CALIFORNIA STATE UNIVERSITY SAN MARCOS

THESIS SIGNATURE PAGE

THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE

MASTER OF SCIENCE

IN

CYBERSECURITY

THESIS TITLE: Designing a Security Architecture for Sports Manufacturing Company

AUTHOR: Erik Chapman

DATE OF SUCCESSFUL DEFENSE: May 2, 2018

THE THESIS HAS BEEN ACCEPTED BY THE THESIS COMMITTEE IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN
CYBERSECURITY.

Teresa Macklin		5-2-2018
THESIS COMMITTEE CHAIR	SIGNATURE	DATE
Yi Sun		5/3/18
THESIS COMMITTEE MEMBER	SIGNATURE	DATE

Designing a Security Architecture for

Sports Manufacturing Company "X"

Erik Chapman

April 14th, 2018

Faculty Advisors

Project Chair: Ted K, Company "X"

Committee Member: Teresa Macklin, Program Coordinator

Committee Member: Yi Sun, Professor

Cybersecurity Professional Science Masters

California State University, San Marcos

Table of Contents

Table of Figures iii
Executive Summary iv
Introduction 6
Materials and Methods 7
Discussion 9
Framework Identification 10
Compliance 10
IT Policies 11
Security Tools Procurement 12
User Training 18

Table of Figures

Figure 1: Defense in Depth layered approach to security 8
Figure 2- Overview of Security Tool Recommendations 12
Figure 3: Vulnerability Scanner Comparison..... 14
Figure 4: Endpoint Detection & Response Solutions (Gartner) 15
Figure 5: Endpoint Protection Solution Comparison 16
Figure 6: VPN & 2-Factor Authentication Comparison 17
Figure 7: CIS Top 20 Security Control Implementation..... 19
Figure 8: Security Products Comparison..... 20
Figure 9: Recommended Actions..... 20

EXECUTIVE SUMMARY

Designing and Building a Security Architecture

and Policies for a Medium Sized Business

Sports Equipment Manufacturing Company "X"

Erik Chapman

April 14th, 2018

Professional Masters Degree Program

Cal State University San Marcos

Organizations often expand exponentially before realizing the need for security based on the many, well publicized breaches, incidents, and outages. This Semester-In-Residence project developed the security framework for a well-known international sports equipment manufacturer, Company "X". This occurred during the period "X" was in the process of a major divestiture from parent company "Y". The project involved assessing the policies and security architecture that had been provided by Company "Y" and developing a plan for new policies and security architecture once Company "Y" no longer provided the infrastructure and services. Requirements included information security policy review, security processes, security assessment, compliance, procurement, implementation, and management of security tools. The product developed for Company "X" was a designed, purchased, and implemented defense-in-depth program, from the network edge to the endpoints. Upon residence completion it was apparent that additional time would be required to fully develop, integrate, and maintain a fully functioning DevSecOps environment.

Acknowledgements

First of all, I would like to thank all of the professors of the program for their unwavering support and accommodations over the past two years. Anytime one of the students felt that they were working hard by balancing work life and school, all they had to do was look at the day in and day out dedication of Professor Macklin. World class professional with an endless amount of knowledge. Lastly, I would like to thank my friends, family, Scarlet, Penelope, Orion, Apollo, and Gracie for being by my side for this learning experience. Never say "goodbye", just "see you soon".

Dedicated to:

A great group of family, friends, Meat Nugget, Penelope, Orion, Apollo, and Gracie

Introduction

Sports manufacturing is the industry where innovative people, who want to pave the path of their own careers, come together in hopes of improving the lives of others through the enjoyment of sports. Manufacturing companies are among the top three most often targeted industries (along with Financial Services and Information Technology) according to the 2016 IBM X-Force Threat Intelligence Report (IBM 2017). Company "X" is a sports equipment manufacturing company and the previous parent company, Company "Y" is a multibillion-dollar apparel and sports company. With locations worldwide, network dependencies and federated trust relationships between the two, they are prime targets for a cybersecurity attack.

The retail and manufacturing industries generate massive revenue and with revenue comes a responsibility to protect the intellectual property of the company, sensitive data of customers, and critical assets in order to ensure a secure and reliable environment. Company "X" is required to comply with GDPR and is a privately held company. GDPR compliance requires companies to practice due diligence in protecting European Union citizens data regardless of where the data resides geographically. This data can include but is not limited to: IP addresses, cookie data, name, address, social security number, birth dates, and biometric data.

Currently, a third-party vendor is responsible for processing all financial transactions thus PCI compliance is not a business requirement for Company "X". A large portion of "X" revenue is from online sales and cyber criminals have taken notice as they continuously try to infiltrate the public facing portal used for online sales. These attacks typically have the objective of financial profit – taking intellectual property, or simply denial of service.

In any organization, the key stakeholders must be able to make informed decisions on projects, on actions to protect the corporate data and information systems and on accepting risk. They do this by listening to their trusted security advisors. Differences in opinion between stakeholders and security advisors often occur because there are many different security frameworks. Security recommendations sometimes lack "big picture" analysis and impact. Also, framework implementation can differ greatly based on whether the architecture is on-premise or in the cloud. For example, for deploying into an AWS environment, the

AWS Cloud Adoption Framework, which is based on NIST 800.53 but tailored to cloud environments, would be a more focused roadmap than the standard NIST framework or CIS 20 controls.

Policies and frameworks must be identified prior to the design of a defense-in-depth architecture. “X” inherited policies from “Y” but decisions must be made on the degree to which these inherited policies should be adopted or modified. These decisions must be based on business needs including weighing security versus convenience, and on risk analysis for company operations

Similarly, Company “X” must also make an executive decision on which framework to follow. Common security industry frameworks such as ISO27001, COBIT, NIST, RMF, and CIS20 are essentially lists of best business practices. The decision here will be informed by the regulations to which Company “X” must comply. As part of this Semester in Residence project I will recommend a framework, and seek leadership buy-in.

The Defense-in-Depth projects proposed for this project were identified as IT Policies, security tools procurement, platform hardening, security assessment, security services, user training, and compliance.

Materials and Methods

The project began by designing a defense-in-depth strategy based on “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies” by Industrial Control Systems Cyber Emergency Response Team (DHS 2016). Although designed for ICS systems, the principles can be applied to all digital platforms. The strategy, listed in order, is:

- Risk Management
- Asset Inventory and Risk Characterization
- Physical Security
- ICS Network Architecture
- Security Architectures
- Host Security
- Security Monitoring
- Vendor Management and Security

- Human Element

The defense-in-depth strategy is designed to continuously secure an environment, relying on the underlying layers of security to address potential failures in preceding layers. :

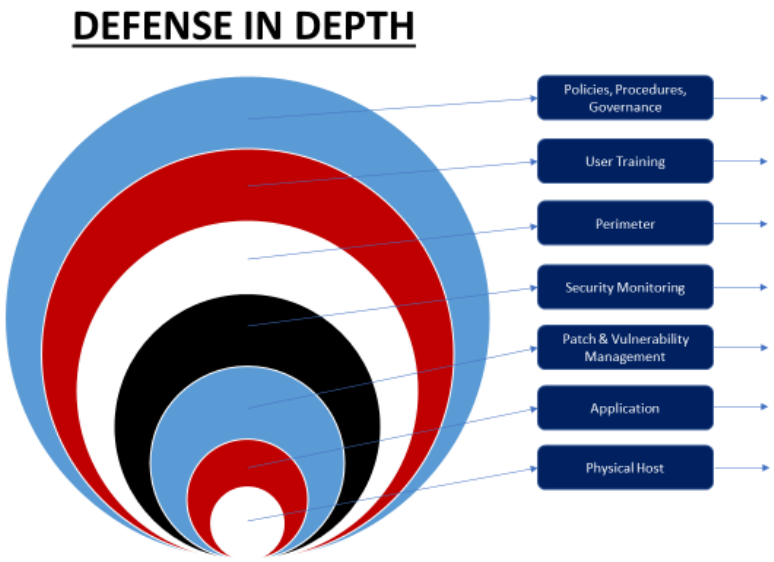


Figure 1: Defense in Depth layered approach to security

The diagram in Figure 1depicts a defense-in-depth strategy from a data flow perspective. The concept is to secure the network by providing security controls at each major step of the data path from the network edge to the individual endpoints across all tiers of the OSI model

Phase two of the project was to gather data concerning the list of information assets, identification of critical assets, and design of the network architecture. Phase three of the project was to gather resources including the annual Gartner report testing the efficacy of different endpoint protection software in various scenarios. Additional online information was also garnered from the FBI cyber news website, security vendor websites, and Mandiant white papers.

Analysis methods included quantitative charts of product pricing, graphs of security product benchmark comparisons, user experience surveys and comparison charts of business needs compared with security concerns. Techniques included interviews, roundtable

discussions with senior leadership, sample tests, surveys, and observation (PMR 2018). One experiment was conducted and it was based on Randomized Block Design, assigning representatives from each department to participate in trial period for the security software and restriction settings to test workflow compatibility. The model used to assess company "X" cloud environment was the Cloud-Trust cloud security assessment model (Gonzales 2015).

Discussion

The divestiture left Company "X" with major business operations gaps. These operations gaps included personnel loss, funding loss, and technological loss. Company "Y" employed personnel for all IT Security positions and those positions stayed under Company "Y" hiring authority. By the nature of the divestiture, Company "X" was now in dire need of filling these positions as soon as possible. Based on the size of "X", IT Security warranted only one new hire and a job reclassification of one current employee. Company "X" does not intend to create a CISO or CSO position. Instead, I reported to the Director of IT. Now that Company "X" was solely responsible for all network, system, and application security, the project goal was to provide a high-level list of bare minimum-security controls to protect the platform. The list could then be referred to in the future for procuring additional or replacement security controls and remediation's.

From project onset, the pace was frenetic. For every day that "X" remained on "Y" services, the transfer licensing agreement mandated payment based on which services were being utilized. Official onboarding would not occur for two months and many projects were already behind schedule. Migration to a new, unmonitored and unprotected domain, had already begun and very few security controls were in place.

Company X uses Office365 for its business function software platform. The Office 365 environment lacked security including no multifactor authentication, endpoint protection lacked adequate attention, firewalls lacked basic security controls, just to name the most obvious security gaps. I was asked to assess the current security controls and build out a plan for defense-in-depth but I quickly realized that no framework had been identified and no IT policies were in place. These would need to come first.

The many different initiatives and projects were simultaneously ongoing because of time constraints and blockers. This way, progress could be made in one project while waiting for a blocker to be resolved in another project. Once a framework was identified, I developed new security policies based on leadership input, procured new security tools, hardened the Office 365 environment, negotiated a security assessment, negotiated the onboarding of a MSSP, developed a cyber user training program, and conducted compliance checks against the environment.

Framework Identification

There were many different frameworks to consider when deciding which one to apply in "X" environment. Three of the most prevalent frameworks are Cobit, ISO, and NIST. COSO focuses on business orientation and IT governance. ISO 27001 (Information Security Management System) includes people, processes, and IT Systems and is a systematic approach to securing sensitive data by applying a risk management process (ISO, 2018). NIST 800-53 is much like ISO except it also includes a cost-benefit analysis and a formal authorization to operate as a culmination of the assessment. These are typically conducted every three years and in some cases, are re-validated on an annual basis. At first, I was considering NIST and ISO27001 because during my time working with government organizations, this was the framework of choice. What I also recall from that experience, was the considerable time that went into developing the document and validating that controls were applied in a timely manner. Due to the shortage of staff at Company "X", I decided to work through the NIST framework once CIS 20 security controls were implemented.

Compliance

Information Security compliance requirements are dependent on the type of business an organization conducts. Some of the most common data security requirements are HIPAA (Health Insurance Portability and Accountability Act), Sarbanes Oxley, FISMA, GLBA (Gramm Leach Bliley Act), PCI-DSS (Payment Card Industry Data Security Standard), and the most recent GDPR (General Data Protection Regulation) (Vanderburg 2018). Many corporate entities are required to adhere to multiple compliance requirements at the same time.

For the purposes of Company "X", GDPR is the only required compliance because all credit card data is stored and processed by a 3rd party which effectively relieves "X" of any liabilities stemming from PCI compliance. Also, no customer birth dates, social security numbers, or medical information is collected thus limiting further regulation requirements. PCI-PAL, integrated with the Cybersource Payment Management platform, eliminates card data from telephone conversations and prevent agents from seeing any card data on the screen (Cybersource 2018). A token is provided verifying that the charge was successful.

GDPR was enacted in April of 2016 by the European Parliament as a replacement for the Data Protection Directive of 1995 but was not scheduled to be mandatory until May of 2018. The GDPR basically requires companies to provide a "reasonable" level of protection for EU citizens data regardless if the data is being held outside of the EU. Some of the requirements are that companies must show that they can purge all customer data within 48 hours of a customer request, must identify where all instances of the customers data resides, and must report a data breach within 72 hours. The data covered includes basic information such as name, address and ID numbers, web data, health data, biometric data, racial or ethnic data, political opinions, and sexual orientation. Companies must be compliant by May 25, 2018. The GDPR allows for penalties up to €20,000,000 or 4 percent of global annual turnover, whichever is higher (GDPR 2018).

The first step in beginning the compliance program at company "X" was reviewing the network architecture and assessing what customer data is retained and where. This was completed in the first month of the internship and from that point I became the technical liaison for the 3rd party GDPR attorney that was hired to provide recommendations on policy deficiencies. I would later be responsible for managing the implementation of the policy decisions in order to become GDPR compliant (Nadeau 2018).

IT Policies

An Information security program is a set of policies and related standards that are intended to protect information technology assets while complying with all relevant federal, state, and local laws and regulations. These policies are generally identified by the framework adopted as the implementation model for the program. Recommended bare minimum categories to be covered by policies were AUP (Acceptable Use Policy), Security Awareness, Information Security, Disaster Recovery/Business Continuity Procedures, Change Management, Incident

Response, Remote Access, BYOD, Vendor Access, and Media destruction including retention and backups (Grachis 2016). The IT policies from the previous ownership company dated back to 2014 and required major revisions before publishing as adopted policies for "X". Some of the major revisions included changing password length from 8 to 12, password history reduced to 8, and lockout attempts before lockout reduced from 12 to 5, 90-day password rotation. Two factor authentication was also another missing element in the previous policies as well as termination policies. After obtaining leadership input and comparing with available personnel resources, recommendations were presented, agreed upon, and set applied to the new policies.

Security Tools Procurement

The security tools procurement process was perhaps the most challenging phase of the project. Although there were no limitations as to possible solutions, the budget limitations for these tools was unclear and this led to many different possible courses of action. There were frequent requests for budget restrictions but it was not until all price quotes were presented that the budget was disclosed. The security tools procurement process focused on the major gaps in the current security controls for the organization. Listed below were the primary categories for security control requirements.

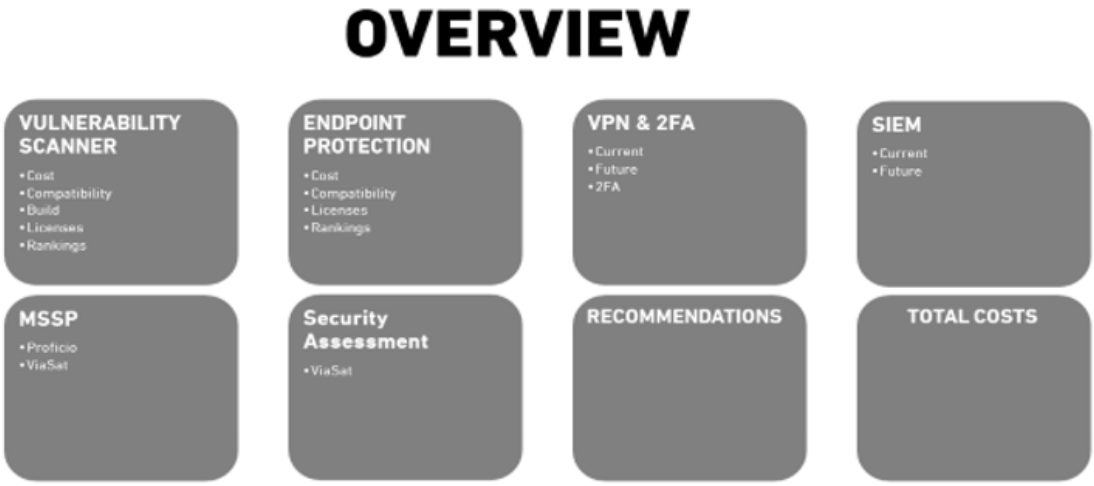


Figure 2- Overview of Security Tool Recommendations

This information in Figure 2 served as the overview slide for the executive board and was spoken to from left to and right and top to bottom.

Company “Y” provided monthly vulnerability scans, basic endpoint protection, a SIEM platform, security analysts, security assessments, firewall management, and IT policies. At the onset of the project it was made clear that all price quotes must be obtained using a third-party software reseller. Having a trusted software reseller streamlines the contract process through the legal department. If a software reseller isn’t used then the legal department is likely to red-line much of the non-disclosure agreement, statement of work, and product order which then adds considerable time before the security control can be implemented.

The same vetting process was applied for assessing each tool. Company “X” required that a third-party software reseller be used as the intermediary and many major software companies mandate the use of a reseller to complete the purchase process. The following quotes were obtained for each of the categories and presented to leadership with the recommendations. Due to the sense of urgency, the quoting process was simultaneously ongoing for all the categories. As part of the vetting process there were a number of crucial questions that needed to be answered. These questions concerned cost, licensing model, supported operating systems, contract length, installation support, server licensing, and known application compatibility issues. The typical licensing models encountered were per-seat or concurrent licensing. Per-seat is determined by assigned licenses regardless of how many are currently using the services (Bruin 2012). Concurrent licensing is based on how many users are using the services at the same time. A company can save considerable amount of money by purchasing based on concurrent licensing. The key here is to have previous usage data and accurate scalability plans. It is best to look at peak use, average use, and plans for growth. For a project, I based the number of concurrent licenses required by looking at the peak use over 24 hours in the last year and then adding 10% for scalability.

There were numerous vendor and architecture options for purchasing a vulnerability scanner. Licensing was based on the number of endpoints and service agreements could include managed or unmanaged. A managed vulnerability scanner would mean that an on-premise scanner would be installed and managed by the support company. Based on the limited resources at “X”, the most viable solution was managed services including outsourcing the setup and deployment of the on-premise appliance. Previously, “Y” had provided monthly vulnerability scans via email but no follow-up occurred and thus patching

became an afterthought. Due to limited human resources, only 1000 users, 900 laptops and 400 servers, the best purchasing option was to include the vulnerability scanner into a managed service security provider. This would negate the need for an on-premise scanner and would also include all scanner licenses as well as network traffic oversight by a team of security analysts. The results of the vendor shopping for a vulnerability scanner was presented as such:

VULNERABILITY SCANNER

	Qualys	Rapid7	Nessus (Tenable)
Cost	$28k Annual	$30k Annual	$51k with $45k Annual thereafter
Compatibility	Win, Mac, Linux	Win, Mac, Linux	Win, Mac, Linux
Build	Cloud	On-prem VM/Cloud	On-prem VM/Cloud
Licenses	1536	1500	1500
Rankings	1	2	3
Contract	1 yr	1 yr	1 yr
Vendor	SoftwareOne Proficio/Viasat –No on-prem scanner required	SoftwareOne	Evotek

Figure 3: Vulnerability Scanner Comparison

The chart provided in Figure 3 represents a comparison of vendor quotes based on cost, compatibility, appliance type, licenses, rankings, contract length, and third-part software reseller that obtained the quote.

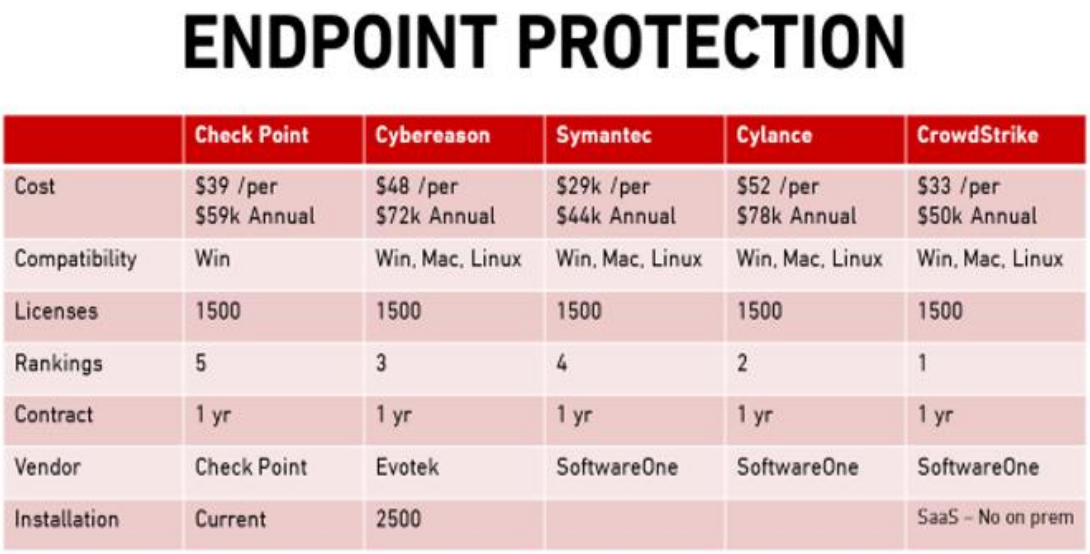
Endpoint protection had the most available solutions. So much so that my email inbox was inundated daily with EDR (Endpoint Detection and Response) startups looking for an opportunity to present their products. Ultimately the decision came down to cost, benchmark performance, and supported operating systems. “X” utilized Windows 7/8/10, Windows Server 2003/2008/2012/2016, Linux RedHat 5x/6x/7x, macOS High Sierra, and iOS 11. It was crucial to find one solution that could protect most, if not all, of the operating systems within the environment. The inconvenience of managing multiple endpoint contracts and solutions was not going to be worth the cost savings. Many vendors answered the supported operating systems question with “in development”, but this would not suffice because the control needed to be deployed as soon as possible. Ultimately, the recommendation was made

to pursue a contract with one of the leading products from the 2018 Gartner Report listed below:

Figure 4: Endpoint Detection & Response Solutions (Gartner)

Figure 4: 2018 Gartner Report for Endpoint Detection and Response solutions based on how they performed against the same benchmark tests evaluating detection capabilities.

A breakdown of the cost and feature comparisons for endpoint protection is listed below:



ENDPOINT PROTECTION

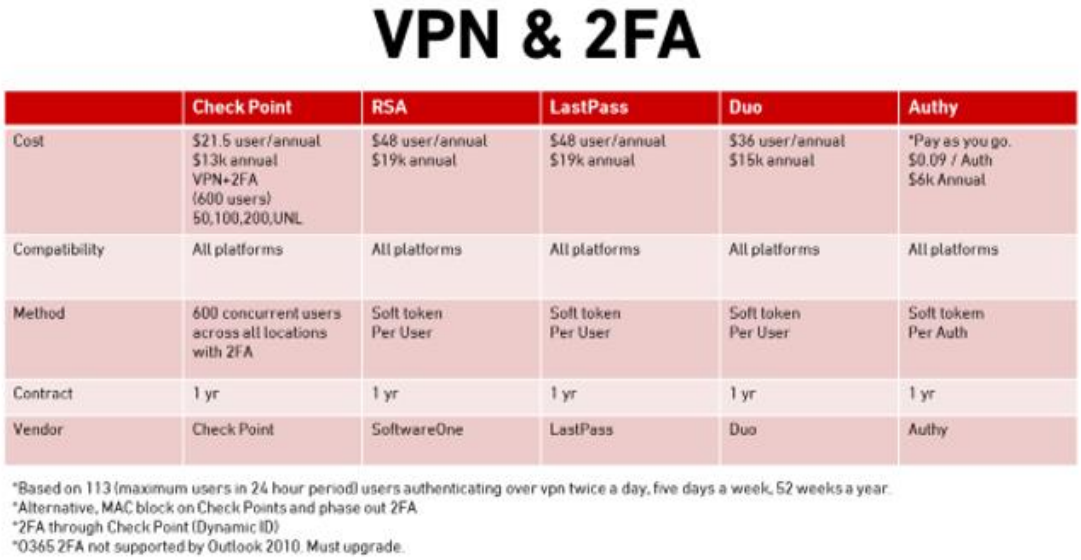
	Check Point	Cybereason	Symantec	Cylance	CrowdStrike
Cost	$39 /per $59k Annual	$48 /per $72k Annual	$29k /per $44k Annual	$52 /per $78k Annual	$33 /per $50k Annual
Compatibility	Win	Win, Mac, Linux	Win, Mac, Linux	Win, Mac, Linux	Win, Mac, Linux
Licenses	1500	1500	1500	1500	1500
Rankings	5	3	4	2	1
Contract	1 yr	1 yr	1 yr	1 yr	1 yr
Vendor	Check Point	Evotek	SoftwareOne	SoftwareOne	SoftwareOne
Installation	Current	2500			SaaS – No on prem

Figure 5: Endpoint Protection Solution Comparison

Figure 5: This chart compares the many different quotes that were obtained for endpoint detection and response solutions.

One of the pre-existing conditions when the project began was that the Proofpoint email filtering appliance managed by "Y" would be decommissioned and the Cisco ASA's used for VPN and authentication would also be decommissioned by May 1st. This meant that alternative VPN and multifactor authentication solutions needed to be vetted, purchased, tested, deployed, and validated by May 1st. The determination in this case came down to comparing per seat vs concurrent user licenses, support costs, and pre-existing business relationships between "X" and the vendor. Ultimately, the decision was made to go with Check Point firewalls that have all of the capabilities needed wrapped into one: email attachment scanning, Intrusion Prevention System, Anti-bot, Anti-spam, Data Loss Prevention, and VPN with Multi Factor Authentication (Check Point 2018). An additional selling point was the high marks that Check Point technology received in the Gartner 2018 ratings for Unified Threat Management. A cost breakdown of considered multifactor authentication solutions is listed below. MFA capability is integrated into the Check Points

and only requires a nominal fee to activate. By not having to integrate a different third-party MFA solution, we were able to eliminate the chance of having compatibility issues between the Check Point firewalls and a non-Check Point MFA solution.



VPN & 2FA

	Check Point	RSA	LastPass	Duo	Authy
Cost	$21.5 user/annual $13k annual VPN+2FA (600 users) 50,100,200,UNL	$48 user/annual $19k annual	$48 user/annual $19k annual	$36 user/annual $15k annual	*Pay as you go. $0.09 / Auth $6k Annual
Compatibility	All platforms	All platforms	All platforms	All platforms	All platforms
Method	600 concurrent users across all locations with 2FA	Soft token Per User	Soft token Per User	Soft token Per User	Soft token Per Auth
Contract	1 yr	1 yr	1 yr	1 yr	1 yr
Vendor	Check Point	SoftwareOne	LastPass	Duo	Authy

*Based on 113 (maximum users in 24 hour period) users authenticating over vpn twice a day, five days a week, 52 weeks a year.
*Alternative, MAC block on Check Points and phase out 2FA
*2FA through Check Point (Dynamic ID)
*O365 2FA not supported by Outlook 2010. Must upgrade.

Figure 6: VPN & 2-Factor Authentication Comparison

Figure 6: This chart compares the cost, compatibility, methods of use, contract, and third-party reseller, for multifactor authentication providers.

Security Information and Event Management products and services are a way to provide real-time analysis of security alerts and events across a platform. The logs required can be imported from network devices, systems, and applications and be tailored based on business needs. These alerts could be system errors, password attacks, malicious software, command and control activity, and a plethora of other nefarious activities. Unfortunately, implementing an on-premise Security Information and Event Management (SIEM) was quickly ruled out as a viable option because of the dedicated security engineers that are required to manage a SIEM.

An excellent alternative is to use a MSSP which can be contracted to either manage an on-premise SIEM and monitor alerts or to allow access to a custom SIEM managed by the MSSP (Pratt 2017).

Early in the project it was identified that a replacement for security services provided by “Y” was needed. Once leadership accepted this requirement, communication between “X”, third-party reseller, and possible MSSP solutions began. Ultimately the decision was made to go with the lowest cost solution that required the least onboarding and could provide the requisite levels of coverage and who agreed to locking in a price for multiple years.

Security penetration tests are conducted to identify unknown weaknesses in networks, systems, and applications. These weaknesses can be caused by poor coding practices, inadequate business processes, and poor network design. Early exploratory questioning at “X” uncovered that neither penetration testing nor secure coding principles were a common practice at the business. The secure coding principles would have to be a later initiative as the implementation would require extensive leadership buy-in, planning, and integration. The penetration could be finished from concept to product in a much short period. Two weeks for the administrative process and two weeks for the penetration test based on the size of the infrastructure and scope of the test. By the end of the project the plan for the penetration test was to have a narrow scope test against public facing endpoints and then a broader scope test focusing on critical assets once the physical divestiture between “X” and “Y” was complete. There were a few reasons behind having multiple tests in a short period and annual penetration tests. One concern was that scans and attacks could inadvertently target and effect “Y” because there was still a shared IP addressing, federated trust, and share network architecture. Another concern was that the results would be null and void because there was an ongoing server migration and decommissioning initiative ongoing and the network architecture was scheduled for major changes in the future. Vulnerabilities and misconfiguration findings may have no value if the platform is going through major changes. There was also a cost savings because there would be less servers to test in the future. Therefore, leadership made the decision to only test the publicly available endpoints at first and then target the internal environment once the initiatives were complete and the platform was closer to a final state.

User Training

As part of the internship I attended the new employee cyber awareness training. Part of the project was to assess the current training, provide recommendations, and then take over the new hire cyber training as well as annual security training. The training was previously

instructed by the physical security manager. This was a bit surprising as the presentation was partitioned for 75% physical security and 25% information security. The slides and data were outdated as well. There was no annual training requirements and no attendance accountability for the course. Many new hires would be on the job for months before attending the training because the organization wanted to have enough new hires to fill a course before scheduling. By the end of the project, I had revamped the new hire security awareness slides, implemented cyber notes into the weekly email bulletin, posted security awareness bulletins around the company, and developed a plan for annual training requirements for the future. ESET has a free cyber awareness training presentation that provides an excellent framework for developing your own corporate training and has interactive lessons as well (ESET, 2018).

The final product presented to senior leadership prior to going forward with the purchasing process is shown below:

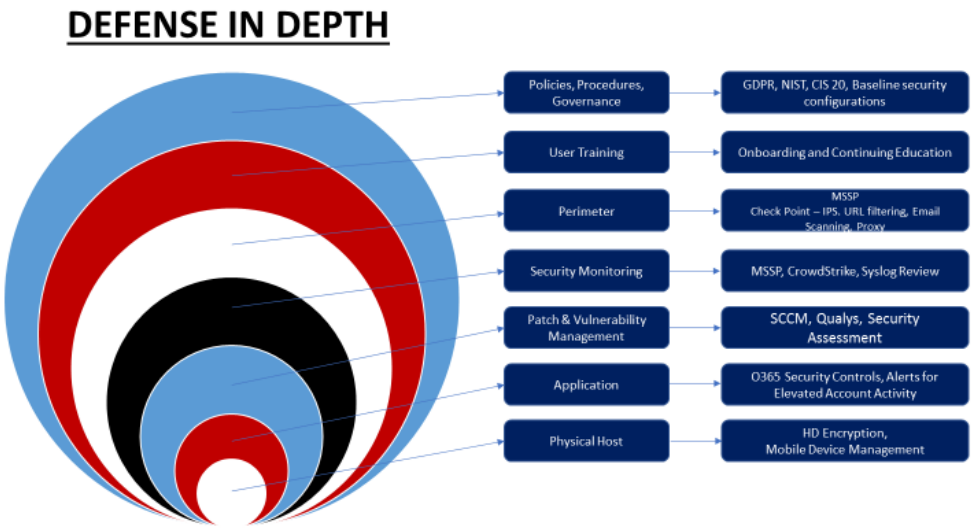


Figure 7: CIS Top 20 Security Control Implementation

Figure 7: This was the final slide that represented CIS 20 security control implementation

SECURITY REQUIREMENTS

"Y" Provided

Product
24x7 CSIRT (includes Vulnerability Scanning)
Endpoint Protection: McAfee, Windows Defender
Security Assessment: None

2018 Budget
Security: $XXX,000
RSA Tokens: $31,500

"X" Option

Product	Cost
MSSP (includes Qualys)	$69k Annual ($4600 setup)
Endpoint Protection: Crowdstrike	$50k Annual
Security Assessment: NDA	~$50k (Pending quote)
Check Point VPN: 600 Licenses	$XXk Annual
Total	$XXXk First Year +30k Option NDA

Figure 8: Security Products Comparison

Figure 8: These charts compare the security products and services that "Y" provided to "X" that would be terminated by May 1, 2018.

TOTAL COSTS

OPTION 1

Product	Cost
Vulnerability Scanner:	$XXk Annual
Endpoint Protection:	$XXk Annual
Security Assessment: NDA	~$XXk (Pending quote)
Check Point VPN: 600 Licenses	$13k Annual
Total	$XXXk First Year $XXXk reoccurring annual

OPTION 2

Product	Cost
MSSP incl. Vulnerability Scanner:	$XXk Annual ($4600 setup) $XXk Annual
Endpoint Protection:	$XXk Annual
Security Assessment: NDA	~$XXk (Pending quote)
Check Point VPN: 600 Licenses	$13k Annual
Total	$XXXk Annual

Figure 9: Recommended Actions

Figure 9: These charts represent two recommended courses of action that were presented to the executive board. Option 2 was the unanimous choice.

Although the project is complete based on the end of the internship, many of the initiatives are purchased and scheduled to be implemented in the future such as the broad scope penetration test, MSSP support, and cloud security features. The relatively short period of time for the internship meant that some initiatives would only be a conceptual product and not entirely in place by the end of the internship. If this is verbalized to senior leadership at the very beginning of the project then expectations can be managed. Regardless of the security controls in place when first stepping into a new environment, CIS 20 provides a great framework to conduct quick assessments of what baseline protections are missing. Once the baseline security controls are in place then a more granular security focus can be taken.

References

Bharania R., Nelson C. Risk Triage and Prototyping in Information Security Engagements. 2017 [accessed 2018 March 20]. Cisco. Retrieved from https://www.cisco.com/c/en/us/about/security-center/risk-triage-whitepaper.html.

Bruin C. Concurrent User vs. Per Seat Licenses – The Analogy: Concurrent User Licensing Saves You Time, Money and Hassle. 2012. MicroPact Blog. [accessed 27 February 2018], https://www.micropact.com/blog/detail/concurrent-vs.-per-seat-licenses-the-analogy.

Cybersource. PCI-PAL. 2018 [accessed 2018 March 15]. https://www.cybersource.com/solutions/merchant/integrations_partnerships/pci_pal/

DHS. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies: Industrial Control Systems Cyber Emergency Response Team. 2016. [accessed 2018 April 10]. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

ESET. Cybersecurity Awareness Training: A short walkthrough. 2018 [accessed 2018 April 5]. https://www.eset.com/us/cybertraining/.

Gonzales D, Kaplan JM, Saltzman E, Winkelman Z, Woods D. Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," in IEEE Transactions on Cloud Computing. 2015; 5: New Jersey.

Grachis G. Critical IT Policies You Should Have in Place. Putting a framework of IT policies that should be the foundation of every company's security plan. 2016. [accessed 2018 January 22]. https://www.csoonline.com/article/3074825/leadership-management/critical-it-policies-you-should-have-in-place.html.

Nadeau M. General Data Protection Regulation [GDPR] requirements, deadlines and facts. 2018 [accessed 2018 March 1]. https://www.csoonline.com/article/3202771/data-

protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.

Pratt M. What is SIEM software? How it works and how to choose the right tool. 2017 [accessed 2018 January 25]. https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html.

Vanderburg E. Information Security Compliance: Which regulations relate to me. TCDI Blog. 2018. [Accessed 2018 Mar 22]. https://www.tcdi.com/information-security-compliance-which-regulations/.