What Should Chief Security Officers Ask Santa For This Christmas? (Part 1)

Duncan Macrae, December 18, 2015, 12:22 pm

image: http://www.techweekeurope.co.uk/wp-content/uploads/2015/01/shutterstock_225552961-684x250.jpg

It's that time of the year when chief security officers (CSOs) can ask Santa for a wee bit of help. But what should they be asking for? Here are a few ideas

Simon Moor, UK regional director for Check Point

"A security gift that many CISOs will want to find in their stocking is a sandbox: not the bucket-and-spade variety, but one which combines traditional virtualised malware detection and more advanced CPU-level sandboxing. Attackers are increasingly deploying more sophisticated, custom variants of existing malware and zero-days that are capable of recognising when they're in a conventional sandbox.

"However, if the sandbox is able to examine activity below the software level, and inspect what's happening in the CPU on which it is running, any malware exploits can be spotted in the execution instructions being sent to the CPU. This means the most dangerous threats can be identified in their infancy, before they can evade detection and infect networks."

Alexei Miller, MD, New York, DataArt

"Dear Santa,

"This Christmas, please bring me a simple pill. I really need it to get simple again. I've been a good boy all year, but this stuff is now hard. IT used to be simple. We had IBM and then Microsoft and that was it. It was simple and beautiful. Now you have all these clouds and Cassandras and Apache Mesoses (or is it Apache Moses, in which case I should pay more attention) and Kafkas and Dell buying EMC and on top of it all business people want their apps to look beautiful. They are crazy! Listen Santa, please bring me my life back or I will hire Chinese hackers to hack into your sleigh and steal all the presents."

image: http://www.techweekeurope.co.uk/wp-content/uploads/2014/12/Santa-security.jpg

Lewis Henderson, consultant at Glasswall Solutions

"Aside from asking for a restful night's sleep in the face of an ever-increasing threat of cyber-breach, how about something different that actually works? CISOs are caught in the same trap as their technology and can only react based on what they know to be bad. Why doesn't someone come wave a magic wand to grant their Christmas wish and render looking bad null and void?

"Imagine how it would be if there was such a sparkling solution that could find its way into every CISO's Christmas stocking. One that is not reactive, but fully proactive, and instead attempting to classify the bad, engineers out cyber threats through a unique approach of regeneration of files and documents to known good standards.

"Like the best Christmas fairies, it is only interested in spreading happiness and doing good, making files truly benign-by-design, simply by excluding anything malicious and hidden. In fact it is not magical, it is available now and works every time.

"That's a CISO's wish that Father Christmas can deliver without a mince pie, granting the entire management team a restful night's sleep."

Eldar Tuvey, CEO and co-founder at mobile threat preventers Wandera

1. A Security Elf app for each of our employee's smartphones with connection to the cloud for real-time scanning and blocking of threats.
2. Christmas crackers for all our employees with acceptable mobile usage policy inside instead of party hats, explaining how to look out for phishing threats, malware, exploits and how to keep their mobile devices safe.
3. A reminder in each employee's Christmas stocking to never visit unapproved app stores or jailbreak their device.
4. A magic sleigh full of machine learning techniques to analyse our company web data and spot anomalies and zero day threats before they reach our employee devices.
5. World peace and an end to user errors and risky behaviour.

Darren Anstee, chief security technologist at Arbor Networks

"This year, given the number of breaches that have been in the media if I was a CISO I would be asking for a 'silent night' – free of worry about increasing business risk. I would be looking for a way to quickly identify and contain the key, targeted threats that could turn into that embarrassing breach. Even the elves don't have a magical, single technology that can do this – but we can help ourselves by giving our operational security teams tools that make them more effective. Tools that can visualise threat indicator and network activity over time can help, especially if they allow the user to navigate through this data at the speed-of-thought, reducing event investigation and incident response times. Truly though, if I was a CISO, I think I would want Santa to pass me by; I would just be worried about another undetectable incursion into a supposedly secure environment."

image: http://www.techweekeurope.co.uk/wp-content/uploads/2012/11/Dusit.jpg

Chris Griffiths, director of New Product and Business Development, Nominet

"Greater DNS insights!

"The Domain Name System (DNS) is a crucial yet often overlooked part of a business' network infrastructure. While you may think the DNS is just for looking up web URLs, the truth is that it's now used for much more, such as for software licence checks and by video services to get around firewalls. Unfortunately, it's also being used by hackers to access company data.

"DNS visualisation tools, using big data analytics, can uncover valuable insights among the billions of DNS queries any large business will generate. They can give CISOs a holistic view of their network's activity, uncovering unusual traffic created by things like botnets, spam, malware, inefficiencies and other threats in the network. In 2011, it allowed us to spot the BIND bug, and continues to help us keep the UK internet safe and secure.

“With benefits such as these, every CISO should be wishing for greater DNS insights this Christmas!”

Mark James, security specialist at IT Security Firm ESET

“Dear Santa, I would like all my hardware devices to automatically receive the latest firmware, patches and updates as soon as they are released (and tested). I would also like them to do exactly the job I purchased them for with optimum efficiency and notify me if they are going to fail. All too often breaches in security happen because exploits have not been patched on hardware that routes important data throughout our organisation. Updating is one of the core processes in building a secure network, and if you’re in a particularly good mood would it be possible to help all of my users understand the risks of opening emails and clicking on links?”

Atchison Fraser, VP marketing, Xangati

“A dual capability to deceive and thwart hackers in order to drain their resources and trick them into revealing their threat vectors, and a master grid analytics fabric that predicts performance impacts of hacker attacks.”

Oscar Arean, technical operations manager at Databarracks

“CISOs this Christmas will be asking for extra resources dedicated to cyber-security. Defending against attacks by organised hacking groups is getting more difficult, and the fact of the matter is CISOs can only ever afford to direct a portion of their budget to defending against them. Hacking groups make a lucrative career out of orchestrating malicious attacks – they will always have more time, money and resources for attacks than a security team will have for defence. Buy-in from the rest of the business when it comes to cyber-security – a bigger budget, more resources, more awareness throughout the business – is the best present they could ask for.”

Vincent Smyth, GM & VP EMEA Flexera Software/Secunia

“CISOs need to keep two things in mind when they ponder what they want for Christmas: That for a large UK organisation, the average cost of their worst security breach is £900,000. And that the vast majority of successful security breaches happen because hackers are able to exploit software vulnerabilities that are publically known and for which a patch is available.

“This last bit is in fact good news: It means that, with the right software vulnerability management tools at the foundation of their IT security strategy, IT departments have the power to counter the threat.

“Here’s how: if IT teams responsible for security have full visibility of the IT products in use throughout the infrastructure and receive actionable intelligence on vulnerabilities as they become known, they are able to assess and mitigate the risk and protect business critical data from intruders.

“Vulnerabilities are the entry points hackers use to gain access to organisations and shutting those doors can save the business a bundle in losses – of money, brand value and resources spent fixing the damage once it’s done.”

Jonathan Sander, VP of Product strategy at Lieberman Software

“This Christmas CISOs should ask Santa for strategies to out automate bad guys, ways to extend security to the hybrid world, and for staff that get the strange new world in IT. Examining the post mortem of each new breach, we see bad guys are more professional and automated. For a CISO to quicken the pace IT has moved until now to automate their cyber defense behind the firewall may take a bit of Santa’s magic. This needs to happen on the new, changing grounds of cloud and hybrid IT. Even a little bit of cloud can change all the rules for security, inverting assumptions about staff, locations, authentication, etc. Security staff that understands cloud, hybrid, automation, and the affect these things have on security policy and operations should be at the top of every CISO’s Christmas list. Security must adapt, and adaptation needs people who know how and why.”

Steve Ward, senior director at iSIGHT Partners

“This year saw another cluster of companies fall victim to cyber attacks, sacrificing partner and customer trust, brand loyalty and share prices. As we come to the end of 2015, wouldn’t it be great if CISOs across the country had a head start, a crystal ball, a new visibility of what could be storming their networks?

“Cyber threat intelligence is the next best thing. It allows CISOs to be one step in front of potential attackers, giving them much better armoury to protect themselves against targeted threats.

“That’s why we think every CISO should ask Santa for threat intelligence this Christmas. No sports team takes to the field without researching its opponent, yet every day most cybersecurity professionals go to work without any idea about the identity and probable actions of their adversaries.

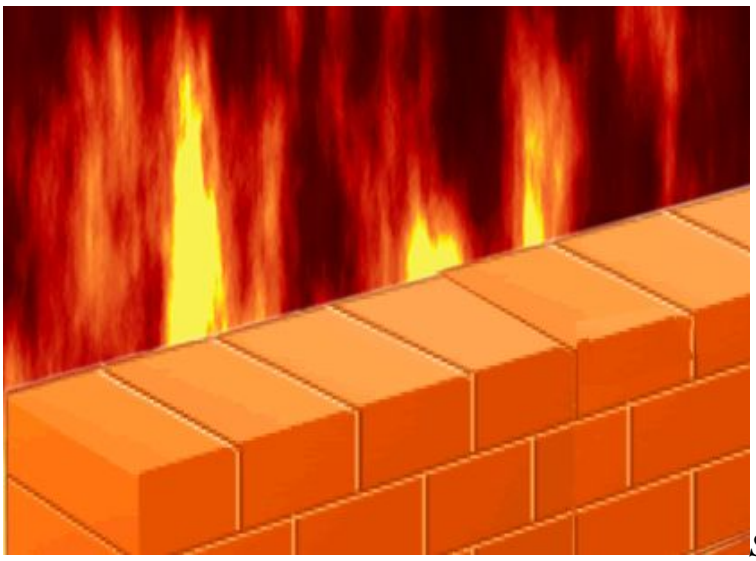
“If you don’t understand the intentions and competencies of your opponents then how can you understand the risks to your company or focus your defence?”

Justin Harvey, CSO at Fidelis

“It’s essential that companies have a security-savvy board of directors, who understand the difficulty in securing a company against advanced attackers. They need to see the value in investing in strategic intelligence services, made up of experts who can analyse threats and draw conclusions about a threat group; its tactics, techniques and procedures, as well as in some cases offer a motivation behind an attack. This can be much more extensive than tactical intelligence which is often generated by machines.

“Typically, 3-5 percent of IT spend goes on security, which is a fraction of what is needed. Top of a CISO’s Christmas list this year, therefore, will likely be a bigger budget – perhaps between 5-10 percent of IT spend. As well as investing in strategic intelligence services, CISOs will want to boost endpoint security, which is increasingly valuable as the network perimeter disappears and organisations move to the cloud.”

image: http://www.techweekeurope.co.uk/wp-content/uploads/2012/02/Firewall.jpg

 ***Stuart Brown, principle solutions architect at Redcentric***

"If Redcentric was playing Santa, we would give CISOs a cyber threat angel to make the network as safe as pigs in blankets over Christmas! We would wrap the network in the latest cyber threat platform so they can rest easy over Christmas.

"Using firewalls, the angel of protection would safeguard the network from known and unknown threats by detecting and stopping any malware, spyware or botnet activity. Even if the malware hadn't been detected before, using the integrated sandbox it would be analysed dynamically and stopped. Once detected the firewall would then distribute details of the threat to all firewalls globally, via automatic, built-in protection, ensuring that companies around the world are kept safe beyond Christmas (and beyond).

"This means the CISO can keep their slippers on by the fire safe in the knowledge that the firewall is busy analysing threats and building protection for their network."

Jeremy Bergsman, practice leader at CEB

"While it is tempting to ask Santa for shiny new technologies, such as Big Data, which help with cybersecurity, CISOs should be asking Santa for their employees to take "security hygiene" more seriously and for increased training for their teams.

"All security breaches happen over a sustained period of time with several individual breaches, which is why hygiene and training is so critical. In fact, research has found that 99.9% of attackers exploit a breach that has been present for over a year. These breaches can be avoided or at least minimised if faults are monitored for and fixed as and when they are detected. Of the 150 companies CEB surveyed on the use of big data, not a single one said they had their big data technologies working properly which is why we advise to prioritise 'security hygiene'.

"I hope this is of interest and look forward to hearing back from you. Please let me know if you require any further information, I would be happy to set up a call with Jeremy if this is of interest."

Ian Muscat, product communications manager, Acunetix

"A stronger voice in boardroom discussions. Given that more organisations are recognising Information Security as a C-Level activity, and that Security policies affect organisations as a whole, security policies need to be endorsed by and overseen by executives and board members. A stronger voice in the board room will make a CISO's role more effective in strengthening an organization's information security posture and sustaining a security-first company culture by shifting employees' mindsets and build strategic alignment to effectively protect property, assets, and sensitive information."

Andy Hardy, EMEA MD at Code42

"Santa's gifts haven't always been that useful—just think back to some of the "misses" you've received. But with 90% of large companies in the UK experiencing cyber security breaches this year, it is high time he puts his data protection gift-giving hat on.

"This Christmas, the prime spot in any CISO's wish list should be reserved for making endpoint security as robust as possible. With the widespread shift to cloud computing and flexible working, employees are increasingly creating and accessing corporate data through devices like smartphones and personal laptops – outside the corporate firewall. It is essential that endpoint data is protected and monitored on the move.

"Recent scandals like TalkTalk also show that enterprises must ensure that all information is encrypted securely. Encryption is no longer a dirty word – regardless of what the Investigatory Powers Bill may suggest – but an absolute necessity to protect a business and its reputation."

image: http://www.techweekeurope.co.uk/wp-content/uploads/2014/12/shadow-IT.jpg

Ben Harknett, VP EMEA, RiskIQ

"This year CISOs should be asking Santa for better visibility into the activities of Shadow IT, particularly where business units or marketing create public facing web sites and mobile apps. Vulnerabilities in public facing digital assets have become low hanging fruit for hackers and are frequently exploited to compromise

organisations and their customers. At the end of the day the security team can't protect what they don't know about and Shadow IT activity can be a major blind spot."

Kane Hardy, VP EMEA, Hexis Cyber Solutions

Dear Santa – CISOs 2015 Christmas Wish List

1. Separate the CISO function from IT enabling a more comprehensive enterprise security strategy and alleviating potential points of conflict.
2. Silo Buster. This toy would be great and would help me become more effective at securing our environments because we need to work better across the silos that exist in and outside of the security department.
3. Better behavior-based detection. It's becoming harder to determine what's naughty and what's nice in my infrastructure. Give me behavior-based detection to improve my visibility into activity occurring on my endpoints and network.
4. Red light reduction. My team is overloaded with security alerts. Red lights are blinking more than Rudolph's nose. Give me security analytics that better prioritise alerts and reduce false positives.
5. Security automation to speed response. Skilled security analysts are harder to find than reindeer for Santa's squad. Give me security automation solutions so I can force multiply cyber response efforts and respond better.

Original article – http://www.techweekeurope.co.uk/security/security-management/security-officers-ask-santa-christmas-182564