CSIRT Schiltron: Training, Techniques, and Talent

Jeff Bollinger
James Sheppard
(Cisco CSIRT)
(1314) Robert the Bruce positioned his army in the New Park with Randolph’s schiltron to the fore and his own immediately behind it. The chosen **method** of combat was for each schiltron to form a **bristling mass of spears** which the English knights would be **unable to penetrate**.

The Scots dug **concealed pits** across the front of their position and along the bank of the Bannockburn to break up any mounted charge against them.
How can an incident response teams enable **readiness** and improve **capabilities** with evolving threat profiles that require new approaches and new skillsets?
• Mail and **phishing** messages have become the primary malware infection vector;
• **Cryptominers** have become an important monetization vector for cyber criminals;
• State-sponsored agents increasingly target banks by using **attack-vectors** utilized in cyber crime;
• The emergence of **IoT environments** will remain a concern due to missing protection mechanisms...
• Cyber **threat intelligence** needs to respond to increasingly automated attacks...
• **Skills and training are the main focus of defenders.**

**PRESS RELEASE**

Exposure to cyber-attacks in the EU remains high - New ENISA Threat Landscape report analyses the latest cyber threats

In 2018, the cyber threat landscape changed significantly. The most important threat agent groups, namely cyber-criminals and state-sponsored actors have further advanced their motives and tactics. Monetisation motives contributed to the appearance of crypto-miners in the top 15 cyber threats.

Published on January 28, 2019
We Value Learning & Development

SANS Courses
Cisco L&D
Conferences
CTFs
Tabletops
Purple Team
We Needed More

- Training based on real cases and real data.
- Useful to newbies and veterans alike.
- Tailored challenges unique to the IR role.
- Teaching on incidents with similar characteristics and techniques.
- Fostering collaboration, camaraderie, and trust.
Team Training Goals

- Security 101
- Case Work
- Data Sources
- Internal Tools
Security 101

- New analysts typically arrive with some domain knowledge
- System and networking basics are crucial to daily work and understanding
- Develops better “hacker mindset” – builds on curiosity
- Evaluates efficacy/comprehension of commercial training programs
Casework

- Pairing operational/technical knowledge with practical security comprehension
- Helps to maintain consistency in response
- Introduces useful tricks/tips that senior teammates have used over the years
- Drawn from real incidents to allow replaying a part of an investigation
Data Sources

- We’re a data-centric team that makes decisions based on evidence in the available data.
- Understanding how to effectively search all the available data sources can take time.
- Knowing what data is available and what questions can be answered delivers better analysis and results.
Internal Tools

• Tools get built over the years and often forgotten.
• The time to learn how to use tools is not during an incident.
• Having practice and understanding how to use features saves time and minimizes delays.
Why a Blue Team CTF?

- Certifications and professional training organizations teach security/technology skills – not operations/SOP
- We can tailor the training content to our team goals
- Hands-on training / terminal time
- Several audits (ex. ISO27001) require annual training programs
- People are familiar with the CTF format
- Gamification* removes the dread of boring training/testing/drilling
- Cost – FOSS. Only need a small server and to develop your own training content
Blue Team CTF

- Must fit the training goals
- Fun
- Interesting interface
- Easy to run/support
- Decent scoring/teaming interface

https://github.com/facebook/fbctf
- 4 Hours
- 30 Participants
- All branches of CSIRT
- 8 Randomly selected teams
- 4 Different Sites
- 49 Flags/Quizzes
- 100+ Tacos
## Prizes!

<table>
<thead>
<tr>
<th>filter_</th>
<th>rank_</th>
<th>team_name_</th>
<th>quiz_pts_</th>
<th>flag_pts_</th>
<th>base_pts_</th>
<th>total_pts_</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>SUPER FLY</td>
<td>255</td>
<td>1220</td>
<td>0</td>
<td>1425</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>KEWL BRAHS</td>
<td>135</td>
<td>1005</td>
<td>0</td>
<td>1031</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>GIGACHADS</td>
<td>85</td>
<td>955</td>
<td>0</td>
<td>999</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>ETERNAL BLU</td>
<td>285</td>
<td>760</td>
<td>0</td>
<td>960</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>TLDR</td>
<td>180</td>
<td>820</td>
<td>0</td>
<td>945</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>IS THIS A FLAG?</td>
<td>200</td>
<td>740</td>
<td>0</td>
<td>940</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>D.E.A.D.</td>
<td>145</td>
<td>685</td>
<td>0</td>
<td>805</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>JE NE SAIS PAS</td>
<td>105</td>
<td>575</td>
<td>0</td>
<td>665</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>QUESTION</td>
<td>HINT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security 101</td>
<td>What networking technique prevented Wannacry from encrypting its victims?</td>
<td>The same technique our DNS RPZ can use...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Security 101

<table>
<thead>
<tr>
<th>FLAG</th>
<th>TESTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sinkhole</td>
<td>How [part of] Wannacry worked</td>
</tr>
<tr>
<td></td>
<td>Common terminology used in takedowns and security research</td>
</tr>
<tr>
<td></td>
<td>Basic understanding of our DNS Response Policy Zone features</td>
</tr>
</tbody>
</table>

### Case Work

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>QUESTION</th>
<th>HINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Work</td>
<td>How many cases have been opened that have references in the case notes to MAC addresses created by “Universal Global Scientific Industrial Co.”?</td>
<td>note:&quot;00:10:C6:*&quot; OR ...</td>
</tr>
</tbody>
</table>
**Case Work**

<table>
<thead>
<tr>
<th>FLAG</th>
<th>TESTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>513</td>
<td></td>
</tr>
</tbody>
</table>
|      | Basic case repository searching  
|      | Case details and typical metadata captured  
<p>|      | Knowledge of MAC Address organizationally unique identifier (OUIs) |</p>
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>QUESTION</th>
<th>HINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Work</td>
<td>Which server (hostname) hosted in the UK triggered the play described in bug 12161?</td>
<td>playbook_id=610002</td>
</tr>
</tbody>
</table>
Case Work

<table>
<thead>
<tr>
<th>FLAG</th>
<th>TESTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SRV-GPK12-RS-T</strong></td>
<td>- Basic case repository searching</td>
</tr>
<tr>
<td></td>
<td>- Connection between Incidents and CSIRT Playbook</td>
</tr>
<tr>
<td></td>
<td>- Knowledge of internal host naming</td>
</tr>
<tr>
<td></td>
<td>- Experience finding playbooks and detection methods.</td>
</tr>
</tbody>
</table>

Hostname of only 1 of the 9 results matches the right Cisco site code/naming convention.
# Data Sources

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>QUESTION</th>
<th>HINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Sources</td>
<td>What is the most common event name in our AWS data?</td>
<td>index=aws</td>
</tr>
</tbody>
</table>
## Data Sources

<table>
<thead>
<tr>
<th>FLAG</th>
<th>TESTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthorizeSecurity</td>
<td>Splunk search/stats</td>
</tr>
<tr>
<td>GroupIngress</td>
<td>Type of AWS log events</td>
</tr>
<tr>
<td></td>
<td>Where to find AWS events</td>
</tr>
</tbody>
</table>

```
index=aws | stats count by eventName | sort -count

Your search is paused.  No Event Sampling
```

**Visualization**

- Pie Chart
- Format
- Trellis

**Event Name**
- AuthorizeSecurityGroupIngress
- DeleteObject
- LookupEvents
Find the Gaps

% Unanswered or Missed

- Security 101
- Casework
- Data Sources
- Internal Tools
The Biggest Win?

The social aspect – getting people to work together that typically don’t work together.
CSIRT Innovation Challenge

Improving Capabilities
CSIRT Innovation Challenge

An invitation to use your creativity, talents, and knowledge to improve security at Cisco

Three...
New challenges are regularly posted to the innovation hub/dashboard, each focusing on a specific area of IR.

Two...
CSIRT Individuals & teams use their creativity and talent to contribute “something” related to the challenge.

One...
Submissions are reviewed by a panel of stakeholders and the most impactful contribution wins a reward.
Cisco Global Problem Solver Challenge 2019

$300,000 in Prizes - Calling Students and Recent Grads

How can your innovative technology solution solve the world’s most pressing social and environmental problems?

View the Winners!
Oorja: Oonnati PAYG Community Solar Pumping Systems

Oorja deploys and operates PAYG Community Solar Pumping Systems to provide affordable pay-per-use irrigation services to smallholder farmers.

Solar Freeze

A one stop turnkey portable off-grid toolkit for localized rural food.

Calla Imaging

A patient-centric cervical cancer screening technology with mHealth communication, patient data storage and artificial intelligence capabilities.
Innovate Everywhere Challenge discovers the greatest ideas within Cisco

by Stephanie Chan  © June 07, 2017

Cisco's Innovate Everywhere Challenge asks employees to bring their most innovative ideas to the forefront. See the excitement from this year's finalist pitches.
Innovation Hub/Dashboard
Innovation Hub/Dashboard

Active/Inactive
• Is this challenge open for submissions?

Stakeholders
• Who sponsored this challenge?

Difficulty
• Corresponds to reward level

Expiration
• When does this challenge end?

Description
• What is the scope of the challenge?

Winner(s) + Solution
• Who won? Why? What did they submit?
Innovation Hub/Dashboard

Active/Inactive
• Is this challenge open for submissions?

Stakeholders
• Who sponsored this challenge?

Difficulty
• Corresponds to reward level

Expiration
• When does this challenge end?

Description
• What is the scope of the challenge?

Winner(s) + Solution
• Who won? Why? What did they submit?
Innovation Hub/Dashboard

CSIRT Innovation Challenge

- **Active/Inactive**
  - Is this challenge open for submissions?

- **Stakeholders**
  - Who sponsored this challenge?

- **Difficulty**
  - Correlates to reward level

- **Expiration**
  - When does this challenge end?

- **Description**
  - What is the scope of the challenge?

- **Winner(s) + Solution**
  - Who won? Why? What did they submit?
Innovation Hub/Dashboard

Active/Inactive
- Is this challenge open for submissions?

Stakeholders
- Who sponsored this challenge?

Difficulty
- Corresponds to reward level

Expiration
- When does this challenge end?

Description
- What is the scope of the challenge?

Winner(s) + Solution
- Who won? Why? What did they submit?
Innovation Hub/Dashboard

Active/Inactive
• Is this challenge open for submissions?

Stakeholders
• Who sponsored this challenge?

Difficulty
• Corresponds to reward level

Expiration
• When does this challenge end?

Description
• What is the scope of the challenge?

Winner(s) + Solution
• Who won? Why? What did they submit?
Innovation Hub/Dashboard

Active/Inactive
• Is this challenge open for submissions?

Stakeholders
• Who sponsored this challenge?

Difficulty
• Corresponds to reward level

Expiration
• When does this challenge end?

Description
• What is the scope of the challenge?

Winner(s) + Solution
• Who won? Why? What did they submit?
CSIRT Innovation Challenge

Winning contribution from the April 2019 Innovation Challenge

The Challenge
Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud IR efforts.

Impact 3...
Automated alerts & reporting directly to tenant owners.

Impact 2...
Provides additional visibility into our Cloud “API Footprint”.

Impact 1...
This contribution was a direct result of an incident.

Winning Solution
A novel detection technique for finding and alerting on API calls coming from unusual IP spaces (typically outside Cisco or AWS). Also includes proposal for proactive enumeration of ACLs attached to programmatic users.
Growing Cloud Presence
Overall Risk Score: A

Security Metrics

<table>
<thead>
<tr>
<th>Section</th>
<th>Section Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identity and Access Management</td>
<td>100/100</td>
</tr>
<tr>
<td>2. Network Security</td>
<td>90/100</td>
</tr>
<tr>
<td>3. Storage (S3 buckets)</td>
<td>100/100</td>
</tr>
<tr>
<td>4. Tagging</td>
<td>90/100</td>
</tr>
<tr>
<td>5. External Vulnerabilities</td>
<td>100/100</td>
</tr>
<tr>
<td>6. CIS AWS Benchmarks</td>
<td>100/100</td>
</tr>
<tr>
<td>7. Trusted Advisor Checks</td>
<td>Not Scored</td>
</tr>
</tbody>
</table>
CSIRT Innovation Challenge

Winning contribution from the April 2019 Innovation Challenge

The Challenge
Cisco’s Cloud presence continues to grow and so does our need for continuous security improvements in this environment. As a global team, let’s align ourselves to the common goal of improving the maturity of our Cloud IR efforts.

Winning Solution
A novel detection technique for finding and alerting on API calls coming from unusual IP spaces (typically outside Cisco or AWS). Also includes proposal for proactive enumeration of ACLs attached to programmatic users.

Impact 1...
This contribution was a direct result of an incident.

Impact 2...
Provides additional visibility into our Cloud “API Footprint”.

Impact 3...
Automated alerts & reporting directly to tenant owners.
Over a period of 90 days, there were **84,751,672** 'AwsApiCall' events originating from 1400+ AWS accounts, sourced from **3,155** different IP addresses. **353** of those IP addresses originate from outside Cisco and Amazon.
CSIRT Innovation Challenge

Winning contribution from the April 2019 Innovation Challenge

The Challenge
Cisco’s Cloud presence continues to grow and so does our need for continuous security improvements in this environment. As a global team, let’s align ourselves to the common goal of improving the maturity of our Cloud IR efforts.

Winning Solution
A novel detection technique for finding and alerting on API calls coming from unusual IP spaces (typically outside Cisco or AWS). Also includes proposal for proactive enumeration of ACLs attached to programmatic users.

Impact 1...
This contribution was a direct result of an incident.

Impact 2...
Provides additional visibility into our Cloud “API Footprint”.

Impact 3...
Automated alerts & reporting directly to tenant owners.
CSIRT Innovation Challenge

Here’s what we’ve learned from implementing and running the challenge

Three...
Motivating people is hard, and people are motivated by different things.

Two...
We have existing momentum we must overcome and this will take time.

One...
Ideas are (mostly) useless without execution.
INNOVATION

Just because something is innovative, doesn't mean it's a good idea.
How do you address the challenges of training & development?