Gaining Log Visibility in ICS Environments

Michael Hoffman
Principle ICS Security Engineer, Shell
CISSP, GSTRT, GICSP, GCIP, GCIH, GCIA, GPYC, GSEC, CEH, CCNA, MCSA
SANS Technology Institute, MSISE Candidate
Definitions & Cautionary Note

The companies in which Royal Dutch Shell plc directly and indirectly owns investments are separate legal entities. In this presentation “Shell”, “Shell group” and “Royal Dutch Shell” are sometimes used for convenience where references are made to Royal Dutch Shell plc and its subsidiaries in general. Likewise, the words “we”, “us” and “our” are also used to refer to Royal Dutch Shell plc and its subsidiaries in general or to those who work for them. These terms are also used where no useful purpose is served by identifying the particular entity or entities. “Subsidiaries”, “Shell subsidiaries” and “Shell companies” as used in this presentation refer to entities over which Royal Dutch Shell plc either directly or indirectly has control. Entities and unincorporated arrangements over which Shell has joint control are generally referred to as “joint ventures” and “joint operations”, respectively. Entities over which Shell has significant influence but neither control nor joint control are referred to as “associates”. The term “Shell interest” is used for convenience to indicate the direct and/or indirect ownership interest held by Shell in an entity or unincorporated joint arrangement, after exclusion of all third-party interest.

This presentation contains forward-looking statements (within the meaning of the U.S. Private Securities Litigation Reform Act of 1995) concerning the financial condition, results of operations and businesses of Royal Dutch Shell. All statements other than statements of historical fact are, or may be deemed to be, forward-looking statements. Forward-looking statements are statements of future expectations that are based on management’s current expectations and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in these statements. Forward-looking statements include, among other things, statements concerning the potential exposure of Royal Dutch Shell to market risks and statements expressing management’s expectations, beliefs, estimates, forecasts, projections and assumptions. These forward-looking statements are identified by their use of terms and phrases such as “aim”, “ambition”, “anticipate”, “believe”, “could”, “estimate”, “expect”, “goals”, “intend”, “may”, “objectives”, “outlook”, “plan”, “probably”, “project”, “risks”, “schedule”, “seek”, “should”, “target”, “will” and similar terms and phrases. There are a number of factors that could affect the future operations of Royal Dutch Shell and could cause those results to differ materially from those expressed in the forward-looking statements included in this presentation, including (without limitation): (a) price fluctuations in crude oil and natural gas; (b) changes in demand for Shell’s products; (c) currency fluctuations; (d) drilling and production results; (e) reserves estimates; (f) level of market share and industry competition; (g) environmental and physical risks; (h) risks associated with the identification of suitable potential acquisition properties and targets, and successful negotiation and completion of such transactions; (i) the risk of doing business in developing countries and countries subject to international sanctions; (j) legislative, fiscal and regulatory developments including regulatory measures addressing climate change; (k) economic and financial market conditions in various countries and regions; (l) political risks, including the risks of expropriation and renegotiation of the terms of contracts with governmental entities, delays or advancements in the approval of projects and delays in the reimbursement for shared costs; and (m) changes in trading conditions. No assurance is provided that future dividend payments will match or exceed previous dividend payments. All forward-looking statements contained in this presentation are expressly qualified in their entirety by the cautionary statements contained or referred to in this section. Readers should not place undue reliance on forward-looking statements. Additional risk factors that may affect future results are contained in Royal Dutch Shell’s Form 20-F for the year ended December 31, 2017 (available at www.shell.com/investor and www.sec.gov). These risk factors also expressly qualify all forward-looking statements contained in this presentation and should be considered by the reader. Each forward-looking statement speaks only as of the date of this presentation, March 19, 2019. Neither Royal Dutch Shell plc nor any of its subsidiaries undertake any obligation to publicly update or revise any forward-looking statement as a result of new information, future events or other information. In light of these risks, results could differ materially from those stated, implied or inferred from the forward-looking statements contained in this presentation.

We may have used certain terms, such as resources, in this presentation that the United States Securities and Exchange Commission (SEC) strictly prohibits us from including in our filings with the SEC. U.S. Investors are urged to consider closely the disclosure in our Form 20-F, File No 1-32575, available on the SEC website www.sec.gov.

Copyright of Shell International B.V. March 2019
ICS Logging Solution - Case for Improvement

- Performing Proof of Concept with a Network Security Monitoring (NSM) solution in a refinery
- Noticed a distinct pattern after analyzing network traffic from the ICS core switch
ICS Logging Solution - Case for Improvement Cont.

- Traffic attributed to a log collection server pulling 230 ICS Windows endpoints every 15 min
- Caused congestion in parts of the network
- Similar configurations in upstream ICS environments caused considerable bandwidth issues
ICS Logging Solution Constraints

- Lack of available bandwidth in older ICS LAN networks
- Remote locations with communication over VSAT, Cell, 900MZ, etc
- ICS Vendor software restrictions that limit installation of third-party or “un-approved” software
- Owners and operators struggling to maintain supported operating systems
- Deployment constraints with remote systems, maintenance windows, “no reboots”
- Limited “best practices” available for asset owners and operators to use
Primary ICS Logs

Syslog:
- ICS devices: PLC, RTUs IED, Analyzers, etc.
- Network equipment: Switches, Routers, Firewalls, Protocol Converters, etc.
- *nix operating systems: Linux, Unix, VMware

Windows Event Logs:
- WMI with DCOM Pulling
- Windows Event Forwarding
- Agent based: Splunk, QRadar, SolarWinds, etc.
Primary ICS Logs

Syslog:
- ICS devices: PLC, RTUs IED, Analyzers, etc.
- Network equipment: Switches, Routers, Firewalls, Protocol Converters, etc.
- *nix operating systems: Linux, Unix, VMware

Windows Event Logs:
- WMI with DCOM Pulling
- Windows Event Forwarding
- Agent based: Splunk, QRadar, SolarWinds, etc.
Gaining Endpoint Log Visibility in ICS Environments

GIAC Gold Certification

Author: Michael Hoffman, mhoffman89@gmail.com
Adviser: Randy Marchany

Accepted: 2/18/19

Abstract

Security event logging is a base IT security practice and is referenced in Industrial Control Security (ICS) standards and best practices. Although there are many techniques and tools available to gather event logs and provide visibility to SOC analysis in the IT realm, there are limited resources available that discuss this topic specifically within the context of the ICS industry. As many in the ICS community struggle with gaining logging visibility in their environments and understanding collection methodologies, logging implementation guidance is further needed to address this concern. Logging methods used in ICS, such as WMI, Syslog, and Windows Event Forwarding (WEF), are common to the IT industry. This paper examines WEF in the context of Windows ICS environments to determine if WEF is better suited for ICS environments than WMI polling regarding bandwidth, security, and deployment considerations. The comparison between the two logging methods is made in an ICS lab representing automation equipment commonly found in energy facilities.
Research ICS Lab Setup

- ICS Lab used for control systems integration and testing
- 40 Windows Hosts used in WMI vs. WEF pulling research
- NSM had visibility of 32 out of the 40 hosts due to placement and virtualized hosts
Research ICS Logging Preparation

■ Needed a consistent log policy baseline
■ Leveraged SANS ICS410 for Local Policies
■ Referenced Australian Cyber Security Center recommendations for Advanced Audit Policy settings
■ Deployed a Windows Security Logging GPO across the environment for Local Policies and Advanced Audit Policies

* Advanced Audit Policies can be viewed in the STI MSISE Whitepaper:
Define Logging Use Cases

- We expect to “Drink from the firehose” at SANS training
- However, aggressive security logging settings can deluge your end points, networks, SIEM platforms, and SOC teams
- The Blue Team Handbook by Don Murdoch is an exceptional reference for developing use cases mapped to data sources
WMI Pulling

- Client Server architecture
- WMI is the mechanism for Windows Event Logs access
- Leverages DCOM as the protocol across the network
- Server requests logs over a pre-determined frequency
WMI Pulling Considerations

- Helps to have one domain for consistent and distributed configuration. However, the same local account/password can be utilized in Workgroups or across Domains. To configure in a domain, the restricted WMI service account is linked to the Event Log Readers and DCOM Users group by Group Policy Preferences in a GPO.
- WMI security settings cannot be modified with a GPO.
- Don’t use a Domain Admin level account for the WMI service account!
WMI Statistics over 6 days of testing

- Leveraged Splunk Enterprise Trial version as WMI pulling source
- Sum of bandwidth for 32 hosts was 17GB
- Consistent TCP connection counts
- Packet size varied significantly over the top 10 hosts
Windows Event Forwarding Overview

- Bleeding edge
- “Easy” to deploy in a Windows Domain. You have to understand Domains, GPOs, and OS…
- Deploy in workgroup or across domain settings with certificates
- Uses Kerberos for authentication and encrypts traffic by default
- Push or Pull configuration options for the Widows Event Collector
- Create multiple subscriptions for different use cases
- Chain WEC servers together into a log hierarchy
Windows Event Forwarding Overview

- Bleeding edge – it's been out since 2008 😁
- "Easy" to deploy in a Windows Domain. You have to understand Domains, GPOs, and OS…
- Deploy in workgroup or across domain settings with certificates
- Uses Kerberos for authentication and encrypts traffic by default
- Push or Pull configuration options for the Windows Event Collector
- Create multiple subscriptions for different use cases
- Chain WEC servers together into a log hierarchy
High Level WEF Setup

- Enable the WinRM service (winrm -qc)
- Enable the WEC service on the server
- Create GPO to point hosts to the WEC Server (contains settings for WinRM, Collector, Security, etc.)
- Create subscription(s)
- Configure forwarding to higher level WEC Server, an OT or IT/OT SIEM
High Level WEF Setup

- Enable the WinRM service (winrm –qc)
- Enable the WEC service on the server
- Create GPO to point hosts to the WEC Server
  (contains settings for WinRM, Collector, Security, etc.)
- Create subscription(s)
- Configure forwarding to higher level WEC Server, an OT or IT/OT SIEM
WEC Subscription Settings

Subscription Properties - Forwarded Events
- Subscription name: Forwarded Events
- Description: Forwarded Security Events
- Destination log: Forwarded Events
- Subscription type and source computers:
  - Source computer initiated
- Events to collect:
- Configure advanced settings:

Copyright of Shell International B.V.
WEC Subscription Settings

Subscription Properties
- Subscription name: Forwarded Events
- Description: Forwarded Security Events
- Destination log: Forwarded Events
- Source computer initiated

Select Computer Groups...

Computer Groups
- \Domain Computers: Included
- \Domain Controllers: Included

Select the certification authorities to be used to authenticate non-domain computers:
- Issued To
- Issued By
- Expiration Date

Add Certificates...
WEC Subscription Settings

Subscription Properties

- Subscription name: Forwarded Events
- Description: Forwarded Security Events
- Destination log: Forwarded Events

Subscription type and source computers

- Source computer initiated: Select Computer Groups
- Events to collect: Select Events
- Configure advanced settings: Advanced

Query Filter

- Logged: Last 24 hours
- Event level: Critical, Warning, Verbose, Error, Information
- By log: Event logs: Security
- By source: Event sources: <All Event IDs>
- Task category:
- Keywords:
- User: <All Users>
- Computer(s): <All Computers>

Advanced Subscription Settings

- Event Delivery Optimization:
  - Normal
  - Minimize Bandwidth
  - Minimize Latency
  - Custom
- Protocol: HTTP
WEF with Push

Logs are forwarded to the WEC server per subscription settings:

- **Normal**: 5 log batch with 15 Batch minute timeout
- **Min Bandwidth**: Batch timeout of 6 hours
- **Min Latency**: Batch timeout of 30 seconds
WEF Statistics Over 6 Days of Testing

- WEC subscription was set to Normal, with 40 hosts forwarding logs
- Sum of bandwidth for 32 hosts (visible to the NSM) was 10GB ~ 40% reduction from WMI
- Inconsistent TCP connection counts
- Packet size is relatively consistent over the top10 hosts
Recommendations

- Review your security tooling and its affect to your ICS environment
- Utilize WEF for Windows client and server operating systems that support WinRM
  - Configure WEF push method with subscriptions targeted for domain computers and servers
  - Modify WEC subscription latency settings for the environment
- Optimize WEC subscription event filtering to support use-cases mapped to Cyberdefense activities and active defense programs in the ICS