AI in Cybersecurity - Should we trust the machines

Paul Hogan CRISC, CGEIT, CISA
Ward Solutions
pioneering, machine-learning technology capable of detecting and fighting back against stealthy ‘unknown unknowns’, such as WannaCry, automatically and in real time.

WannaCry
Ransomware Attack

By leveraging machine learning and artificial intelligence to predict malicious code pre-execution without relying on a signature, heuristic ruleset, cloud connection, or any of the methods used by traditional antivirus products.
Artificial Intelligence and Machine Learning

The answer to Cybersecurity Challenges?
Dave: Open the pod bay doors, please HAL.

HAL: I'm sorry Dave. I'm afraid I can't do that
HAL: This mission is too important for me to allow you to jeopardize it.
**Artificial Intelligence**
Behavior and reason based, Human intelligence exhibited by machines. Ability to improve based on understanding.

**Machine Learning**
Prediction using models, draw interference and make predictions based on data without explicit programming.

**Deep Learning**
Multiple layers, artificial neural networks
Challenges in Cybersecurity

- Skills shortage analysts
- Knowledge and knowhow shortage
- 93% of SOC managers cannot triage all potential threats
- 71% of SOCs with a level 4 maturity closed incident investigations in less than a week

INTELLIGENCE  SPEED  ACCURACY
ASSESS
Identifying, risks and threats, determining and improving your security posture

PROTECT
Implementing technologies and controls to protect critical assets and stop advanced threats

DETECT
Detecting security vulnerabilities and incidents that are in your organisation right now.

RESPOND
Determining the impact, and responding and recovering from security incidents

Risk Assessment
Audit
Vulnerability Assessment
Firewall
SIEM
EDR
S-IRP
Endpoint
IPS
Threat
Anomalies are events that haven't been seen previously.

“.But there are also unknown unknowns – the ones we don't know we don't know.”
Cognitive Security – increase accuracy, reducing average incident detect, response and resolution times

Threat Detection
Predictive Defence
Windows Logon

- Create a context and model around that
- Consider the different user account types
  - Users, administrators, machine accounts, service accounts
- Consider type of logon
  - Physical, Network, Remote, Terminal
- Consider time
- Create clusters.
- Anomalies fall outside these clusters
Windows Logon

- End users
- Administrators
- VPN Users
Windows Logon

- No ‘grand’ truth, cannot say for certain what is happening, probabilistic not deterministic.
- Validate date, use feedback, iterate and improve.
- Need a corpus of data.
- We still need experts.
Increased Complexity

1. Large amounts of data from multiple sources.
2. Distributed Attack Surface.
3. Complex environments.
4. Multiple Vectors.
Increased Complexity

1. User VPN access.
2. User logs onto a machine.
3. Initiates a connection to a database.
4. Performs an extract as CSV.
5. Copies to local machine.
6. Creates Excel File
7. Copies to cloud service.
Day in the Life of an Analyst

1. Console delivers a range of incidents.
2. Search locally, determine context and formulate strategy for threat research.
3. Use threat intelligence feeds to learn about indicators of compromise (IOC) associated with the incident.
4. Investigate IOCs to qualify the incident.
### Current Search Parameters:

- Exclude Hidden Offenses (Clear Filter)
- Exclude Closed Offenses (Clear Filter)

<table>
<thead>
<tr>
<th>Id</th>
<th>Description</th>
<th>Offense Type</th>
<th>Offense Source</th>
<th>Magnitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>240</td>
<td>TCP_HIT preceded by System Infected: Ransomware Activity</td>
<td>Source IP</td>
<td>192.168.0.119</td>
<td></td>
</tr>
<tr>
<td>237</td>
<td>TCP_HIT preceded by System Infected: Backdoor DarkMoon Activity</td>
<td>Source IP</td>
<td>192.168.0.235</td>
<td></td>
</tr>
<tr>
<td>243</td>
<td>virus_found-unknown_action preceded by TCP_HIT preceded by ...</td>
<td>Username</td>
<td>tom_wilson</td>
<td></td>
</tr>
<tr>
<td>244</td>
<td>TCP_HIT preceded by TCP_MISS preceded by System Infected: ...</td>
<td>Username</td>
<td>lance.springwell</td>
<td></td>
</tr>
</tbody>
</table>
### Offense 237

**Magnitude**
- TCP_HIT

**Description**
- System infected: Backdoor DarkMoon Activity preceded by Web Attack: Suspicious Executable File Download

**Source IP(s)**
- 192.168.0.235

**Destination IP(s)**
- 10.64.2.200, 147.188.76.90

**Network(s)**
- Multiple (2)

**Offense Source Summary**

<table>
<thead>
<tr>
<th>IP</th>
<th>192.168.0.235</th>
<th>Location</th>
<th>Net-10-172-192.192.168.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnitude</td>
<td></td>
<td>Vulnerabilities</td>
<td>0</td>
</tr>
<tr>
<td>Username</td>
<td>Unknown</td>
<td>MAC Address</td>
<td>Unknown NIC</td>
</tr>
<tr>
<td>Host Name</td>
<td>Unknown</td>
<td>Weight</td>
<td>0</td>
</tr>
<tr>
<td>Asset Name</td>
<td>Unknown</td>
<td>Events/Flows</td>
<td>116</td>
</tr>
<tr>
<td>Offenses</td>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Last 5 Notes**

<table>
<thead>
<tr>
<th>Notes</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TCP_HIT preceded by System Infected: Backdoor DarkMoon Activity preceded by Web Attack: Suspicious Executable...

Source Details:
- Source IP: 192.168.0.235
- Description: TCP_HIT preceded by System Infected: Backdoor DarkMoon Activity preceded by Web Attack: Suspicious Executable File Download
- Location: Other, Server_Network, Server_Network
- Assigned To: Watson

Watson Insights:
"QRadar Advisor has not investigated this incident."

Investigate this incident.
Incident 237
TCP_HIT preceded by System Infected: Backdoor DarkMoon Activity preceded by Web Attack: Suspicious Executable...

Overview

Incident Type
Source IP
Categories
Trojan Detected, Backdoor Detected, Object Cached, Misc Network Communication Event, Object Not Cached, Suspicious Activity, User Behavior

Created
7 days ago

Source Details

Source IP
192.168.0.235
Description
TCP_HIT preceded by System Infected: Backdoor DarkMoon Activity preceded by Web Attack: Suspicious Executable File Download
Location
other, Server_Network, Server_Network
Assigned To

Watson Insights

“QRadar Advisor has analyzed this offense and a total of 14 observables. Reasoning over the offense discovered ten new indicators that were not part of the offense. A total of eight data points have been found to be linked with the offense. Two of all of the indicators are known to be related with suspicious activity, all of them have been observed actively in this offense. In particular, two files have been found, which are known to be suspicious or malicious.”
TCP_HIT preceded by System Infected: Backdoor DarkMoon Activity preceded by Web Attack: Suspicious Executable...

Watson Insights

"QRadar Advisor has analyzed this offense and a total of 14 observables. Reasoning over the offense discovered ten new indicators that were not part of the offense. A total of eight data points have been found to be linked with the offense. Two of all of the indicators are known to be related with suspicious activity, all of them have been observed actively in this offense. In particular, two files have been found, which are known to be suspicious or malicious."

Supporting Details

- Reputation (21%)
- Filename (21%)
- Hash (14%)
- Ip Address (14%)
- Url (14%)
Watson Advisor assisted threat analysis

Quick and accurate analysis of security threats, saving precious time and resources

- Accelerates incident triage with more automation
- Alleviates pressure of skills gap
- Augments contributions of security teams
- Empowers security analysts in clearing backlog

Manual threat analysis

Triage  Investigate & Impact Assessment  Remediation

Days to Weeks

Minutes to Hours

Manual threat analysis:

- Triage
- Investigate & Impact Assessment
- Remediation

Watson Advisor assisted threat analysis:

- Triage
- Investigate & Impact assessment
- Remediation

Quick and accurate analysis of security threats, saving precious time and resources

- Accelerates incident triage with more automation
- Alleviates pressure of skills gap
- Augments contributions of security teams
- Empowers security analysts in clearing backlog
Dark Side of AI

- Advanced Phishing Attacks
- Autonomous malware
- Vulnerability Scanning
Summary

The correct application of machine learning (AI) promises exciting new opportunities for Cybersecurity, enhancing protection and improving the speed and accuracy of detect and respond. There may be greater challenges ahead, but in the meantime we need to be aware of and recognise marketing hype.