to detect it within our network.
TVM 2.0		
2.01	Vulns in Tech Stack	Tracking news, or release of vulnerabilities within your tech stack
2.02	PoC in Tech stack	Tracking news, or release of Proof of concept within your tech stack
2.03	Exploits in Wild Tech Stack	Tracking uses of exploits in your network being used in the wild.
2.04	Vuln Risk List	Exporting PoC, and use in the wild data to TVM data for risk based patching
Brand Intel 3.0		
3.01	Domain Intel	Tracking newly created domains/subdomains similar to our organization
3.02	Code Leaks	Using keyword to search for possible code leaks
3.03	Social Media Intel	Tracking possible social media mentions of the organization
3.04	Logo intel	Tracking where organizations logo is being used.
Dark web 4.0		
4.01	Dark web Brand	Monitoring for communications mentioning your brand
4.02	Dark web Vuln	Monitoring for communications on vulnerabilities you are tracking
4.03	Dark web Marketplace Tracking	Monitoring Marketplaces for possible sales of access to organization network
4.04	Dump Site tracking	Monitoring Dumps sites for mentions of your organization
Geo-political 5.0		
5.01	Geo-political Risk	Tracking possible geo-political problems where our organization has assets or people.
Active Intel 6.0		
6.01	New Deception deployment	Actively deploying and improving deception tactics within the organization network.
6.02	Deception Testing	Monitoring and testing deception Tactics
OSINT 7.0		
7.01	OSINT augmentation	Ability to help or argument OSINT investigations.
7.02	competitor tracking	Tracking if competitors breaches and other information.
7.03	Industry tracking	Tracking if competitors breaches and other information.
Financials 8.0		
8.01	Financials Tracking	Tracking use of financial indicators such As Credit Cards, Bank Accounts, or SWIFT Account numbers
Risk 9.1		
9.01	Partners and Vendor Tracking	Tracking vital partner and vendors for Breaches/compromise

What are some PIRs your organization would use?

They Do


INTEL471
ACCOUNT CHECKERS
DROP ACCOUNTS
CASHOUT SERVICES
CALL CENTERS
CASHOUT
MALWARE INSTALLS
MULES
EXPLOITS
RANSOMWARE AFFILIATES NEEDED
NETWORK ACCESSES
EXPLOITS
RANSOMWARE AFFILIATES WANTED
CREDIT CARDS
SALES
CU-GIRH
CYBER UNDERGROUND GENERAL INTELLIGENCE REQUIREMENTS HANDBOOK