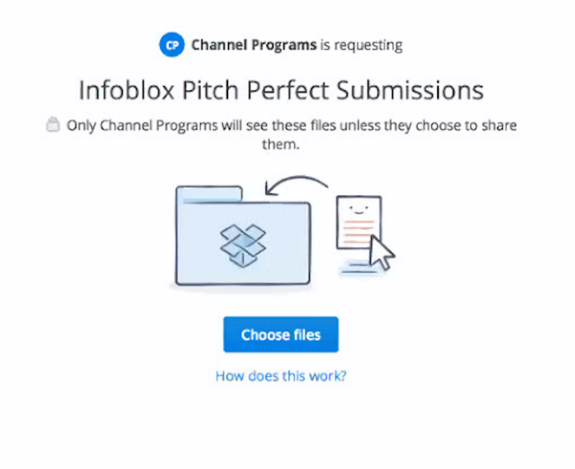
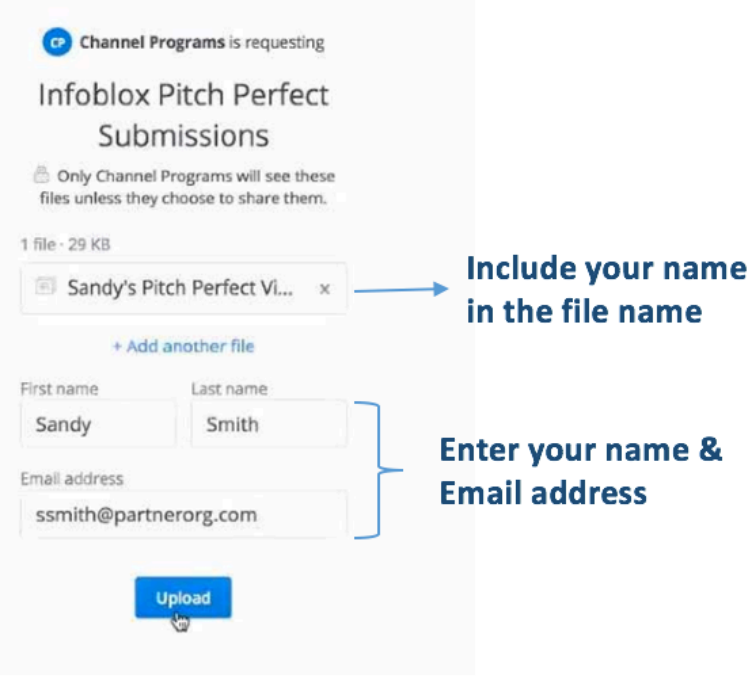
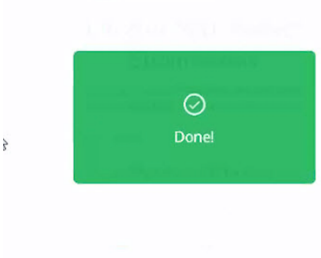
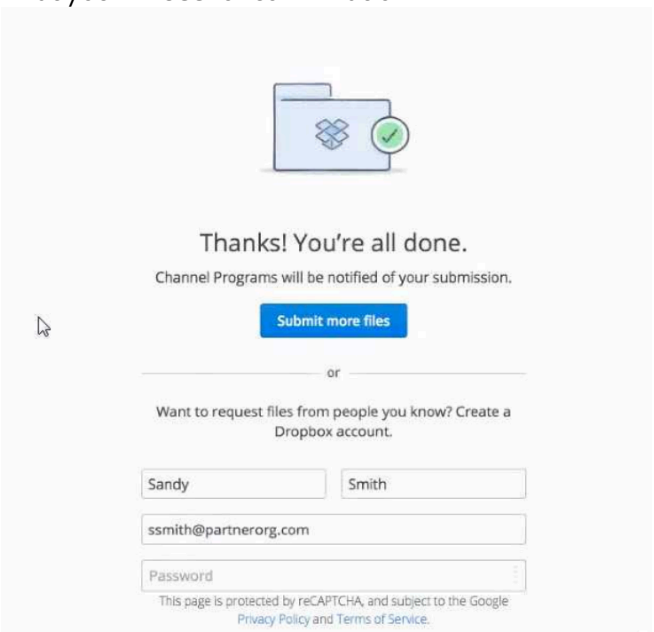
Creating the WINNING Perfect Pitch – Tips and Tricks

Recording your pitch	• Watch the pre-recorded sample pitches available on the Micro-portal on the What to Know page. • Practice your own version of the pitch before you record • Record your pitch in whatever tool using whatever device is most convenient for you. • We are not looking for professional videographers, the focus is on your pitch and your message • Do make sure you have good audio quality to ensure your presentation can be fairly evaluated • Follow the instructions in the Loading your Video section of this document. MAKE THIS PERSONAL – **YOUR** MESSAGE TO **YOUR** CUSTOMER
Audience for your pitch:	**The scenario: How would you position Infoblox with what you sell today?** **Your mission:** Pitch imagining you are speaking to a security person **Your audience may be thinking:** "I'm an existing Infoblox customer, but I'm not the network person - I'm the security person and I have a *vague* idea of who you are and what you do…. Why am I talking to Infoblox? I already have security solutions. You're the Networking company. The network person is trying to get me come to this meeting, why am I here…?" Try to avoid any Infoblox acronyms and specific terms the customer might not understand.
Sales Rep., Remember to include the critical points	1. **Target account type:** Tell us who you are talking to 2. **Integration vendor**: you plan to integrate with and why 3. **Problem statement:** Business Issue: 91% OF REPORTED MALWARE INCIDENTS USE DNS IN ITS LIFECYCLE (Cisco Report) • Most companies have invested heavily into protection of key network assets such as port 80, Email, Web, FTP ETC. • Some have even implemented DDoS protection solutions. That's a good start, but it's only signature or reputational protection. • Cisco also says 100% of corporate networks contain malware, and this malware almost always connects to C&C over DNS queries, bypassing corporate firewalls. 4. **The Hook:** What would you say if I told you - we can help make the security tools and systems you currently own work better together, share data more easily, and provide your business more ROI? • If you own a vulnerability scanner, SIEM, endpoint security solution, NGFW, Web Gateway, or even a Sandboxing APT detection solution, NONE of these offers adequate protection from the #1 attack vector on the Internet today – DNS. 5. **The problem to solve:** PROTECTING YOUR DATA from DNS attacks • DNS Traffic has exploded due to BYOD/IOT. • NGFW as an enforcement point running reputational black lists are providing "some" measures of defense but it is insufficient to stop exfiltration and DNS tunneling • The #1 way hackers are getting data out of customer networks is via DNS today. • REPUTATIONAL ONLY DEFENSE FOR DNS IS NOT ENOUGH! Hackers have ways of working around them

	• Net result: APT malware can circumvent the black list and communicate freely over port 53 **6. <u>How Infoblox can help</u>:** • Security Solution Enhancement • Visibility into DNS activity • Automated Responses to DNS events • Enhanced identification of DNS attacks – REPUTATIONAL lists are not enough • Ecosystem: Infoblox provides over 35 API integrations to security venders in the market to take automated action if we find malware or DNS exfiltration in your network environment **7. <u>Value – what does our solution do for you</u>** • Improved incident response time • Reduce risk of NW compromise and Data Exfiltration • Visibility into new devices and infected hosts in a single place for networks and security Ops team • Context for prioritization of threats • Automate remediation • Improve security posture while maximizing ROI of existing solutions • best-in-class protection • Safeguard against losing sensitive data **8. <u>Call to Action</u>**: RUN A DATA EXFILTRATION DEMO FROM INFOBLOX • We can show you how easy it is to send a file of sensitive data over DNS queries out to an Infoblox-hosted "malicious" Amazon DNS server. Only simulated data is used in this demo. • But if we can exfiltrate any file in less than 5 minutes without your current system seeing it couldn't APT Malware do the same thing with real data? • Is this resonating with you? If so, when can we meet next for a deeper discussion on Infoblox DNS Security?
<u>Pre-Sales Rep., Remember to include the critical points</u>	**1. <u>Target account type:</u>** Tell us who you are talking to **2. <u>Integration vendor</u>:** you plan to integrate with and why **3. <u>Problem statement</u>**: <u>Technology Risk:</u> DNS IS AN UNENCRYPTED, UNAUTHENTICATED UDP PROTOCOL THAT'S PASSED THROUGH PORT 53 WITHOUT INSPECTION • C2/Botnet Command and Control Traffic over Port 53: Instruction sets to infected devices. • Data Exfiltration over DNS: Transfer of your confidential data over DNS Query. • Denial of Service VS DNS: Volumetric attacks to knock out DNS services. **4. <u>The Hook</u>:** What would you say if I told you - we can help make the security tools and systems you currently own work better together, share data more easily, and provide your business more ROI? • If you own a vulnerability scanner, SIEM, endpoint security solution, NGFW, Web Gateway, or even a Sandboxing APT detection solution, NONE of these offers adequate protection from the #1 attack vector on the Internet today – DNS. **5. <u>The problem to solve:</u>** PROTECTING YOUR DATA from DNS attacks • DNS Traffic has exploded due to BYOD/IOT. • NGFW as an enforcement point running reputational black lists are providing "some" measures of defense but it is insufficient to stop exfiltration and DNS tunneling • The #1 way hackers are getting data out of customer networks is via DNS today. • REPUTATIONAL ONLY DEFENSE FOR DNS IS NOT ENOUGH! Hackers have ways of working around them

	• Day Zero DNS Exploits go unseen • Net result: APT malware can circumvent the black list and communicate freely over port 53 **6. <u>How Infoblox can help</u>:** • Security Solution Enhancement • Visibility into DNS activity • Automated Responses to DNS events • Enhanced identification of DNS attacks – REPUTATIONAL lists are not enough • Ecosystem: Infoblox provides over 35 API integrations to security venders in the market to take automated action if we find malware or DNS exfiltration in your network environment **7. <u>Value – what does our solution do for you</u>** • Improved incident response time • Reduce risk of NW compromise and Data Exfiltration • Visibility into new devices and infected hosts in a single place for networks and security Ops team • Context for prioritization of threats • Automate remediation • Improve security posture while maximizing ROI of existing solutions • best-in-class protection • Safeguard against losing sensitive data **8. <u>Call to Action</u>**: RUN A DATA EXFILTRATION DEMO FROM INFOBLOX • We can show you how easy it is to send a file of sensitive data over DNS queries out to an Infoblox-hosted "malicious" Amazon DNS server. Only simulated data is used in this demo. • But if we can exfiltrate any file in less than 5 minutes without your current system seeing it couldn't APT Malware do the same thing with real data? • Is this resonating with you? If so, when can we meet next for a deeper discussion on Infoblox DNS Security?
Loading your video	**How to Submit your pitch perfect video** **1. Click dropbox link** http://bit.ly/IBPitchPerfectSubmission This is what you'll see on the landing page:  1. Upload your video file. **Please include your name and company name in the file name.**

	(Example: SandySmith (***company name***) Pitch. **Enter your name and email address in the fields.**  2. Click 'upload'. Finished! This is what you will see for confirmation.   Thank you for pitching! **Pitch guidelines: We suggest 5 minutes**
What happens next:	Once you've submitted your video 1. Your CAM will review, and you will receive feedback if required. 2. Use this link to access the SPIFF claim form: http://bit.ly/IBSPIFFClaim 3. Our security judge panel will meet monthly and review submissions. 4. The top 10 videos will be selected in January. Semi-finalists will be contacted and invited to refresh their videos for a more professional look.

	5. The winner will be announced in February.