Seeing Clearly and Communicating Effectively to Address Event Overload

Thomas V Fischer
FVT SecOps Consulting
I am ...

• Security Advocate & Threat Researcher focused on Data Protection
• 25+ years' experience in InfoSec
• Spent number years in corporate IR team positions

• BSidesLondon Director
• ISSA UK – VP of Data Governance

• Contact
  • tvfischer+sec@gmail.com tvfischer@tvf-prod.com (secure email)
  • @Fvt
  • keybase.io/fvt
Learning from 1st Responder Lessons Learnt

➢ Communications issues
➢ Self dispatching & recall
➢ Lack of accountability
➢ Unclear chain of command
➢ Uncertain roles/task assignments

Thanks to Chris Sutherland (ING) for these references
Communication Issues

- Unclear if units received dispatch instructions
- Portable radio limitations
- 10 different Call Codes
- Lack of situational awareness
- Structural collapse
- Many firefighters and officers in tower 1 unaware of tower 2 collapse
Visualization enables an analyst to gain an overview of data during an investigation.

Schrenk and Poisel, 2011
Printed 4 pages.

jsarmiento printed 4 pages in an hour, a significantly larger number of pages compared to others. People typically print 1 page per hour, and at most 1 page.
• Matching IOC
• Signature Based

• Security/Hunting Analytics
• Stats Methods
• Start of UEBA

• Supervised machine learning
• Incorporate previous signals

Thanks to Alex Pinto
<table>
<thead>
<tr>
<th>Commonly Used Port</th>
<th>Expense Access</th>
<th>Execution</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Through Removable Media</td>
<td>Accessibility Features, Binary Padding, Accessibility Features</td>
<td>Application Window Discovery, Bash History</td>
<td>Application Deployment Software, Automated Collection</td>
<td>Audio Capture, Data Compressed</td>
<td>Automated Exfiltration, Data Compressed</td>
<td>Background Infiltration Service</td>
</tr>
<tr>
<td>Connection Proxy</td>
<td>Appinit DLLs, Bypass User Account Control, Appinit DLLs</td>
<td>File and Directory Discovery, Brute Force</td>
<td>Command-Lite Interface, Exploitation of Vulnerability</td>
<td>Clipboard Data, Data Encrypted</td>
<td>Data Transfer Size Limits</td>
<td>Hafnium</td>
</tr>
<tr>
<td>Custom Command and Control Protocol</td>
<td>Application Shimming, Dear Command History, Application Shimming</td>
<td>Network Service Scanning, Create Account</td>
<td>Execution through API, Logon Scripts</td>
<td>Data Staged</td>
<td>Data Staged, Data Transfer Size Limits</td>
<td>Hafnium</td>
</tr>
<tr>
<td>Custom Cryptographic Protocol</td>
<td>Authentication Package, Code Signing, Bypass User Account Control</td>
<td>Network Share Discovery, Credential Dumping</td>
<td>Execution through Module Load, Past the Hash</td>
<td>Data from Local System, Exfiltration Over Alternative Protocol</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Exfiltration Over Command and Control Channel</td>
</tr>
<tr>
<td>Data Encoding</td>
<td>Bootkit, Component Firmware, DLL Injection</td>
<td>Peripheral Device Discovery, Credentials in Files</td>
<td>Graphical User Interface, Past the Ticket</td>
<td>Data from Network Shared Drive, Exfiltration Over Command and Control Channel</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Exfiltration Over Command and Control Channel</td>
</tr>
<tr>
<td>Data Obfuscation</td>
<td>Change Default File Association, Component Object Model Hijacking</td>
<td>DLL Search Order Hijacking, DLL Search Order Hijacking</td>
<td>Permission Groups Discovery, Exploitation of Vulnerability</td>
<td>InstallUtil, Remote Desktop Protocol</td>
<td>Data from Removable Media, Exfiltration Over Other Network Medium</td>
<td>Exfiltration Over Other Network Medium</td>
</tr>
<tr>
<td>Fallback Channels</td>
<td>Component Firmware, DLL Injection, Dylib Hijacking</td>
<td>Process Discovery, Input Capture</td>
<td>Launchctl, Remote File Copy</td>
<td>Email Collection, Exfiltration Over Physical Medium</td>
<td>Exfiltration Over Physical Medium</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td>Multi-Stage Channels</td>
<td>Component Object Model Hijacking, DLL Search Order Hijacking</td>
<td>Exploitation of Vulnerability, Query Registry</td>
<td>Input Prompt, PowerShell</td>
<td>Remote Services, Input Capture</td>
<td>Scheduled Transfer</td>
<td>Scheduled Transfer</td>
</tr>
<tr>
<td>Multiband Communication</td>
<td>Cron Job, DLL Side-Loading</td>
<td>File System Permissions Weakness, Remote System Discovery</td>
<td>Keychain, Process Hollowing, Application Through Removable Media</td>
<td>Screen Capture</td>
<td>Screen Capture</td>
<td>Screen Capture</td>
</tr>
<tr>
<td>Multilayer Encryption</td>
<td>DLL Search Order Hijacking, Doobfuscate/Decode Files or Information</td>
<td>Launch Daemon, Security Software Discovery</td>
<td>Network Sniffing, RegRaku/Regasm</td>
<td>Shared Webroot, Video Capture</td>
<td>Video Capture</td>
<td>Video Capture</td>
</tr>
<tr>
<td>Incommonly Used Port</td>
<td>Hypervisor, Gatekeeper Bypass</td>
<td>Gatekeeper Bypass, Gatekeeper Bypass</td>
<td>Gatekeeper Bypass, Gatekeeper Bypass</td>
<td>Gatekeeper Bypass, Gatekeeper Bypass</td>
<td>Gatekeeper Bypass, Gatekeeper Bypass</td>
<td>Gatekeeper Bypass, Gatekeeper Bypass</td>
</tr>
</tbody>
</table>
Orientation by Framework – Does it Help?

- **Reconnaissance** → **Weaponization** → **Delivery** → **Exploitation** → **C2** → **Exfiltration**

- **Acquire**
  - **Recon Inside**
  - **Escalation**
  - **Obtain Creds**
  - **Move Laterally**

- **Maintain**
  - **Stage Data** → **Exfil Data** → **Hide Footprints**

- **MITRE**

- **Acquired?**
  - **Y**
  - **N**

- **MITRE Framework**
  - **Recon**
  - **Weaponize**
  - **Deliver**
  - **Exploit**
  - **Control**
  - **Maintain**
  - **Privilege Escalation**
  - **Defense Evasion**
  - **Credential Access**
  - **Discovery**
  - **Lateral Movement**
  - **Execution**
  - **Collection**
  - **Exfiltration**
  - **Command and Control**
Key Phases in the Monitoring Process

- Collect relevant event data
- Fuse events together
- Analyse anomalous events
- Take appropriate action

Cyber Security Monitoring and Logging Guide
iz not stalking... just intently staring
“Sharp and original, this book should alter how readers look at the world.”

—KIRKUS

VISUAL INTELLIGENCE

SHARPEN YOUR PERCEPTION,
CHANGE YOUR LIFE

Amy E. Herman
Portrait by Kumi Yamashita
What is this Work of Art?

• Is it a painting?
• Is it a sculpture?
• What is it made of?
Learning to frame the question to elicit the information to do our jobs
The 4 A’s

We find only the world we look for.

Henry David Thoreau

Amy Herman, *The Art of Perception*
Something Gets Lost

- Effective break down between what we see down to what we communicate
- Ability to translate what we see to others
- Talk about complicated situations to simple situations
- Everything in between
What is in Front of Us

Study Thoroughly

saper vedere
No Two People See the Same Way
“Luncheon on the Grass” by Manet 1863
Count how many times the players wearing white pass the ball.
The Monkey Business Illusion

- So what was the answer? 16
What is important?

What do I need?

What don’t I need?

Analyse the elements observed

Inattentional blindness
Articulate the facts succinctly
Remove assumptions
Also what don't you see

Assumptions
Danger! Danger!

Explain what you have seen and communicate it
Adapt

Formulate questions to address the seeming inconsistencies

Observations inform perceptions and perceptions inform inferences

Step back take another look
Take an Action Based on What we See and Communicate
Did you see ... Renshaw’s Cow
Summarise the picture

But what did you leave out?

René Magritte Time Transfixed
Giuseppe Arcimboldo - The Vegetable Gardener
Do you want to send more information about the problem?

Additional details about what went wrong can help Microsoft create a solution.

View Details  Send information  Cancel
An important message regarding your E*TRADE account is waiting for your attention

Thomas Fischer:
Your stock options are awaiting verification. Please review the attached statement.

If you have any questions or concerns, please don’t hesitate to contact us at 1-800-E*TRADE-1 (1-800-387-2331)

between 7a.m. and midnight ET, seven days a week.

We appreciate the opportunity to continue to serve you and your investing needs.

-RJ Lilen
President, COO and Director, E*TRADE Financial

Do you want to send more information about the problem?

Additional details about what went wrong can help Microsoft create a solution.

View Details  Send information  Cancel
Contextual or Situational Awareness
Where are you now?

How do you proceed?

Are you comfortable about what you are seeing?

What else is around you?

What are the problems I am aware of?
Choice of words in both spoken and written language is important
Present Your Ideas

• In a way your reader can understand and build a picture

• Lead with the key fact, to
  • Seed your findings
  • Build a clear summary

• Begin with an action verb

• Highlight the impact
Keep it Succinct

• Write a sentence
• Re-evaluate it
• Shorten it
• Get to the point faster
Be Precise

• Remove
  • Clutter
  • Assumptions
  • unnecessary/irrelevant details
• Highlight the important information
In Conclusion

Understand how you come across both figuratively and literally!

There are things you are seeing that are right in front of your eyes...

Have you gone back and told your colleagues, and re-evaluated how did I miss that?

It was right there?
In Conclusion
Collaborate

Here is my issue, here is my problem.

Is there something that I might be missing?

Do you know something that I don’t
In Conclusion

Don’t reach for what you want to see

Be accountable for your observations

Jump to a conclusion; document how you get there
“If you change the way you look at things, the things you look at change”

Dr. Wayne Dyer

@Fvt
› tvfischer+sec@gmail.com  tvfischer@tvf-prod.com (secure)
› keybase.io/fvt