Leveraging Open-Source Intelligence (OSINT)

How Social Footprints Lead to Cyber Risk

Chris Coryea | International Cyber Intelligence Services Manager
I have Defender DNA.

I am determined to continuously learn from the past. I leverage my relentless drive to understand the ever-evolving threat landscape and solve the continuous challenges waged by our cyber enemies.
400M users

1B posts/day

2.5 Exabytes data/day

500M tweets/day
1 Analyst / 5 Hours
Cybersecurity Footprint: Exposing your Strategy

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Location</th>
<th>Time Frame</th>
<th>Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Awareness</td>
<td>Middle East</td>
<td>1 year</td>
<td>£1.5M</td>
</tr>
<tr>
<td>Advanced Email Security</td>
<td>Global</td>
<td>1 year</td>
<td>N/A</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>United States</td>
<td>2 years</td>
<td>£4M</td>
</tr>
<tr>
<td>Endpoint Security</td>
<td>Global</td>
<td>1 year</td>
<td>£4M</td>
</tr>
<tr>
<td>Application Security</td>
<td>Global</td>
<td>3 years</td>
<td>£8M</td>
</tr>
<tr>
<td>SOC Transformation (20 staff)</td>
<td>London</td>
<td>2 years</td>
<td>£15M</td>
</tr>
<tr>
<td>Supply Chain Security</td>
<td>AsiaPac</td>
<td>3 years</td>
<td>£5M</td>
</tr>
<tr>
<td>Hybrid Cloud Security</td>
<td>N/A</td>
<td>2 years</td>
<td>£11M</td>
</tr>
</tbody>
</table>
Cybersecurity Footprint: Exposing your **Technology**

**Network Implementation Engineer**  
September 2012 – Present (3 years 5 months)

My role responsibilities are business-a-usual tasks and small projects:
- LAN: Small configurations on **Cisco switches and routers** (access and trunk ports, VLANs with HSRP, VPC)
- Small projects such as new switch landing and configuration (**Nexus 5K, Nexus 2K**)
- Firewall: Small firewall changes on **Juniper, Checkpoint** and **FortiGate firewalls** (rules, routes, NAT)
- Management of DNS and DHCP services through **Infoblox Grid Manager**

Additionally I take a part in organizing knowledge sharing sessions for my colleagues, interns, apprentices.

**Network Security Specialist**  
April 2012 – Present (3 years 10 months)

Working with the **Security Operations Centre** on a wide range of technologies including:
- McAfee IDS / IPS product suite
- BeCrypt Enterprise Manager
- Symantec Scan Engine Products
- Checkpoint IPS software blade technology
- Juniper IDP Devices
Cybersecurity Footprint: Exposing your *Technology*

**Firewalls**
- Palo Alto
- Checkpoint (includes some Nokia appliances)
- Fortinet
- Cisco ASA
- Lucent
- Juniper NetScreen
- McAfee Sidewinder
- Imperva SecureSphere (WAF)
- FortiGate
- Huawei

**Load Balancing & Application Delivery**
- F5 BIG-IP: LTM/GTM, Enterprise Manager, VIPRION (hardware)
- Citrix NetScaler
- Foundry ServerIron

**ACME**
*an Anvil Corporation*

- **Firewalls**: Palo Alto, Juniper SRX
- **Load Balancing**: F5 LTM & GTM
- **External Proxies**: BlueCoat 5G
- **IDS & IDP**: TippingPoint
- **Antivirus & Endpoint Protection**: FireEye WebMPS (malware), McAfee Endpoint Protection Suite
- **Emails**: McAfee Endpoint Protection Suite
  - + Nexus Cisco Routers and Switches
  - + ArcSight for analysis of external security threats

**Adversaries can:**

1. learn where current TTPs will be most effective
2. construct attacks to avoid or subvert known security measures
3. exploit vulnerabilities

Additionally, I take part in organizing knowledge sharing sessions for my colleagues, interns, apprentices.
Executive Footprint: Exposing your **Company & Family**

- **Private social media accounts**
  - Separation of work & personal life
  - **LOW RISK**

- **Private & public social media accounts**
  - Mix of work & personal life
  - **MEDIUM RISK**

- **Public social media accounts**
  - Association between work & personal life
  - **HIGH RISK**
Executive Footprint: Exposing your *Company & Family*

16 Executives, 30 Accounts:
- 94% LinkedIn
- 63% Twitter
- 31% Facebook

Exposure:
- Detailed information on conferences and business travel
- Detailed resume/CV public on LinkedIn
- Friends public on Facebook
Executive Footprint: Exposing your Company & Family

- **Twitter**: Father tweets daughter from his work account
- **Twitter**: Jane consistently tweets her location and activities
- **LinkedIn**: Detailed CV/resume information listed publically
- **Facebook**: Account is public, bio list numerous interests, friends are also public
- **Facebook**: Friends list is public and using same picture as business profile
- **YouTube**: Account is private but links to Facebook account
- **Pinterest**: Account is public and links to Facebook account

**Risk Levels**
- **Low Risk**
- **Medium Risk**
- **High Risk**
Open-Source Intelligence (OSINT): Scope of Capabilities

Technology and Strategy Exposure

Executive Footprint

Geopolitical Predictions

Supply Chain

Internet of Things (IoT)
- **Know** the scope of intelligence publically available to your adversaries
- **Understand** how the aggregation of this intelligence can expose your vulnerability landscape
- **Leverage** OSINT to monitor and mitigate your exposure
Thank you.

Questions and Discussion