Developing Cyber Threat Intelligence…

or not failing in battle.

SANS Cyber Defense Summit,
19 August 2014

Adrien de Beaupré
SANS ISC Handler
SANS Instructor
Intru-Shun.ca Inc.

About me

- 34+, 24+, 14+ years
- Contributor to OSSTMM 3
- Contributor to Hacking Exposed, Linux 3rd Ed
- Contributor to SANS Incident Handling Guide
- Co-developer of Incident Management Capability Maturity Framework (Bell Canada)
- SANS Instructor 401, 503, 504, 542, 560
- Threat Intel and IR with CCIRC

Introduction

- What is CTI
- Where can I get some?
- Proposed architecture and tools
- Conclusion

CTI

- "The ability to collect, share, and analyze data in order to tailor responses to a threat..."
  Paul E. Kurtz
  Cyber Security Expert and Presidential Advisor
- Situational awareness for organizations is comprised of relevant information on new threats, new vulnerabilities, trends, and targeted attacks from external sources. This must be combined with detailed knowledge and data from internal activities.

Requirements

- Useful! ☺
- Timely – Moving at Internet speed
- Accurate – Trusted sources, validated data
- Tailored – Relevant to your organization
- Correlated – Multiple sources of data
- Actionable – Prevention, detection, or mitigation
- Analyzed – Intelligent human analysis
- Mitigation – How to respond, recommendations
- Metrics – Quantitative, measurable, trends
- Severity – Rating system
- Interactive – Consulting and research

Intel

- Incidents
- Indicators (IOC)
- Vulnerabilities
- Malware
- Exploits
- Tools
- Tactics
- Techniques

- Signatures
- File hashes
- Trends in technology
- Trends in threats
- Threat agents, human intel
- Known bad domains and netblocks
- Anything else new

Frameworks

- Open Indicators of Compromise (OpenIOC) framework
- Vocabulary for Event Recording and Incident Sharing (VERIS)
- Cyber Observable eXpression (CybOX)
- Incident Object Description and Exchange Format (IODEF)
- Trusted Automated eXchange of Indicator Information (TAXII)
- Structured Threat Information Expression (STIX)
- Traffic Light Protocol (TLP)
- Open Threat Exchange (OTX)
- Collective Intelligence Framework (CIF)
  - Greg Farnham, Tools and Standards for Cyber Threat Intelligence Projects (SANS Reading Room 2013)

Capability Maturation

1. No Threat Monitoring
2. Web Surfing as needed (ad hoc)
3. Public Feed Correlation
4. Commercial Feed and Correlation
5. Industry Participation
6. Threat Analysis Leadership (internal capability)

Source: Incident Management Capability Maturity Framework

How to

- This proposed threat environment monitoring capability uses a variety of processes, tools, information sources, etc to gather external and internal information regarding known threats and vulnerabilities pertinent to the organization in order to develop targeted cyber threat intelligence.
- Includes collection of security incident alerts and warnings from external organizations, as well as internal indicators (logs, traffic analysis, etc)

Sources of Information

TYPE	INTERNAL	EXTERNAL	
		Open	Closed/ Private
Free	Logs IDS DNS Honeypot Dark net Netflow	SANS ISC CERT Feeds AV Vendors MSRC SRI	FIRST MSRA / GIAIS ISC SIE
Commercial	MSSP	Secunia Symantec iDefense Dell Secureworks …	

Internal Sources

- People, process, technology.
- Trouble ticket/incident database.
- IDS/IPS, System logs, Application logs, Firewall logs, Router logs, Anti-malware logs, DNS (passive), Sniffers, SIEM, Log collectors, anything that can provide network traffic or logs.
- Anything that can provide metrics and trend them over time.
- Anything that can provide an indicator of compromise.

OSI

- Open source intelligence gathering
  - On yourself
  - On your industry
  - On your competitors
  - On your enemy
- Know yourself, know your enemy, pick your battlefield, arrive at the field of battle well informed and before the opponent. (Paraphrasing Sun Tzu and Musashi)

External Free Sources

- Threat Information
  - SANS Internet Storm Center: http://isc.sans.edu/
  - SRI Malware Threat Center: http://mtc.sri.com/
  - Malware domains: http://www.malwaredomains.com/
  - Team Cymru: http://www.team-cymru.org/
  - and many many many more…

External Free Sources

- C*RTS
  - CERT: http://www.cert.org/blogs/vuls/
  - US-CERT: http://www.us-cert.gov/
  - Aus-CERT: http://www.auscert.org.au/
  - AU GovCERT: https://www.cert.gov.au/
  - CCIRC: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx
  - NZ: http://www.ncsc.govt.nz/
  - UK: http://www.cpni.gov.uk
  - and others…

External Free Sources

- Twitter!
- AV Vendor Blogs
  - Avert Labs: http://www.avertlabs.com/research/blog/
  - TrendLabs: http://blog.trendmicro.com/
  - Kaspersky Lab Weblog: http://www.viruslist.com/en/rss/weblog
  - F-Secure Weblog: http://www.f-secure.com/weblog
  - and many more…

External Free Sources

- Other:
  - BugTraq: http://seclists.org/rss/bugtraq.rss
  - MSRC: http://blogs.technet.com/msrc/rss.xml
  - Microsoft Malware Protection Center: http://blogs.technet.com/mmpc/
  - Microsoft Research & Defence: http://blogs.technet.com/srd/default.aspx
  - and many many more…

External Commercial Sources

- Secunia: http://secunia.com/vulnerability_information/
- VeriSign®: http://www.verisigninc.com/
- Symantec™ DeepSight: http://www.symantec.com/deepsight-products
- iSIGHT Partners IntelliSIGHT: http://www.isightpartners.com/products/threatservice/
- Dell Secureworks: http://www.secureworks.com/
- Others…

External Private Sources

- FIRST
- Microsoft Security Response Alliance
- ISC Security Information Exchange
- Many 'un-named closed lists‘
- Others…

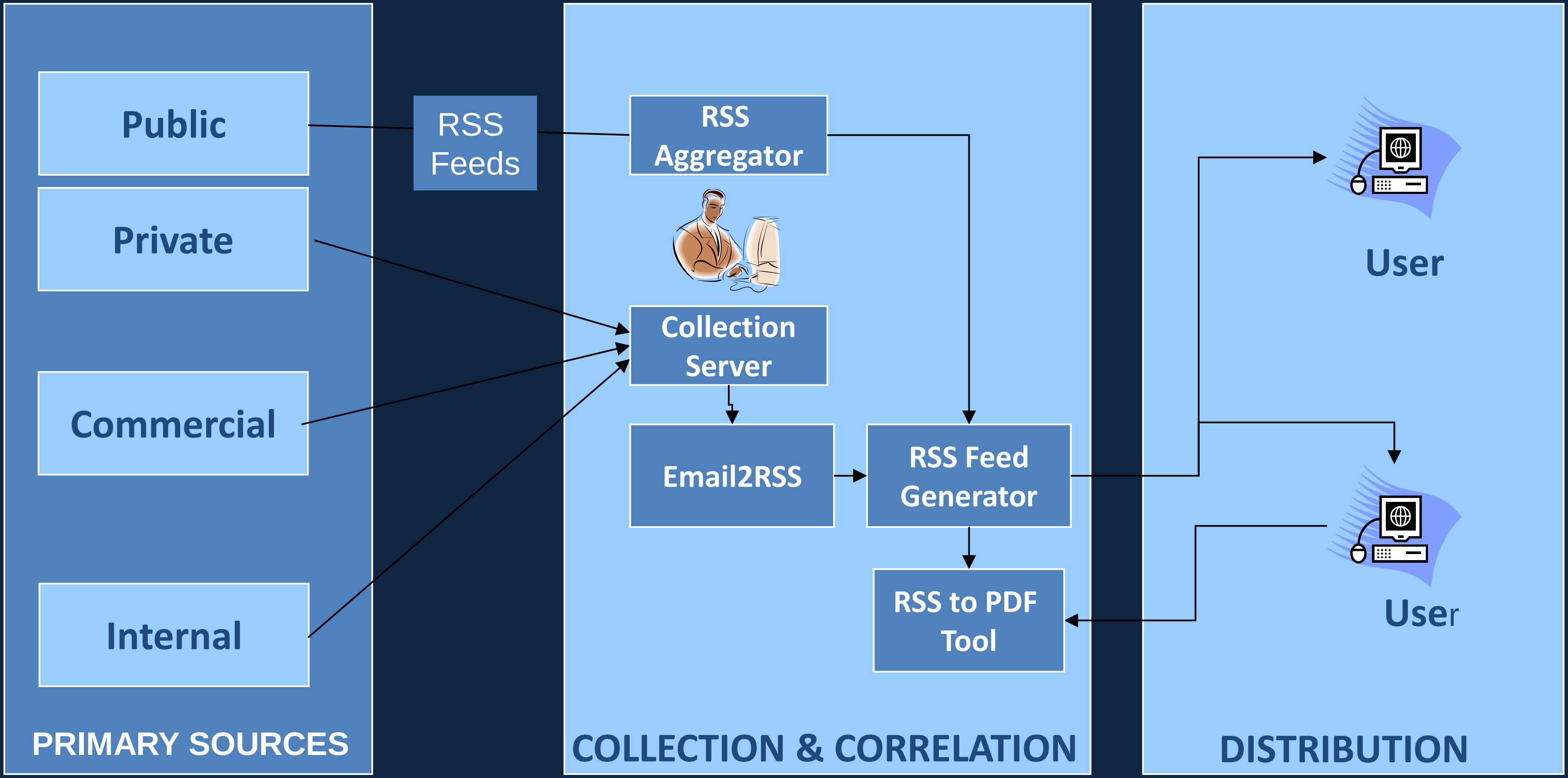
Issues & Challenges

- Quality of Threat Feeds (Free & Commercial)
- Technical Accuracy of Threat Feeds
- Timeliness of Threat Feeds (Early Warnings)
- Time Intensiveness
- Data Sensitivity
- Internal Information Sharing
- Liabilities with external information sharing
- Proving Organizational Value

Correlation of Sources

- The primary issue with threat environment monitoring is that few specific toolsets exist which allow for the correlation of threat feeds from multiple sources.
- Some SIEM tools, along with some Business Intelligence tools, can be used to create a work around, but each requires a certain amount of manual analysis for validation & verification.

Internal Architecture – Preliminary Low Cost Capability


PRIMARY SOURCES

Public

Private

Commercial

Internal

RSS Feeds

COLLECTION & CORRELATION

RSS Aggregator

Collection Server

Email2RSS

RSS Feed Generator

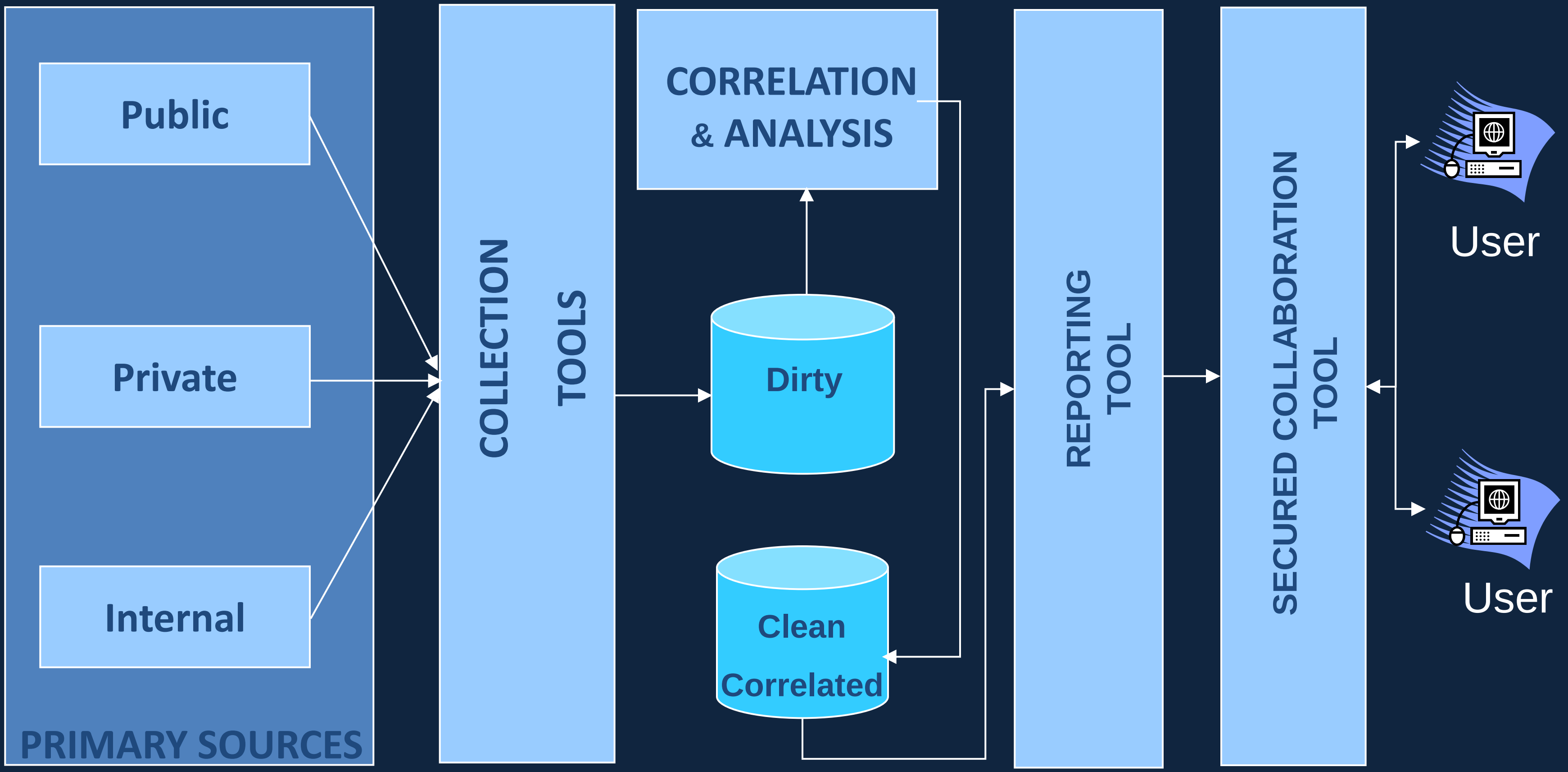
RSS to PDF Tool

DISTRIBUTION

User

User

Internal Architecture – Advanced Capability



Tools

- Collective Intelligence Framework https://code.google.com/p/collective-intelligence-framework/
- MANTIS http://django-mantis.readthedocs.org/en/latest/
- MISP https://github.com/MISP/MISP
- CRITS https://github.com/crits/crits

Conclusion

- Enterprises and organizations can build their own CTI capability.
- Requires internal, external, public, and private sources.
- Some of which may be specific to their industry or agency mandate.
- Trained analysts, good workflow, with good inputs and some technology gets good output.

Questions?

Thanks!

Adrien de Beaupré
SANS ISC Handler
Certified SANS Instructor
Consultant
Intri-Shun.ca Inc.
adrien@intru-shun.ca