Security Intelligence Status Report For Last 24 Hours
Business Area: Eastern Region
PST Friday March 8,
Security Event Activity Summary
E – Unknown Severity
D - Normal – Audit Trail
C - Suspicious – Alarm But No Damage
B - Threatening – Potential Harm
A - Critical – Business Impairment
Internal/External

ArcSight

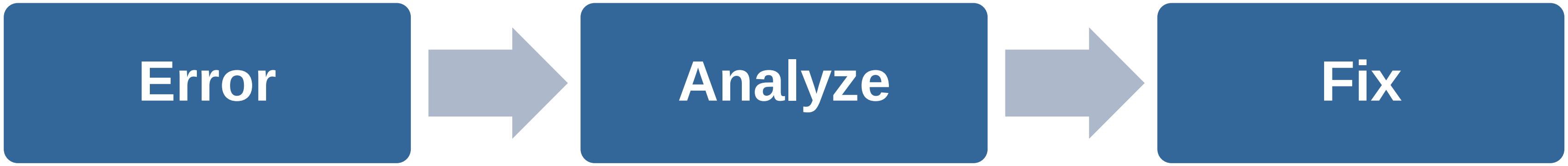
We! Secure

We! Analyze

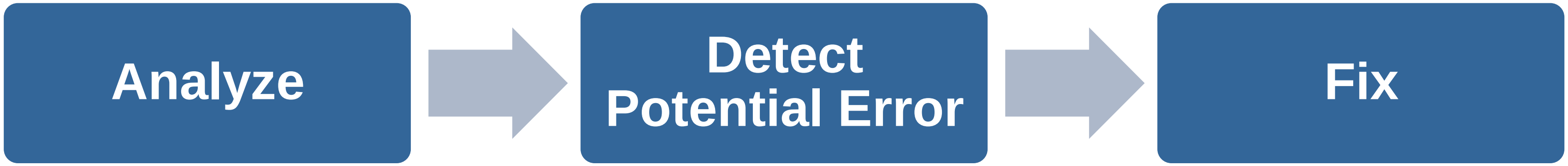
By: Or Cohen
We! Consulting

Troubleshooting Approach

Today, usually, we use a reactive approach to treat issues that appear in SmartConnectors:



We! Analyze changes that approach to a proactive one, which targets issues in the making:



By switching our approach, we can detect issues faster and fix them before they have the chance to cause actual critical damage.

Difficulties In Locating Errors

- Connectors service may be up and running but events are not forwarded to ESM/Logger/Express.
- Some Connectors collect events from several locations at once.
- Some Connectors only receive/read events once an hour/day/week.
- It is hard to detect the exact time the Connector stopped working properly.
- Relying on the Manager to tell you when something is wrong with the Connector.

The Solution – We! Analyze

- An independent system with its own UI which searches the Connectors logs on demand for a known list of 129 errors (in version 3.0.0.0) alongside custom errors.
- Post analyze, We! Analyze enables us to:
  - View the errors.
  - Google search the error.
  - Search the error in the ArcSight Forum.
  - Send the error by e-mail.
  - View a possible solution for the error.
  - Search the errors.
  - View errors statistics.
  - Send error by CEF Syslog.

We! Analyze – API

- We! Analyze can also be run via API with or without user intervention:
  - Activated thru a rule in the ESM/Express.
  - Activated thru a Tool or Integration Command.
  - Activated thru a schedule task in Windows.
- The results can be sent via CEF Syslog to a Syslog listener or saved locally to a file.

Tech. Details - We! Analyze

- We! Analyze supports network paths (UNC).
- It works while the Connector is up.
- It requires about 40mb of memory while analyzing (may require more with a large set of results).
- Analyzing a full log folder (200MB~, 22 log files) on a local server with all 129 known errors should take about 30 seconds to 2 minutes.
- Needs **.NET Framework 3.0** or higher to run.

About We!

- We! Consulting Group has been integrating ArcSight solutions for a long time and has gained a lot of experience with ArcSight product and troubleshooting issues of ArcSight products.
- We! specialize in troubleshooting and maintenance of ArcSight products alongside ArcSight planning, deployment, customization for customer needs and IR.
- If We! Analyze - 3.0.0.0 found an error that you are unable to fix, please feel free to contact us at any time using the contact information at the next page.
  We'll be happy to assist with any issue you may have.

Contact Information

- We! Analyze was developed by Or Cohen:
  - E-mail: Cohen88or@Gmail.com
  - E-mail: Or@We-Can.co.il
  - Phone: +972-050-8488497
  - Phone: +972-052-3279374
  - LinkedIn: Or Cohen
- We! Consulting Group:
  - Web Site: http://en.we-can.co.il/
  - Web Site: http://www.wemeansecurity.com/
  - Phone: +972-09-9718222
  - LinkedIn: We! Consulting Group

- Contact us for updates or if you need any assistance.