|  |
| --- |
| 0:60-09:00 AM - Slide 1a |
| How did the team deal with the Loki Malspam Message? |

|  |
| --- |
| 10:29 AM - Slide 4 |
| What actions did you take?  What core infoSec principles are being affected (CIA)?  What other teams do you get involved at this point?  What do you do next?  Did they alert the proper chain of command? |

|  |
| --- |
| 11:31 AM - Slide 6 Pos or Neg |
| What actions did you take?  What core infoSec principles are being affected (CIA)?  What other teams do you get involved at this point?  What do you do next? |

|  |
| --- |
| 11:42 AM - Slide 7 Pos or Neg |
| What would you do with this information? |

|  |
| --- |
| 12:30 - Slide 8 |
| What actions did you take?  What core infoSec principles are being affected (CIA)?  What other teams do you get involved at this point?  What do you do next?  Did they divide up the work and form 2 smaller teams? |

|  |
| --- |
| 12:30 - Slide 9 y or n |
| What actions did you take?  What core infoSec principles are being affected (CIA)?  What other teams do you get involved at this point?  What do you do next? |

|  |
| --- |
| 12:56 - Social A |
| What actions did you take?  What core infoSec principles are being affected (CIA)?  What other teams do you get involved at this point?  What do you do next? |

|  |
| --- |
| 12:56 - Social A |
| What actions did you take?  What core infoSec principles are being affected (CIA)?  What other teams do you get involved at this point?  What do you do next?  Did they alert the Major Incident Team?  Did they change the password and enable 2FA? |

|  |
| --- |
| 12:56 - IF Social FAIL |
| The accounts have been taken again. How can this be?  What actions did you take?    What core infoSec principles are being affected (CIA)?  What other teams do you get involved at this point?  What do you do next? |

|  |
| --- |
| Debrief |
| Identify – What went well?  Identify – What could be improved?  Protect – What went well?  Protect – What could be improved?  Detect – What went well?  Detect – What could be improved?  Respond – What went well?  Respond – What could be improved?  Recover – What went well?  Recover – What could be improved? |

|  |
| --- |
| Debrief 2 |
| Any concerns for the ACME as a whole?  Any issues with procedures / documentation?  Any issues with process?  Any issues with technology / logs / IR platform?  In what ways did the involvement of the media change the dynamics of the incident?  How could the media have gotten involved? |