TruSTAR & Retail-CISC: Optimize ISAO Intelligence Into Your Security Workflow

May 2018
Agenda

1. Overcoming Challenges
2. Optimizing Your Data
3. R-CISC Member Workflow Example
4. Threat Intelligence Exchange Best Practices
5. Resources
Overcoming the Challenges
The most valuable security data is locked inside the four walls of companies.
Security teams have many operational challenges

**Analyst Burnout**
Short staffed, overworked, burning out, given tedious tasks

**Unorganized Data**
Too much, no context, not timely, limited means to manage and organize, inability to leverage external sources, false positives, lack of metrics

**Non-Interoperable Technology**
Inefficient workflow, integration challenges, unclear privacy provisions
Streamline workflow to free-up analyst cycles

Data Flow

Enrich + Correlate

- R-CISC Member Submissions
- R-CISC Enclave/s
- 20+ OSINT Sources

Automated Detection

- R-CISC Enclaves

Enrich & Correlate

Extract indicators from email ingest and cross correlate with closed sources

TruSTAR / CyberUSA

Detect

Pull enclave data into Splunk to show direct correlation to logs with the ability to deep dive into TruSTAR
The TruSTAR // R-CISC Model

TruSTAR takes on the burden of ingesting and parsing data from ISAO and other intel sources.

It’s important to give ISAO members options to engage with ISAO and other sources:
- STIX/TAXII
- REST API
- Native Workflow Apps
- Email
- UI / Portal

platform gives R-CIS
Driving Intelligence into Enterprise Security Ops
Three Ways to Optimize Intelligence for Enterprise Security Operations

1. Capitalize on the intelligence value of your own event data
2. Operationalize ISAO relationships and other sources into your security operations workflow
3. Engage and grow your intelligence ecosystem
1. Capitalize on the intelligence value of your own event data

The richest data exists within your four walls.

Focus on correlating on that event data first that may be coming out of your SIEM, email gateway, Firewall, and sitting inside your case management / ticketing tools.
2. Operationalize ISAO relationships and other sources into your workflow

Integrate the external sources into your workflow.

Focus on minimizing noise and maximizing signal when ingesting data into your SIEM.

Then make sure you are shepherding intelligence to any alerts that are created - on-demand and IN-WORKFLOW!
3. Manage your intelligence ecosystem.

The intelligent enterprises of the (not-too-distant) future will be built on intelligence ecosystems that leverage data from across internal teams and external partners.

These relationships will be streamlined and bi-lateral. We won’t be talking about ‘sharing’ as much as we are talking about ‘EXCHANGE’ of intelligence.
So how does this look in an R-CISC member’s workflow?
See How R-CISC Reports Correlate to OSINT Data
See How R-CISC Reports Correlate to OSINT Data
Our traction

The most valuable data is locked in silos inside and across companies.

Exchange Best Practices
## The Old Way vs. The New Way

<table>
<thead>
<tr>
<th>LEGACY INFORMATION SHARING PROGRAMS</th>
<th>THREAT INTELLIGENCE EXCHANGE PROGRAMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share data about incidents after events are vetted, analyzed and often mitigated</td>
<td>Share suspicious event data as soon as it is identified</td>
</tr>
<tr>
<td>Data often shared via email, listservs and other manual</td>
<td>Data shared in many different formats, including via APIs</td>
</tr>
<tr>
<td>Often rely on trusted third party to manually scrub shared data of confidential information or submitter identity</td>
<td>Leverage encryption and other technologies to provide automation, anonymity, and sensitive or proprietary data redaction</td>
</tr>
</tbody>
</table>

Cite: Cloud Security Alliance
## A New Framework for Threat Intelligence Exchange

### IDENTIFY SUSPICIOUS EVENTS
Start with events generated by the SIEM or other tools that require review by an analyst.

### GATHER RELEVANT EVENT DATA
Don't limit sharing to indicators of compromise, but consider adding insight into adversary tools, techniques and procedures when available.

### DECIDE HOW TO SHARE DATA AND WITH WHOM
Determine with whom to share data and prepare it for submission. Organizations like CloudCISC cover the cloud community, but there may be value in sharing with other organizations and groups.

### MONITOR FOR EVENT FEEDBACK AND CORRELATION
Some tools that allow for real-time submission can also provide immediate feedback.

### ASSESS THE NEED FOR COLLABORATIVE RESPONSE
Decide whether and with whom to collaborate on defensive strategies.

Cite: [Cloud Security Alliance](http://www.cloudsecurityalliance.org)
Our traction

The most valuable data is locked in silos inside and across companies.
Reach Out to Learn More About R-CISC & TruSTAR

Visit: r-cisc.org/membership/
Contact: tommy.mcdowell@r-cisc.org

Visit: www.trustar.co/integrations
Contact: pcoughlin@trustar.co
Thank You!