COVID-19: Hardening Security Operations

Prepare for evolving threats and advanced attacks

Security operations teams are managing an increasing number of attacks stemming from today’s unprecedented coronavirus pandemic. There has been a sharp increase in social engineering attacks using COVID-19 themes to deliver various malware packages. Sudden work-from-home (WFH) models are increasing attack surfaces, creating new vulnerabilities attackers can target.

Hardening your security operations is more important now than ever before. It is imperative to be aware of the current threat landscape and to take the critical technical steps needed to harden security operations—and prepare the teams responsible for maintaining them.

Educating employees through a programmatic security awareness training and understanding all of the components of your attack surface are key. Security teams can then prioritize and execute short-term and long-term objectives to reduce risk. Once we return to our ‘new normal’ state, proactive steps like assessing your past response plans will help evolve response planning and threat modeling to harden security operations.

**IMMEDIATE ACTIONABLE STEPS TO TAKE**

### Short-Term Priorities

- **Threat Intelligence**
  - Be aware of threats by reviewing all warnings and notifications
  - Verify the source of the alert or warning before taking action. Direct Dial attention to a phishing attempt
  - Stay informed: check www.cdc.gov or your local state emergency management website
  - Don’t spread rumors. Focus on confirmed facts

- **Response Planning**
  - Develop threat modeling for processes in your organisation
  - Utilize risk tolerance reduction modeling
  - Prioritize and manage events once attackers have time to weaponize

- **Threat Modeling**
  - Create WFH threat modeling
  - Utilize risk tolerance reduction modeling
  - Assess and prioritize threats once attackers have time to weaponize

### Long-Term Priorities

- **Operations**
  - Secure all connections – VPN, 2FA, jump boxes, etc.
  - Secure an at home workspace vs. working from public areas
  - Ensure proper bandwidth
  - Provide up-to-date remote work guidelines
  - Work from approved devices to ensure device management
  - Utilize team chats for collaboration
  - Remove blacklisted IP’s and retrain monitoring tools for new user behaviors

- **Vulnerability/Patch/Remediation Management**
  - Invest in a vulnerability management program
  - Patch! Patch! Patch! This reduces the attack surface area
  - Center on remediation management – Not just the number of CVEs, but also the number of affected hosts

In times of need and crisis, it can be challenging to know who to turn to for help and support. Optiv is here to provide our valued clients with the expertise, staffing and technology needed to ensure business continuity.

Please contact your Optiv sales representatives, as needed, during this tumultuous time.

---

**SECURITY OPERATIONS TEAMS**

**Prepare for evolving threats and advanced attacks.** Security operations teams are managing an increasing number of attacks stemming from today’s unprecedented coronavirus pandemic. There has been a sharp increase in social engineering attacks using COVID-19 themes to deliver various malware packages. Sudden work-from-home (WFH) models are increasing attack surfaces, creating new vulnerabilities attackers can target.

Hardening your security operations is more important now than ever before. It is imperative to be aware of the current threat landscape and to take the critical technical steps needed to harden security operations—and prepare the teams responsible for maintaining them.

Educating employees through a programmatic security awareness training and understanding all of the components of your attack surface are key. Security teams can then prioritize and execute short-term and long-term objectives to reduce risk. Once we return to our ‘new normal’ state, proactive steps like assessing your past response plans will help evolve response planning and threat modeling to harden security operations.

**IMMEDIATE ACTIONABLE STEPS TO TAKE**

### Short-Term Priorities

- **Threat Intelligence**
  - Be aware of threats by reviewing all warnings and notifications
  - Verify the source of the alert or warning before taking action. Direct Dial attention to a phishing attempt
  - Stay informed: check www.cdc.gov or your local state emergency management website
  - Don’t spread rumors. Focus on confirmed facts

- **Response Planning**
  - Develop threat modeling for processes in your organisation
  - Utilize risk tolerance reduction modeling
  - Prioritize and manage events once attackers have time to weaponize

- **Threat Modeling**
  - Create WFH threat modeling
  - Utilize risk tolerance reduction modeling
  - Assess and prioritize threats once attackers have time to weaponize

### Long-Term Priorities

- **Operations**
  - Secure all connections – VPN, 2FA, jump boxes, etc.
  - Secure an at home workspace vs. working from public areas
  - Ensure proper bandwidth
  - Provide up-to-date remote work guidelines
  - Work from approved devices to ensure device management
  - Utilize team chats for collaboration
  - Remove blacklisted IP’s and retrain monitoring tools for new user behaviors

- **Vulnerability/Patch/Remediation Management**
  - Invest in a vulnerability management program
  - Patch! Patch! Patch! This reduces the attack surface area
  - Center on remediation management – Not just the number of CVEs, but also the number of affected hosts

In times of need and crisis, it can be challenging to know who to turn to for help and support. Optiv is here to provide our valued clients with the expertise, staffing and technology needed to ensure business continuity.

Please contact your Optiv sales representatives, as needed, during this tumultuous time.

---

**TECHNICAL CHECKLIST**

<table>
<thead>
<tr>
<th>Technical Checklist</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**4.20</td>
<td>F1.1**</td>
</tr>
<tr>
<td><strong>Reduce your attack surface area by continuously patching</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Find Out More**