USF | Muma Case Review
A publication of the Muma College of Business | University of South Florida

Volume 5 Number 5 1 JUNE 2020

GARY HOLLAND, CHELSEA NAUTA, RYAN PUSINS, ALBERTO SOCORRO, CHRIS TEODORSKI

TECHGENICS' DATA SECURITY COMPLIANCE[1]

"This is bad, really bad," Jay Santos thought to himself. An email from Microsoft greeted him first thing in the morning with news of several new vulnerabilities, many that the software manufacturer had rated as critical. What troubled Jay was that the vulnerable software subsystem was the remote desktop protocol (see Exhibit 1). The use of this protocol was ubiquitous across the Microsoft using world to manage fleets of Windows servers. As was typical of recent large-scale vulnerability (see Exhibit 1) notifications, this one too had been given a clever name, Deja Blue. Microsoft named it thus because it followed closely on the heels of a previous critical vulnerability in the same subsystem called BlueKeep.

Jay was the duty handler that week for Techgenics' Emergency Vulnerability Management Program. This meant that it was his responsibility to herd the various system owners and get them to patch as quickly as possible. Given that this vulnerability had just been released and the vendor had confirmed no active exploit code (see Exhibit 1) was available, convincing them to take a business disrupting reboot might be difficult.

The Vulnerability Management team had been leveraging a combination of both off-the-shelf and homegrown tooling (see Exhibit 1) to deliver their services. At the core of their tooling was a database that contained all of the vulnerability information for the entire enterprise. This database and the interface to it had implemented role-based access and discrete permissions to the data, but ultimately the database was supported by a potential team of dozens of IT support people, both onshore, offshore, United States citizens and foreign nationals. The sensitivity of this data was not lost on either Jay or his manager Dean Wheeler. If this data was to land in the hands of a malicious actor, it would be a virtual roadmap and how to guide to compromising Techgenics.

Right before the announcement of Deja Blue, Jay's manager, Dean, had informed Jay that the program was going to be underfunded. While the business understood the criticality of the program, the full budget request was going to be denied. The vulnerability team was, however, still expected to continue to deliver the same level of service to the business and with an expansion of the business into the Federal space, the data store had to be brought into compliance with the Federal Risk and Authorization Management Program (FedRamp). How would they deliver these critical controls while still staying within their now reduced budget?

[1] Copyright © 2018, *Chris Teodorski, Alberto Socorro, Chelsea Nauta, Ryan Pusins, Gary Holland.* This case was prepared for the purpose of class discussion, and not to illustrate the effective or ineffective handling of an administrative situation. Names and some information have been disguised. This case is published under a Creative Commons BY-NC license. Permission is granted to copy and distribute this case for non-commercial purposes, in both printed and electronic formats.

Editor: Grandon Gill

Data Security Industry

Prior to Jay Santos's challenge to improve Techgenics Vulnerability Management Program, data security had become increasingly important throughout both public and private industries. The vulnerability team was considering many perspectives in making their decision on what to do next. Cost was certainly in consideration, but the security of the data was highly important. It was critical to understand the data security industry and what risk the ultimate decision would take on. While certain types of attacks were more common in some industries, no industry was immune to cybercrime. Exhibit 2 showed a variety of different types of cybercrime incidents across different industries. Companies across all industries were being challenged to protect computers, networks, programs and data from unauthorized users. As hackers increased their attack sophistication, the demand for improved prevention and protection protocol increased. Several key factors had been considered when Techgenics and alike companies evaluated their data security protocol including the tools they used, the people who used them and their cost. These factors were considered when Techgenics considered preventing attacks, managing an attack and recovering from one. Santos found the experiences of four unrelated technology companies to be particularly instructive.

AT&T

When AT&T purchased cybersecurity company AlienVault and their technologies, they were able to offer a comprehensive security management platform to its customers. They utilized the AlienVault Unified Security Management Platform (USM) that was updated every 30 minutes with data from the Open Threat Exchange (OTX). The USM appliance combined SIEM (security information and event management) and log management capabilities. Exhibit 3 showed AT&T's AlienVault Dashboard that their customers utilized for data visualization. They also offered asset discovery services, vulnerability assessments, and intrusion detection services. AlienVault was most appropriate for security teams between 1-20 employees, however, their reach was worldwide with over 7,000 customers across over 140 countries. AlienVault customers enjoyed comprehensive functionality at a low cost compared to the competition. Their pricing model was a simple subscription model offered at three different levels, Essentials, Standard and Enterprise. Because AlienVault was available as a cloud-based or on-premise hardware appliance, it could have been adapted to monitor cloud-based or on-premise environments. Critics noted that AlienVault lacked some of the advanced analytics functionalities that were necessary for larger, enterprise-level companies.

AT&T's AlienVault provided valuable perspective that Santos considered. The fact that the data was updated frequently and regularly gave AT&T customers high confidence that the data had high integrity and wasn't out of date.

BlackBerry

BlackBerry's cybersecurity offering was backed by the Cylance endpoint detection and response (EDR) platform. Cylance, the California-based startup company, utilized artificial intelligence, algorithmic science, and machine learning to predict, detect and prevent security incidents. While other cybersecurity companies relied on human-generated data, Cylance customers enjoyed the ability to combine AI/ML with vast datasets that generated automated feedback. This platform also allowed customers to prevent unknown (zero-day) threats, unlike other companies. The Cylance EDR was deployed across 14.5 million endpoints across large private companies as well as government entities. Exhibit 4 showed the dashboard end users used to see their device security level. Cylance gained praise from the FBI after they successfully uncovered a cyberwar operation carried out by the Iranian government called Operation Cleaver. This history showed that Cylance had been a successful security partner within the public sector.

By understanding BlackBerry's offering, Santos' team recognized the value of a robust and data centric model. The end users of Techgenics' data needed to feel confident that the data was well protected, that integrity had been maintained and that they could rely on that data being available when it was needed.

Cloudflare

Cloudflare had led the Content Delivery Network (CDN) market and offered a platform that provided security to IoT (Internet of Things) devices. They served both the private and public markets protecting websites, mobile devices, application programing interfaces or APIs (see Exhibit 1), Software as a Service (SaaS) services and other devices connected to the internet. Exhibit 5 showed the Cloudflare IoT device authentication process. Based in San Francisco, California, with offices in London, Munich and various US cities, they served customers across 194 cities in more than 90 countries. By having leveraged the Google Cloud infrastructure, customers experienced reduced latency. In addition, Cloudflare technology protected customers against distributed denial-of-service (DDoS) attacks and data breaches. Their tools blocked unauthorized users from gaining access through authentication and monitoring. Customers enjoyed a simple cost structure that scaled from small to large companies. Customers signed up for any one of four different plans; free, professional, business, and enterprise all priced as a monthly subscription model. There were also add-on features available for all plans for an additional monthly cost. Cloudflare supported both a cloud-based and an on-premise environment.

Cloudflare's ability to deliver an always-on service was a model for Santos' team to consider. When looking at the possibility of deploying to a third-party outsourcer, they had to be sure that the outsourcer could achieve uptime similar or better than what Techgenics could provide internally.

Idaptive

Idaptive was a unique competitor when compared to its peers in that was a spinoff of a larger company, Centrify, instead of being acquired by a large corporation. Idaptive Nex-Gen Access platform offered solutions including single sign-on (SSO), multi-factor authentication (MFA), enterprise mobility management (EMM) and user-behavior analytics (UBA) to customers with a zero-trust approach. Exhibit 6 showed the dashboard end users used to see their device security. Idaptive customers spanned across the globe including over 1,300 users, 515 devices and 329 apps. Idaptive partnered with various MSP (managed service providers) that helped increase their presence across the cybersecurity landscape. Their pricing model was simple, which allowed the customer to choose between standard and advanced models across their service offerings. These models were a monthly subscription like many of their competitors.

By understanding the history of Idaptive and recognizing their success, Techgenics saw a future partnership with Idaptive as an example of a successful partnership with a smaller company. They also appreciated the zero-trust approach Idapative took since this was mission critical to their work and provided a good model for data security.

Understanding the cyber security landscape helped Techgenics understand the risk involved with making a decision on how to handle their Vulnerability Management Program. AT&T, Blackberry, Cloudflare and Idaptive were a few of the cybersecurity industry examples that showcased how technology, processes and systems could ultimately impact the security of a company's data. If Techgenics decided to keep things in-house, outsource to a third party or find a partner, they could make a more educated decision by understanding the security of these options.

Techgenics

Computer science and technology created many challenges and opportunities for the corporate world. Many times, one discovery that solved a critical item created the need for other tools and options to make that new discovery successful. With these solutions, a need was discovered for an efficient way to communicate within an organization for corporations to capitalize on the utilization of updated technology. For an organization to maintain a competitive edge, it had to be able to communicate effectively and securely beyond the confines of the organization.

In the early 1990's, Beauregard Bossier and Thibodaux Acadia worked together at an industry-leading information technology services company. Bossier and Acadia watched as this company struggled to implement solutions within budget and on increasingly aggressive timelines to meet customers quickly growing demands. Both were confident that they could apply their expertise and experience to offer services that could meet these demands.

From these brilliant yet humble beginnings, Techgenics was created. Bossier and Acadia, saw their business grow very rapidly during the 1990's as the dotcom era saw the explosion of technology and the introduction of the Internet as a core piece of almost all businesses. The growth of Techgenics was explosive. Although they started in New Orleans, Louisiana, they quickly saw the expansion of their business to serve the entire East Coast of the United States and, in a limited fashion, some of the midwest.

Initially, Techgenics was a managed service provider, providing implementations, post-implementation support, and consulting for traditional IT systems, including Enterprise Resource Planning (ERP) Systems, E-mail, collaboration systems, and document management systems. Their reputation for delivering on a budget quickly enabled them to expand beyond these offerings. In the late 1990's and very early 2000's they branched out into providing similar support to networking, including implementing routers, switches, and firewalls.

After the attacks on the United States on September 11th, 2001, Bossier and Acadia saw the opportunity to expand into the information security realm. They began to offer vulnerability assessments, penetration testing, SIEM (Security Incident and Event Management) implementations, and a full suite of compliance offerings, including Sarbanes-Oxley support, Payment Card Industry Data Security Standard (PCI-DSS) and the Health Insurance Portability and Accountability and Health Information Technology for Economic and Clinical Health Act (HIPAA HITECH) audits.

Techgenics was recognized in the eastern United States as one of the best places to work. Techgenics regularly appeared on "Best Places To Work" lists and this was a recognition that Techgenics took great pride in and invested resources to maintain.

Acquiring and retaining talent in the technology industry required a prowess that many companies could not grasp. Techgenics had to become a leader in employee satisfaction in order to provide the products and services that were needed. The competition was growing as the technology boom created a frenzy of subject matter experts that flooded the job market. This was when Techgenics was recognized as a leader in talent acquisition. As technology changed, the need for a more educated, capable, and skilled workforce became even more prevalent. Techgenics rose to the challenge and attracted one of the most talented workforces in the industry. Techgenics was also recognized in the industry as one of the highest-ranked companies for talent acquisition and retention.

In 2015, Bossier and Acadia stepped away from the day to day operations of Techgenics, to pursue opportunities as angel investors. They had built Techgenics into a successful, full-service managed service provider (MPS) with $4.4 billion dollars in revenue in 2014. Identifying customer needs and constant innovation positioned Techgenics as a critical piece in nearly every major industry. Consumer's needs seemed to be changing at the same pace as technology as they became more dependent and demanded efficiency. Industries such as education, energy, financial services, government, healthcare, hospitality, insurance, manufacturing, retail, sports and entertainment, transportation and even communities created exponential opportunities for Techgenics. These industries understood that they must, at minimum keep up or become obsolete.

Explore the Technology

Computer Economics stated that "In 2018, only 9.4% of the average IT budget for major corporations were allocated to outsourcing, which is lower to the 2017 figure of 11.9%. This is due to IT organizations relying on their in-house talents to meet service goals, with these reasons also factoring in." Could this be a viable solution for Techgenics? Why had Techgenics depended for so many years on offshoring their DBA support? Offshore outsourcing was a strategic practice in which a business hired a third-party supplier to perform work in a nation other than the one in which the hiring business primarily conducted its operations. One benefit of this was cost savings. But there were many risks associated with it, including compliance; Techgenics faced a problem with foreign nationals encountering saved data.

Some of the technology used at Techgenics consisted of:

- Python is an interpreted, high-level, general-purpose programming language. Python's design philosophy emphasizes code readability with its notable use of significant whitespace. Its language constructs and object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects. Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including procedural, object-oriented, and functional programming. Python is often described as a "batteries included" language due to its comprehensive standard library

- Python was used to create API's intended to simplify the building of client-side software. More importantly Techgenics used these API's in REST, (REpresentational State Transfer). It is an architectural style for distributed hypermedia systems and was first presented by Roy Fielding in 2000 in his famous dissertation. Like any other architectural style. One of the key advantages of REST APIs is that they provide a great deal of flexibility. Data is not tied to resources or methods, so REST can handle multiple types of calls, return different data formats and even change structurally with the correct implementation of hypermedia. There are 6 principles of Restful API Client-Server:

    1. There should be a separation between the server that offers a service, and the client that consumes it.

    2. Stateless: Each request from a client must contain all the information required by the server to carry out the request.

    3. Cacheable: The server must indicate to the client if requests can be cached or not.

4. Layered System: Communication between a client and a server should be standardized in such a way that allows intermediaries to respond to requests instead of the end server, without the client having to do anything different.

5. Uniform Interface: The method of communication between a client and a server must be uniform.

6. Code on demand: Servers can provide executable code or scripts for clients to execute in their context. This constraint is the only one that is optional.

- Flask has its strengths. Flask was built with scalability and simplicity in mind as a Web Server Gateway Interface (WSGI) application framework. Flask applications are known for being lightweight, mainly when compared to their Django counterparts. Flask developers call it a microframework, where micro (as explained here) means that the goal is to keep the core simple but extensible. Flask won't make many decisions for us, such as what database to use or what template engine to choose. Lastly, Flask also has extensive documentation that address everything that developers need to start. It was designed to make getting started quick and easy, with the ability to scale up to complex applications. It supported Jinja2 templating and secure cookies and was 100% WSGI 1.0 compliant. Flask became one of the most popular Python web application frameworks used in Techgenics. It's key in the creation and use of REST API's Building web services with Flask is surprisingly simple, much simpler than building complete server-side applications. There are a couple of Flask extensions that help with building RESTful services with Flask. Being lightweight, easy to adopt, well-documented, and popular, Flask is a very good option for developing RESTful APIs (see Exhibit 7).

- Oracle Database was a relational database management system (RDBMS) from the Oracle Corporation. Originally developed in 1977 by Lawrence Ellison and other developers, Oracle DB is one of the most trusted and widely used relational database engines (see Exhibit 8).

> The system was built around a relational database framework in which data objects could be directly accessed by users (or an application front end) through structured query language (SQL). Oracle was a fully scalable relational database architecture often used by global enterprises, which managed and processed data across wide and local area networks. The Oracle database had its own network component to allow communications across networks.
>
> A key feature of Oracle was a split architecture between the logical and the physical. This structure meant that for large-scale distributed computing, also known as grid computing, the data location was irrelevant and transparent to the user, allowing for a more modular physical structure that could be added to and altered without affecting the activity of the database, its data or users. The sharing of resources in this way allowed for very flexible data networks whose capacity could be adjusted up or down to suit demand, without degradation of service. It also allowed for a robust system to be devised as there was no single point at which a failure could bring down the database, as the networked schema of the storage resources meant that any failure would be local only.
>
> Techgenics relied on Unified Computing System (UCS) Servers, which helped change the way IT organizations did business. Its combined industry-standard, x86-architecture

servers with networking and storage access into a single unified system. UCS increased productivity, reduced total cost of ownership, and improved data center scalability.

- Qualys Scanners to ensure quality. These scanners quickly determined what was running in different parts of the network. The system uncovered unexpected access points, web servers and other devices that could leave the network open to attack. Qualys also continuously scanned and identified vulnerabilities with Six Sigma (99.99966%) accuracy, protecting IT assets on-premises, in the cloud and mobile endpoints. Its executive dashboard displayed an overview of security posture and access to remediation details.

  As enterprises adopted cloud computing, mobility, and other disruptive technologies for digital transformation, Qualys VM offered next-generation vulnerability management for hybrid IT environments whose traditional boundaries had been blurred. With its fast deployment, low Total Cost of Ownership (TCO), unparalleled accuracy, robust scalability, and extensibility, thousands of organizations relied on Qualys VM throughout the world (see Exhibit 9, 10, 11 & 12).

- Techgenics depended on the services of Remote DBA (Database Administrators) support for these servers. DBAs used specialized software to store and organize data. The role included capacity planning, installation, configuration, database design, migration, performance monitoring, security, troubleshooting, as well as backup and data recovery

Techgenics Insider Insights

Techgenics had an official enterprise-wide Vulnerability Management (VM) program for over five years and that program had reached a significant maturity level. This program included vulnerability discovery and reporting for the entire Techgenics enterprise and offered additional support to ensure product vulnerabilities were discovered and managed. Data collected by the Vulnerability Management team was enriched and custom risk ratings were applied to each vulnerability. Those scores and metrics were rolled up into an executive-level presentation that is presented to the leadership every quarter (see Exhibit 13, 14).

The Vulnerability Management program had grown organically over the years. The new software had been written to support the various reporting requirements that had been established by management. In some cases, this meant developing a dashboard to show the compliance of the business. In other cases, it meant exposing an Application Programming Interface (API) that allowed the businesses to pull the data themselves and develop custom reports.

Jay Santos was hired to manage the Vulnerability Management team's DevOps program. DevOps was a set of practices that looked to bring the disciplines of software development and system administration together (see Exhibit 15). The goal of this merger was to create a culture of collaboration between teams that historically functioned in distinct siloes.

Santos's team had been tasked with modernizing the program and getting it in line with more modern computing practices, including integration into the continuous integration/continuous development pipeline, eliminating the dependence on physical hardware, support of Docker containers as scanning targets, and better control of access to the vulnerability data.

Santos's manager, Dean Wheeler had previously submitted a large budget request to support the effort of modernizing the vulnerability management program. However, in the middle of the budget cycle, Wheeler learned that most of the budget for this effort had been pulled back. When that information reached the team, the assumption was that this project would be pushed back in priority. However, after a strategy meeting with the executive leadership team, Wheeler was informed that this effort was a core piece of the organization's efforts for that year. Specifically, the business had decided to use FedRamp as their compliance baseline, which meant bringing all systems in line with FedRamp controls.

The organic growth of the program meant that much of the infrastructure the team utilized was supported by teams outside of the vulnerability management team. Several of the various sister teams in the organization, including the Incident Response Team (IRT) and Enterprise Delivery Team (EDT), had allowed the VM team to piggy-back on their infrastructure. The relationship between these teams had historically been symbiotic. However, the reorganization had resulted in the VM team reporting to a different management structure than the other two teams, which made sharing resources more challenging.

The Decision

The data management issue was multi-faceted with far-reaching implications no matter which path was chosen. With some of the data stored in locations outside of the US, could Techgenics continue to fulfill government contracts that restrict or prohibit foreign nationals from accessing this information, without a major overhaul (Exhibit 16)? More importantly, was Techgenics putting future business at risk by having a database with a single point of failure in the hands of foreign nationals?

It seemed an acceptable alternative was to utilize a DBA to manage all this data. This, of course, led to different questions. Who would this DBA work for? Jay and his team didn't have enough work for a full-time DBA. Could they use a DBA from another team or potentially a third-party contractor? Where would Jay and his team fall in the priority list if the DBA didn't work exclusively for their team? Could Techgenics even afford to allow lapses in data management?

Lastly, it was clear that Jay and his team were going to be constrained by the available funding as set forth by Techgenics. Could Jay deliver an acceptable solution that limited the risk to Techgenics without putting a full-scale solution in place? Would this solution even appease his bosses if it required additional work down the road? Maybe the right answer was waiting for additional funding so he could do the solution right, but how long could Jay and Techgenics wait before it was too risky?

Jay knew that a decision needed to be made quickly. He had a meeting with his Manager, Dean to discuss the path forward but also new vulnerabilities were being published every day and Jay and his team needed to have a solution in place to manage all this data so they could concentrate on the important task of vulnerability response. So, what was the right way to proceed:

- **Do Nothing.** This was the most cost-effective solution but also increased the liability risk to Techgenics as well as putting the future business at risk.
- **Hire a Full-Time DBA.** This enabled Techgenics to maintain their federal database requirements and thus federal contracts. It also allowed Jay and his team full control of the DBA and ensured responsiveness. However, it was the most expensive option and was still a single point of failure. A full-time experienced DBA when factoring in benefits would cost Techgenics around $200,000 per year.

- **Cost-share a DBA with another Techgenics business element.** This would reduce the cost to Techgenics while still ensuring compliance with the federal requirements and reduced risk to future business. A timeshare did mean that sometimes the DBA would be unavailable to assist Jay and his team potentially during periods when timeliness was crucial. Depending on the amount of effort dedicated to support Jay's database needs, this cost sharing would cost Jay's department between $45,000 and $75,000 per year.

- **Outsource database management to a third-party that still meets federal requirements.** This was initially cost-effective and had the added benefit of eliminating database maintenance costs, but frequent changes to the data could prove costly as administrator time was charged at a premium. Additionally, Techgenics would lose all control over the DBA and would instead be in a queue and have their requests handled when the DBA got around to them. Depending on the service level agreements, this would cost the Techgenics between $96,000 and $120,000 per year.

What was clear to Jay and his team was that this issue needed to head down the right path. Picking the wrong option would have expensive consequences later. This mindset helped eliminate options such as foreign third-party vendors and implementing lower FedRamp certifications. Maintaining that mindset would help Jay and his team manage both the expectations of Techgenics and FedRamp while working within their budget.

References

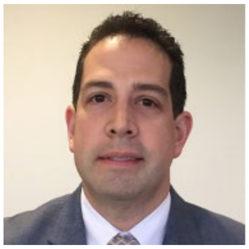
Nasdaq. (2018, June 25). *Cybersecurity: industry report & investment case*. Retrieved 2019, from https://business.nasdaq.com/marketinsite/2018/GIS/Cybersecurity-Industry-Report-Investment-Case.html

Biographies

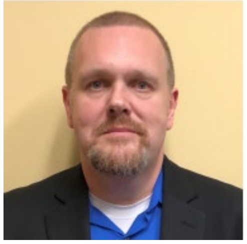
Gary Holland is on the move. Fresh from completing a very intensive educational program that encompassed studying for and passing three difficult state law exams and a general securities representative exam, the investment rep is setting his sights on an Executive MBA. The culture of the business world, he says, requires leaders and executives to have an MBA. Passing those self-study exams meant he has completed the USAA Financial Advice Services Group training program. He credits those around him for their support, the same support he will have while he is involved in the Executive MBA program. Holland has 29 years of work experience, with 25 in management positions and has been an investment representative with USAA for a year. He says the Executive MBA program will provide the skills, critical knowledge and ability to benefit his corporate journey. He also hopes to expand his network of professional colleagues, relationships he expects will last a lifetime. Holland received a bachelor’s degree in business administration from Argosy University in Tampa.

Chelsea Nauta shifted gears soon after graduating college less than a decade ago. She had been a collegiate swimmer and pursued a career after graduation as a professional swimmer but made a career decision after the Olympic Trials in 2012. She decided to follow a path to medical school but discovered that clinical medicine was not all that appealing. Through her associates, she found the career she now is all in on. She is an account executive with Greenway Health, a company that provides support to medical practices through software and services. Her responsibilities include management of 85 medical practices in which she develops annual and quarterly business plans and visits to offer support. She provides weekly and monthly forecast budget numbers to Greenway Health sales vice presidents and the chief financial officer and offers advice on how to strengthen the sales and marketing efforts. Nauta received a bachelor’s degree in biology with a minor in Spanish from the University of Georgia and a graduate certificate in business administration from USF.

Ryan Pusins is a 20 year veteran of the United States Marine Corps. Throughout his career he has had the opportunity to shape lives at home and abroad through his transformational leadership and mentorship capabilities. Ryan’s primary job with the Marines is a helicopter instructor pilot but he also speciallizes in Logistics, Maintenance Administration and Quality Control, and Aviation Safety. Ryan has earned a Masters Degree in Public Administration from Florida Gulf Coast University to compliment his USF Undergrad in Elementary Education. He will soon be joining the faculty of Rensselaer Polytechnic Institute where he will continue to in his service as the Executive Officer for the Naval Reserve Officer Training and Associate Professor.



Alberto Socorro saw a need in 2011 and did something about it. He is the founder and director of Recovery Services of Tampa Bay, a nonprofit that provides supportive housing for persons with disabilities. The model gives each person a private room while sharing a common area. Costs are kept at a minimum through a series or relationships with both private and public agencies. Currently, Recovery Services of Tampa houses 40 men and woman, who would be living on the streets, if not for the work of the nonprofit. He says pursuing an Executive MBA does more than open up opportunities for him; it will give him the tools to better represent himself professionally, especially when addressing community members for donations or loans, a vital aspect to the growth of Recovery Services of Tampa Bay. It also makes him a role model for his children, teaching them how important education is and that anything is possible through hard work and commitment. Socorro received a bachelor's degree in business analytics/information systems from USF.



Christopher Teodorski is a 20+-year veteran of the IT industry. He is the first to admit that everything he knows about business, he learned while on the job. Priot to starting his MBA, he had no formal business training and recognizes that has been a limiting factor in his career. He is pursuing his Executive MBA to fill in those gaps. He was promoted to a people manager because of his strong technical capabilities coupled with his leadership ability. Teodorski received a bachelor's degree in English literature from Indiana University of Pennsylvania and a master's degree in information security and assurance from Robert Morris University in Pennsylvania. His hobbies include combat robotics and amateur radio. His call sign is KB3VCJ and he holds the highest FCC amateur radio license, known as the Amateur Extra.

Exhibit 1: Technical Glossary

Protocol: A network protocol defines rules and conventions for communication between network devices. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into sent and received messages.

https://www.lifewire.com/definition-of-protocol-network-817949

Vulnerability: A computer vulnerability is a cybersecurity term that refers to a defect in a system that can leave it open to attack. This vulnerability could also refer to any type of weakness present in a computer itself, in a set of procedures, or in anything that allows information security to be exposed to a threat.

https://enterprise.comodo.com/blog/computer-vulnerability-definition/

Exploit Code: An exploit is any attack that takes advantage of vulnerabilities in applications, networks, or hardware. They usually take the form of software or code that aims to gain control of computers or steal network data.

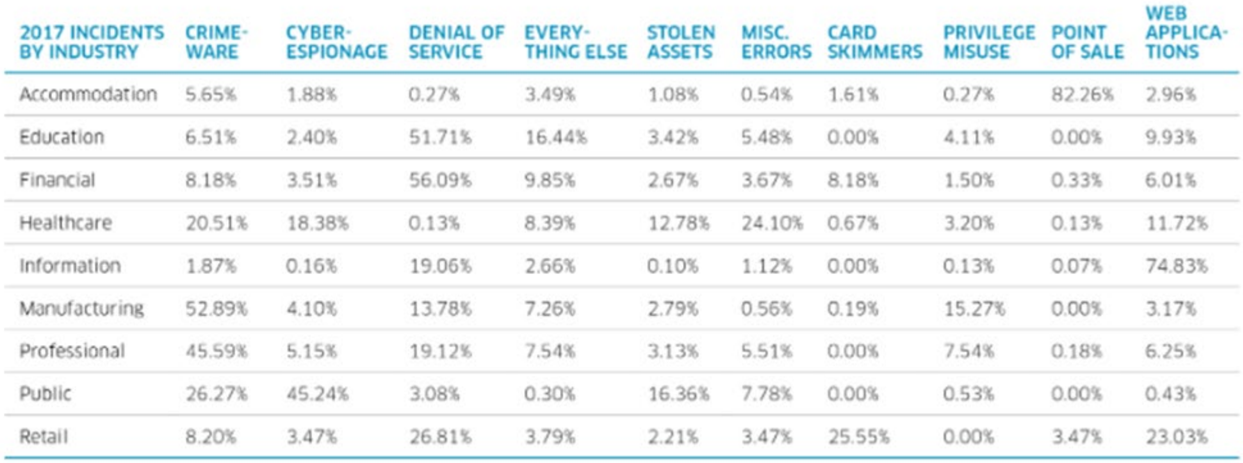
https://www.avast.com/c-exploits

Tooling: Assorted tools, especially ones required for a mechanized process.

https://www.lexico.com/en/definition/tooling

API (Application Programming Interface): An API is a set of commands, functions, protocols, and objects that programmers can use to create software or interact with an external system. It provides developers with standard commands for performing common operations so they do not have to write the code from scratch.

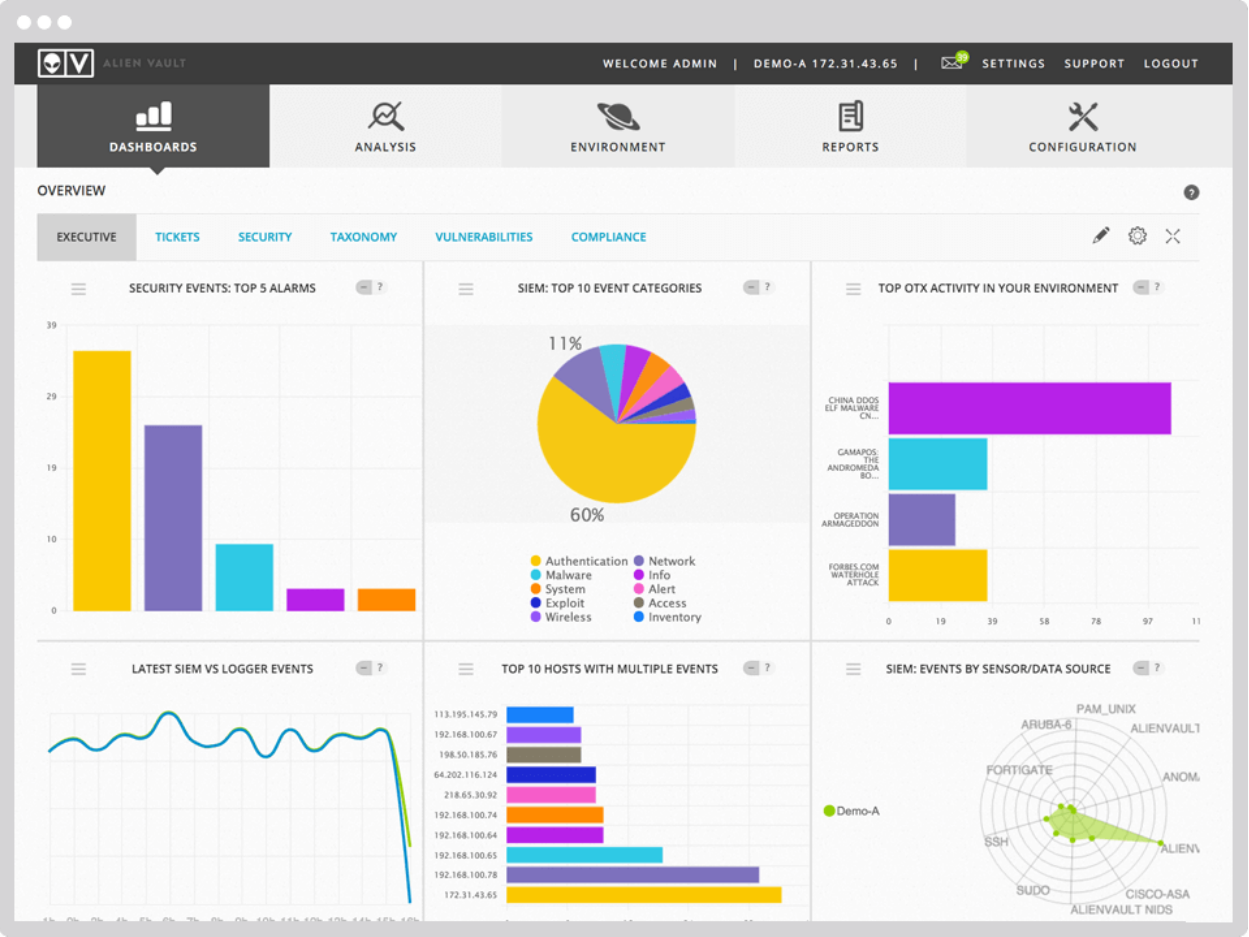
Exhibit 2: Cybercrime Incidents Across Different Industries



2017 INCIDENTS BY INDUSTRY	CRIME-WARE	CYBER-ESPIONAGE	DENIAL OF SERVICE	EVERY-THING ELSE	STOLEN ASSETS	MISC. ERRORS	CARD SKIMMERS	PRIVILEGE MISUSE	POINT OF SALE	WEB APPLICA-TIONS
Accommodation	5.65%	1.88%	0.27%	3.49%	1.08%	0.54%	1.61%	0.27%	82.26%	2.96%
Education	6.51%	2.40%	51.71%	16.44%	3.42%	5.48%	0.00%	4.11%	0.00%	9.93%
Financial	8.18%	3.51%	56.09%	9.85%	2.67%	3.67%	8.18%	1.50%	0.33%	6.01%
Healthcare	20.51%	18.38%	0.13%	8.39%	12.78%	24.10%	0.67%	3.20%	0.13%	11.72%
Information	1.87%	0.16%	19.06%	2.66%	0.10%	1.12%	0.00%	0.13%	0.07%	74.83%
Manufacturing	52.89%	4.10%	13.78%	7.26%	2.79%	0.56%	0.19%	15.27%	0.00%	3.17%
Professional	45.59%	5.15%	19.12%	7.54%	3.13%	5.51%	0.00%	7.54%	0.18%	6.25%
Public	26.27%	45.24%	3.08%	0.30%	16.36%	7.78%	0.00%	0.53%	0.00%	0.43%
Retail	8.20%	3.47%	26.81%	3.79%	2.21%	3.47%	25.55%	0.00%	3.47%	23.03%

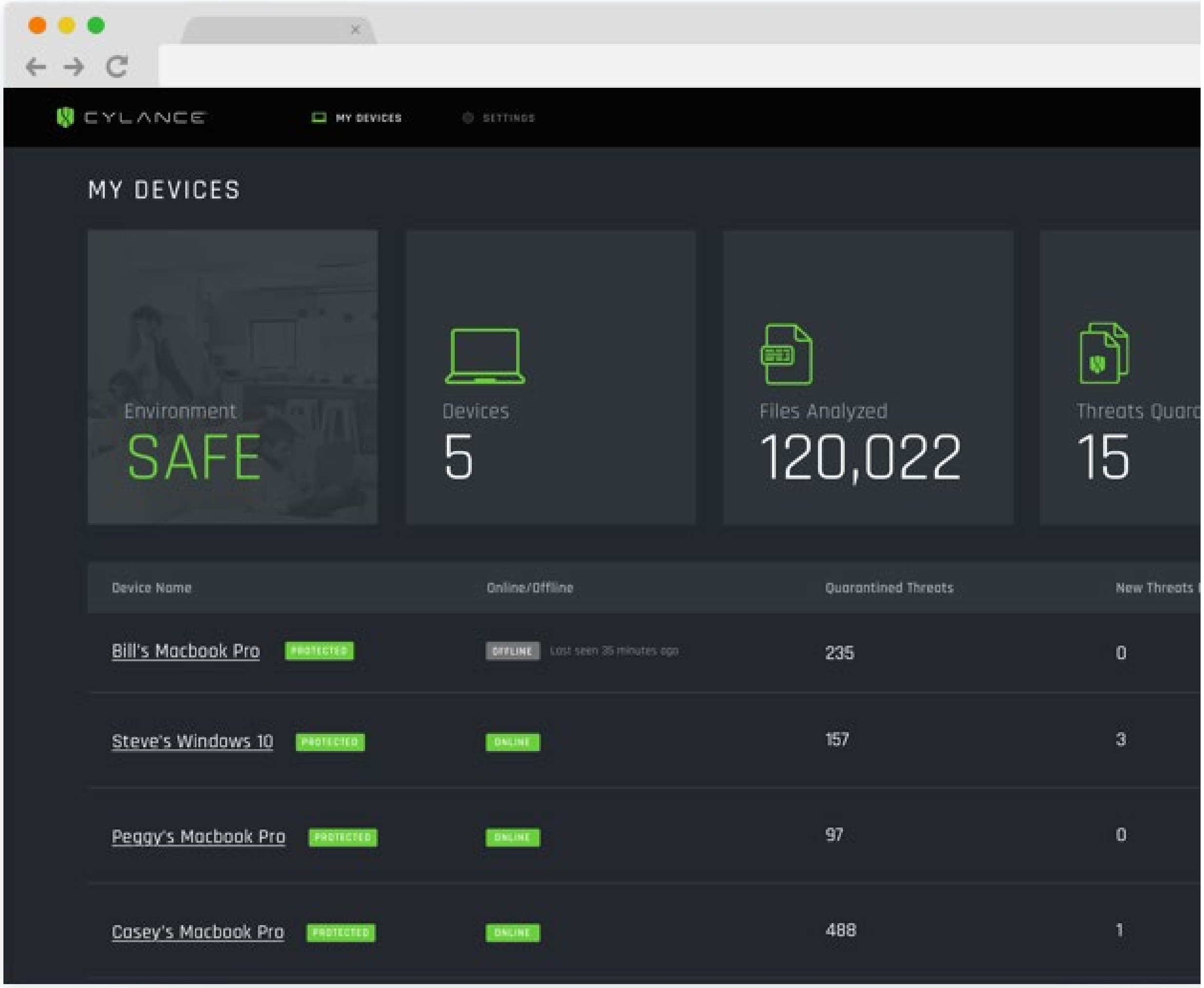
Source: Nasdaq (2018)

Exhibit 3: AT&T AlienVault Dashboard



Source: https://www.g2.com/products/alienvault-usm-from-at-t-cybersecurity/reviews

Exhibit 4: BlackBerry Cylance Dashboard



MY DEVICES

Environment
SAFE

Devices
5

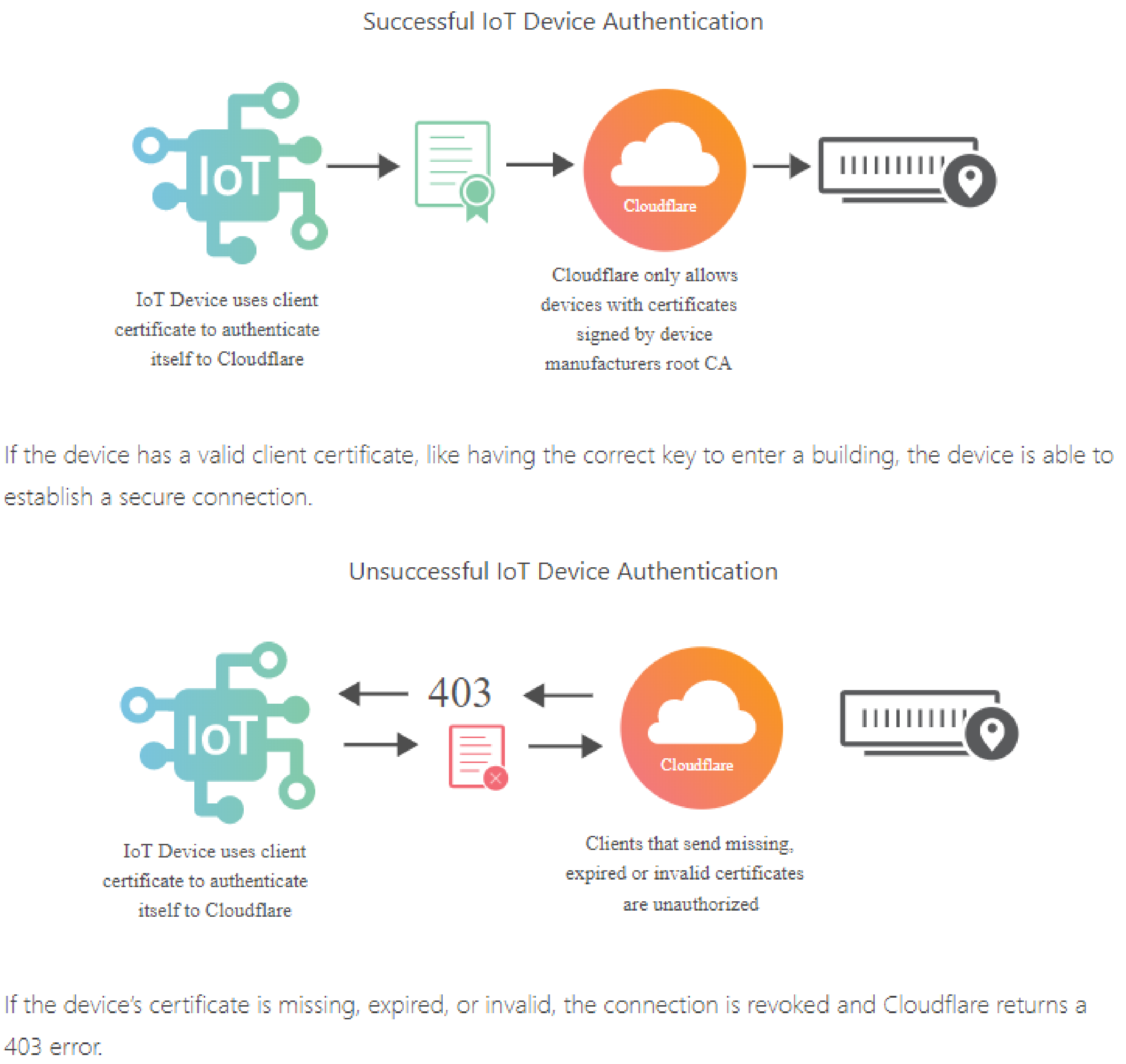
Files Analyzed
120,022

Threats Quar
15

Device Name		Online/Offline		Quarantined Threats	New Threats
Bill's Macbook Pro	PROTECTED	OFFLINE	Last seen 35 minutes ago	235	0
Steve's Windows 10	PROTECTED	ONLINE		157	3
Peggy's Macbook Pro	PROTECTED	ONLINE		97	0
Casey's Macbook Pro	PROTECTED	ONLINE		488	1

Source: https://promos.cylance.com/en-us/?utm_source=ppc&utm_medium=nmpi&gclid=Cj0KCQjwiILsBRCGARIsAHKQWLPIcmWTJWHuKEq8IQ_AljfB32UtpMvrm9QqAJi3KDvLOjQ9GCSWlZ4aAsiiEALw_wcB

Exhibit 5: Cloudflare IoT Devices Authentication



Successful IoT Device Authentication

IoT
Cloudflare
IoT Device uses client certificate to authenticate itself to Cloudflare
Cloudflare only allows devices with certificates signed by device manufacturers root CA

If the device has a valid client certificate, like having the correct key to enter a building, the device is able to establish a secure connection.

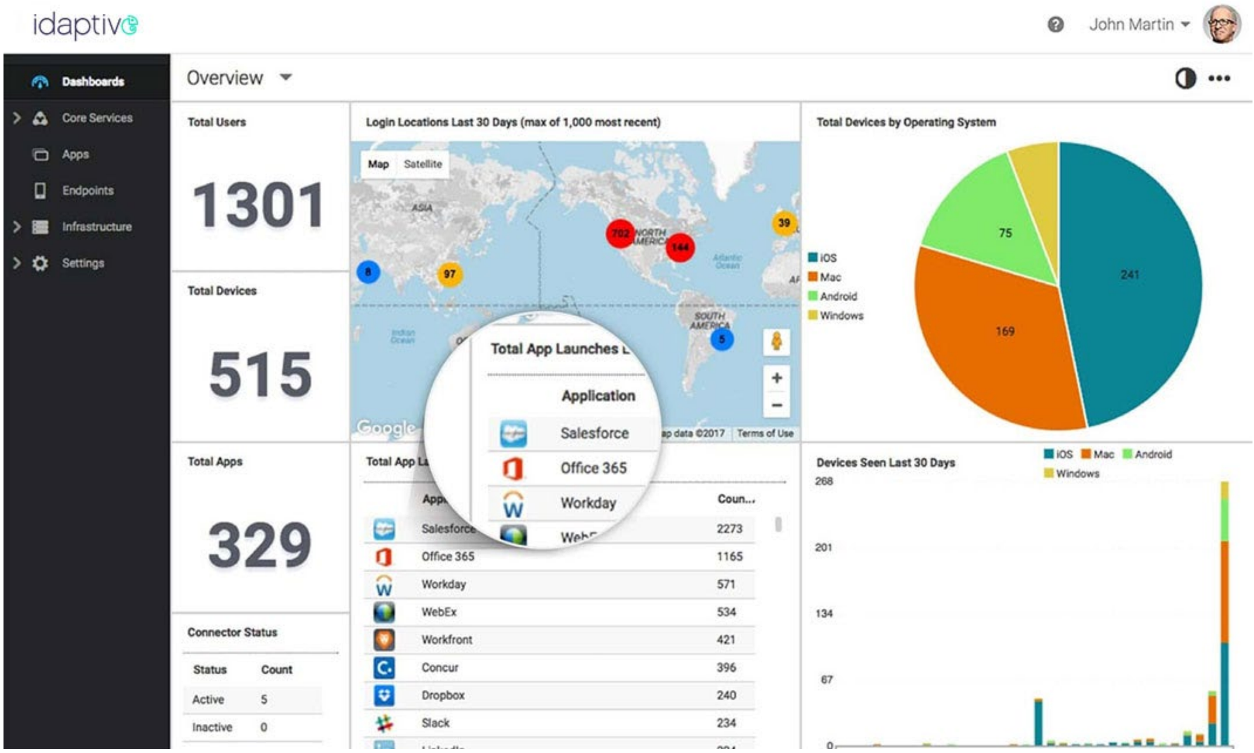
Unsuccessful IoT Device Authentication

IoT
403
Cloudflare
IoT Device uses client certificate to authenticate itself to Cloudflare
Clients that send missing, expired or invalid certificates are unauthorized

If the device's certificate is missing, expired, or invalid, the connection is revoked and Cloudflare returns a 403 error.

Source: https://www.cloudflare.com/orbit/

Exhibit 6: Idaptive Next-Gen Access Dashboard



Total Users

1301

Total Devices

515

Total Apps

329

Connector Status

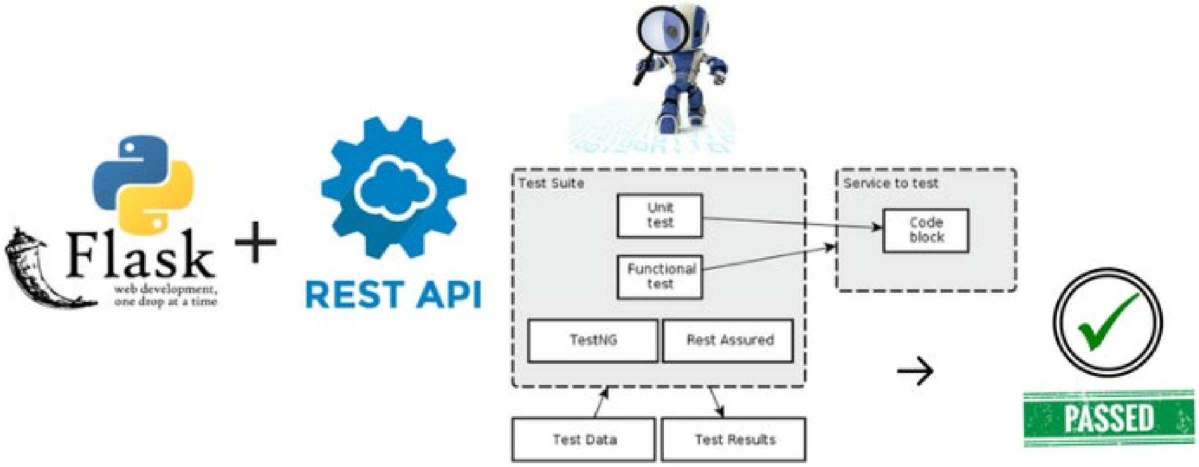
Status	Count
Active	5
Inactive	0

Total App La

App	Coun...
Salesforce	2273
Office 365	1165
Workday	571
WebEx	534
Workfront	421
Concur	396
Dropbox	240
Slack	234

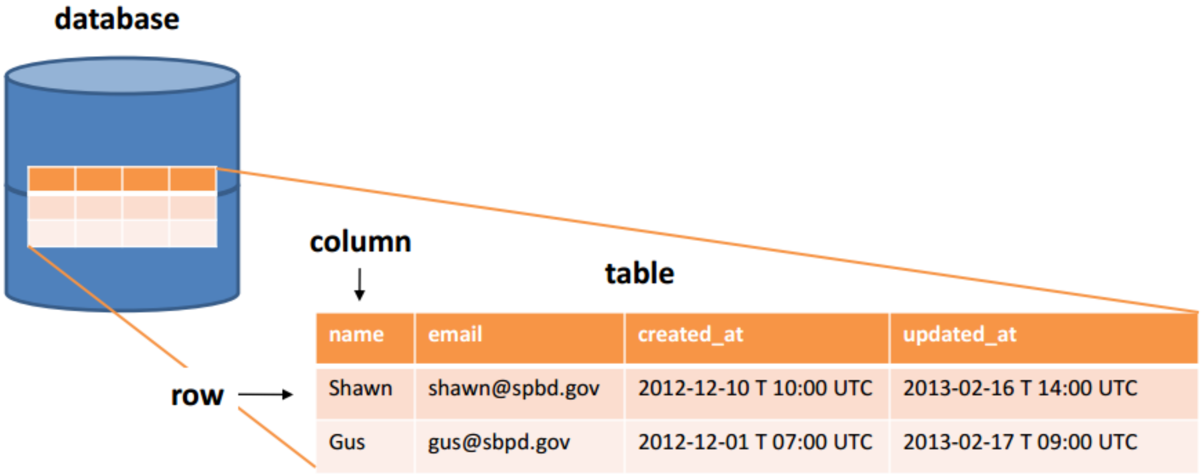
Source: https://www.idaptive.com/

Exhibit 7: Flask Web with REST API



Source: https://www.codementor.io/parths007/writing-unit-tests-for-rest-apis-in-python-ge8wmbofg

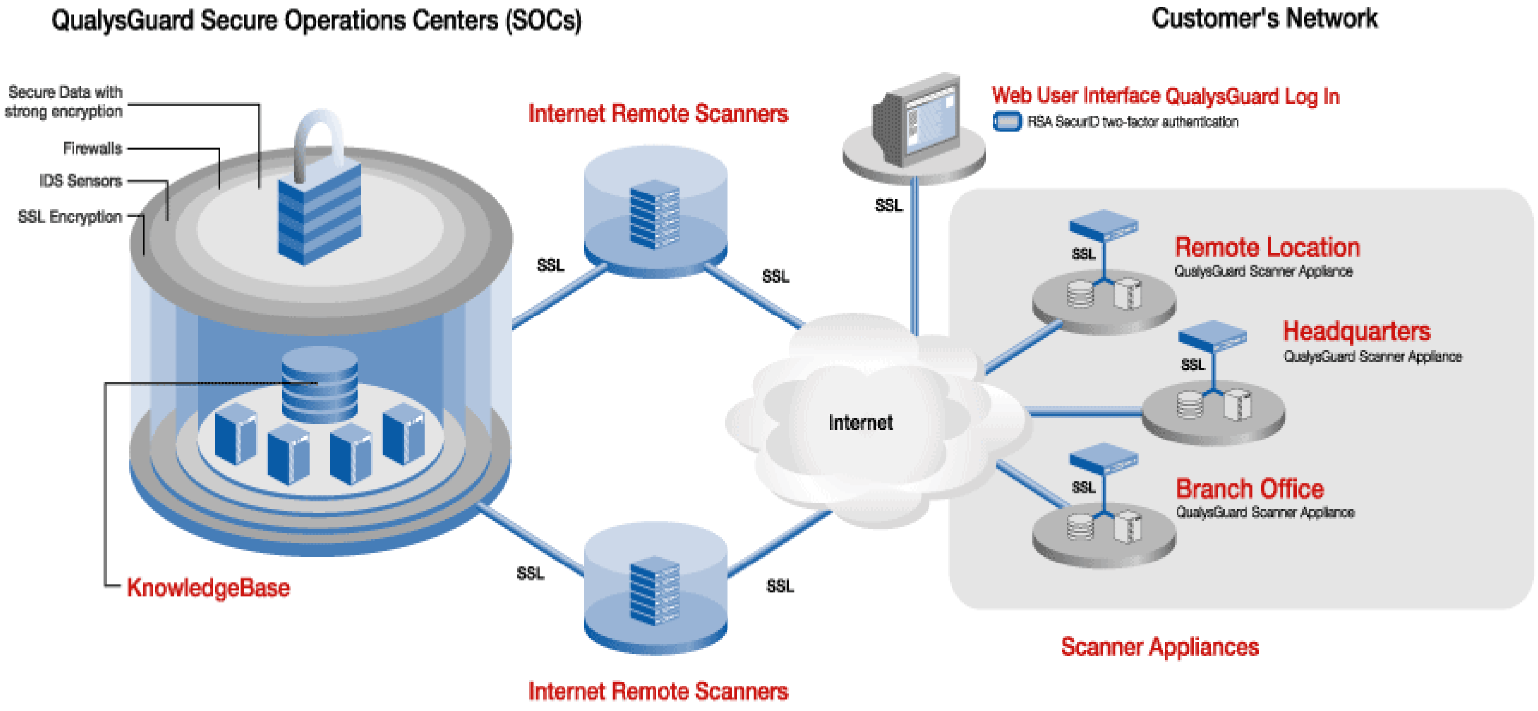
Exhibit 8: Relational Database Example



name	email	created_at	updated_at
Shawn	shawn@spbd.gov	2012-12-10 T 10:00 UTC	2013-02-16 T 14:00 UTC
Gus	gus@sbpd.gov	2012-12-01 T 07:00 UTC	2013-02-17 T 09:00 UTC

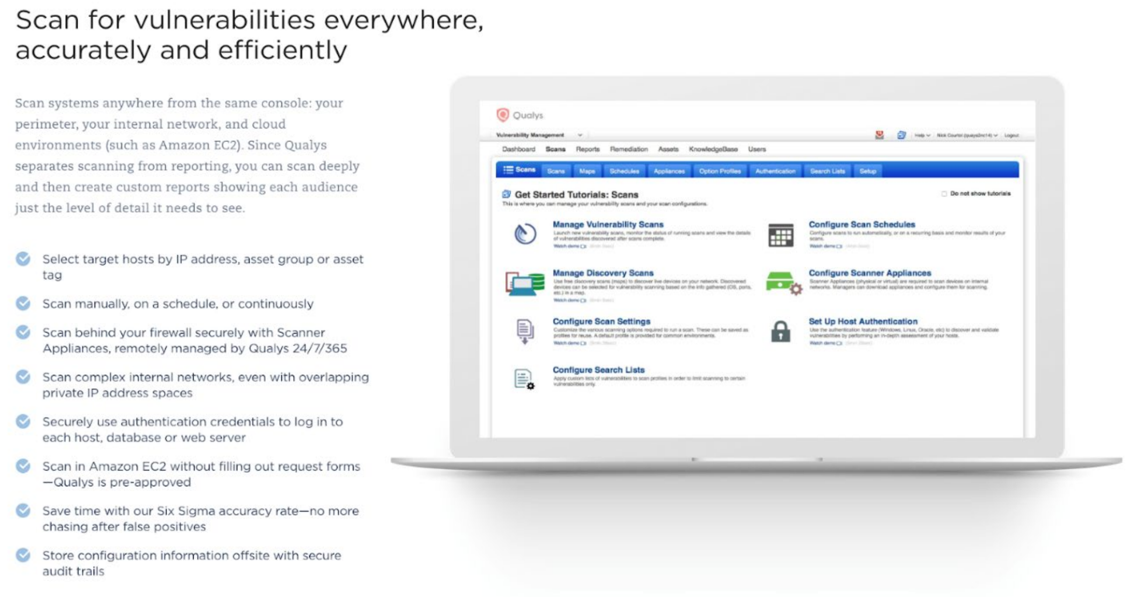
Source: https://code.tutsplus.com/tutorials/relational-databases-for-dummies--net-30244

Exhibit 9: Qualys Network Protection


QualysGuard Secure Operations Centers (SOCs)
Customer's Network
Secure Data with strong encryption
Firewalls
IDS Sensors
SSL Encryption
KnowledgeBase
Internet Remote Scanners
SSL
SSL
SSL
SSL
Internet Remote Scanners
Internet
SSL
Web User Interface QualysGuard Log In
RSA SecurID two-factor authentication
SSL
Remote Location
QualysGuard Scanner Appliance
SSL
Headquarters
QualysGuard Scanner Appliance
SSL
Branch Office
QualysGuard Scanner Appliance
Scanner Appliances

Source: http://www.inbusys.com/qualsysguard.asp

Exhibit 10: Qualys Display



Scan for vulnerabilities everywhere, accurately and efficiently

Scan systems anywhere from the same console: your perimeter, your internal network, and cloud environments (such as Amazon EC2). Since Qualys separates scanning from reporting, you can scan deeply and then create custom reports showing each audience just the level of detail it needs to see.

- Select target hosts by IP address, asset group or asset tag
- Scan manually, on a schedule, or continuously
- Scan behind your firewall securely with Scanner Appliances, remotely managed by Qualys 24/7/365
- Scan complex internal networks, even with overlapping private IP address spaces
- Securely use authentication credentials to log in to each host, database or web server
- Scan in Amazon EC2 without filling out request forms —Qualys is pre-approved
- Save time with our Six Sigma accuracy rate—no more chasing after false positives
- Store configuration information offsite with secure audit trails

Get Started Tutorials: Scans

This is where you can manage your vulnerability scans and your scan configurations.

Manage Vulnerability Scans
Launch new vulnerability scans, monitor the status of running scans and view the details of vulnerabilities discovered after scans complete.
Watch demo

Configure Scan Schedules
Configure scans to run automatically, or on a recurring basis and monitor results of your scans.
Watch demo

Manage Discovery Scans
Use free discovery scans (maps) to discover live devices on your network. Discovered devices can be selected for vulnerability scanning based on the info gathered (OS, ports, etc.) in a map.
Watch demo

Configure Scanner Appliances
Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.

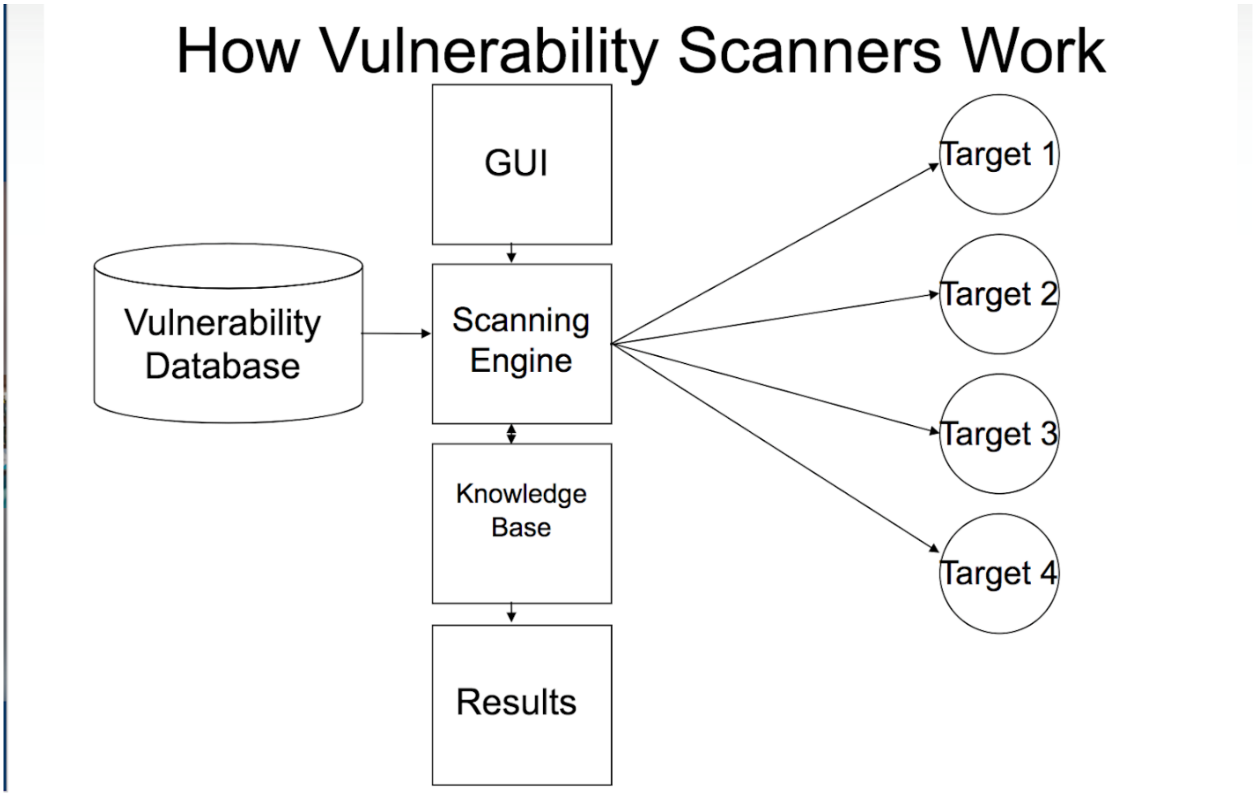
Configure Scan Settings
Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.
Watch demo

Set Up Host Authentication
Use the authentication feature (Windows, Linux, Oracle, etc) to discover and validate vulnerabilities by performing an in-depth assessment of your hosts.
Watch demo

Configure Search Lists
Apply custom lists of vulnerabilities to scan profiles in order to limit scanning to certain vulnerabilities only.

Source: https://www.qualys.com/apps/vulnerability-management/

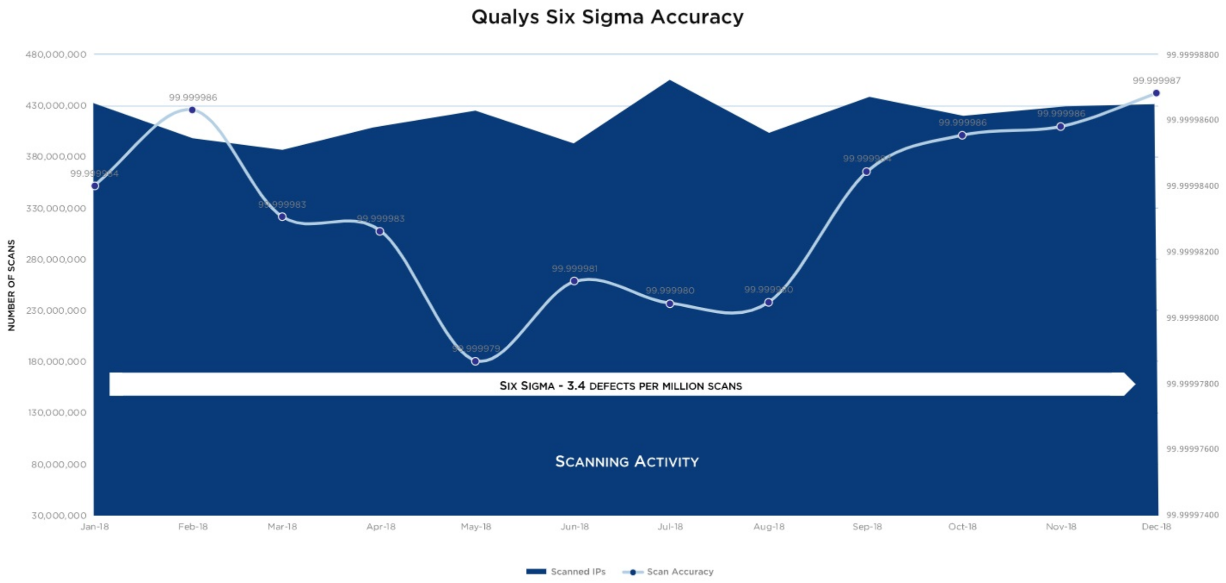
Exhibit 11: How Scanners Work



How Vulnerability Scanners Work

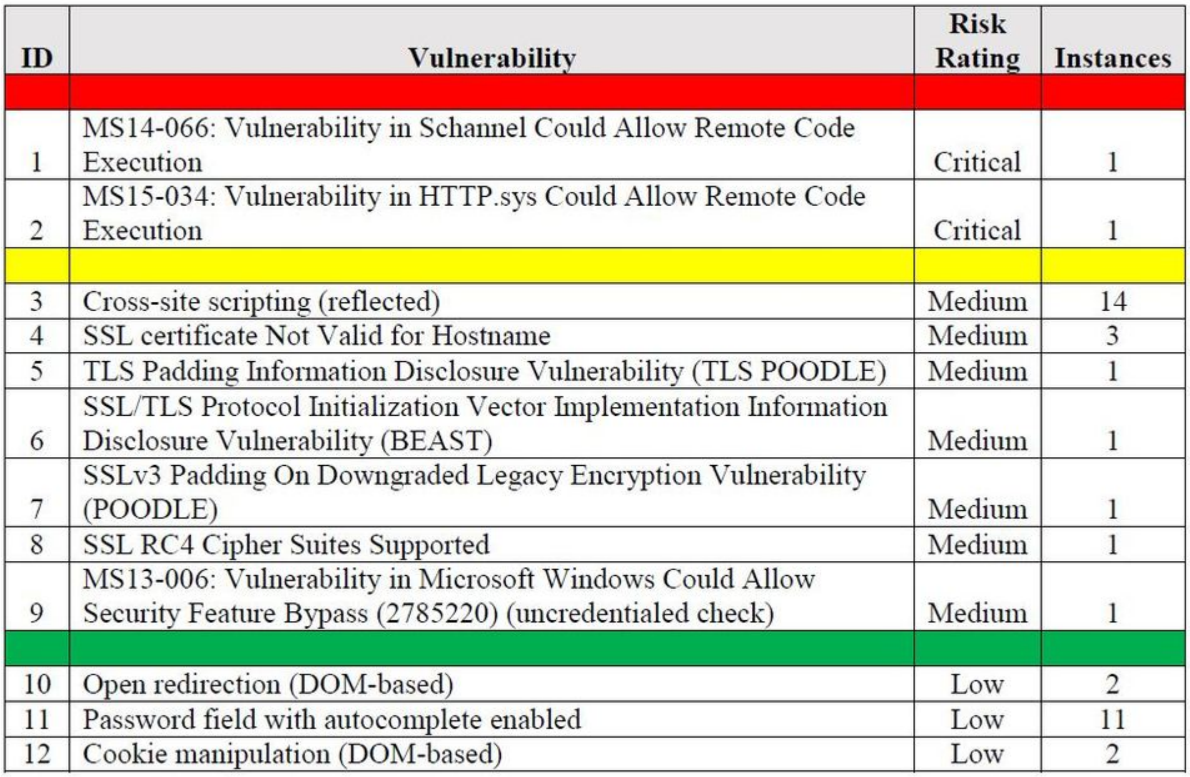
Source: https://www.qualys.com/scanning-accuracy/

Exhibit 12: Qualys Six Sigma Accuracy



Source: https://www.qualys.com/scanning-accuracy/

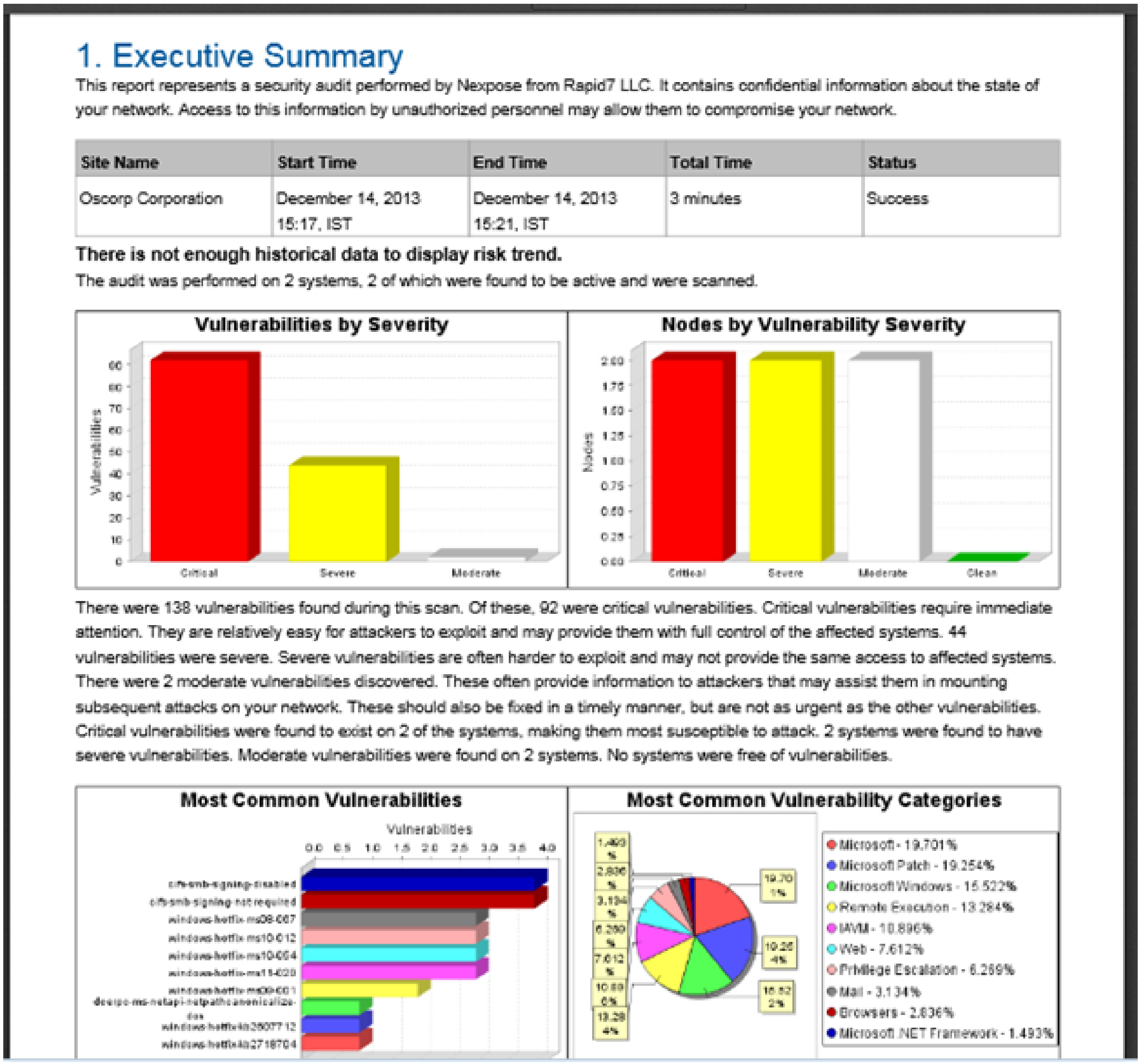
Exhibit 13: Example Vulnerability Report #1



ID	Vulnerability	Risk Rating	Instances
🟥	🟥	🟥	🟥
1	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution	Critical	1
2	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution	Critical	1
🟨	🟨	🟨	🟨
3	Cross-site scripting (reflected)	Medium	14
4	SSL certificate Not Valid for Hostname	Medium	3
5	TLS Padding Information Disclosure Vulnerability (TLS POODLE)	Medium	1
6	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	Medium	1
7	SSLv3 Padding On Downgraded Legacy Encryption Vulnerability (POODLE)	Medium	1
8	SSL RC4 Cipher Suites Supported	Medium	1
9	MS13-006: Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220) (uncredentialed check)	Medium	1
🟩	🟩	🟩	🟩
10	Open redirection (DOM-based)	Low	2
11	Password field with autocomplete enabled	Low	11
12	Cookie manipulation (DOM-based)	Low	2

Source: https://www.nsiserv.com/blog/vulnerability-assessment-checklist-for-small-businesses

Exhibit 14: Example Vulnerability Report #2



1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
Oscorp Corporation	December 14, 2013 15:17, IST	December 14, 2013 15:21, IST	3 minutes	Success

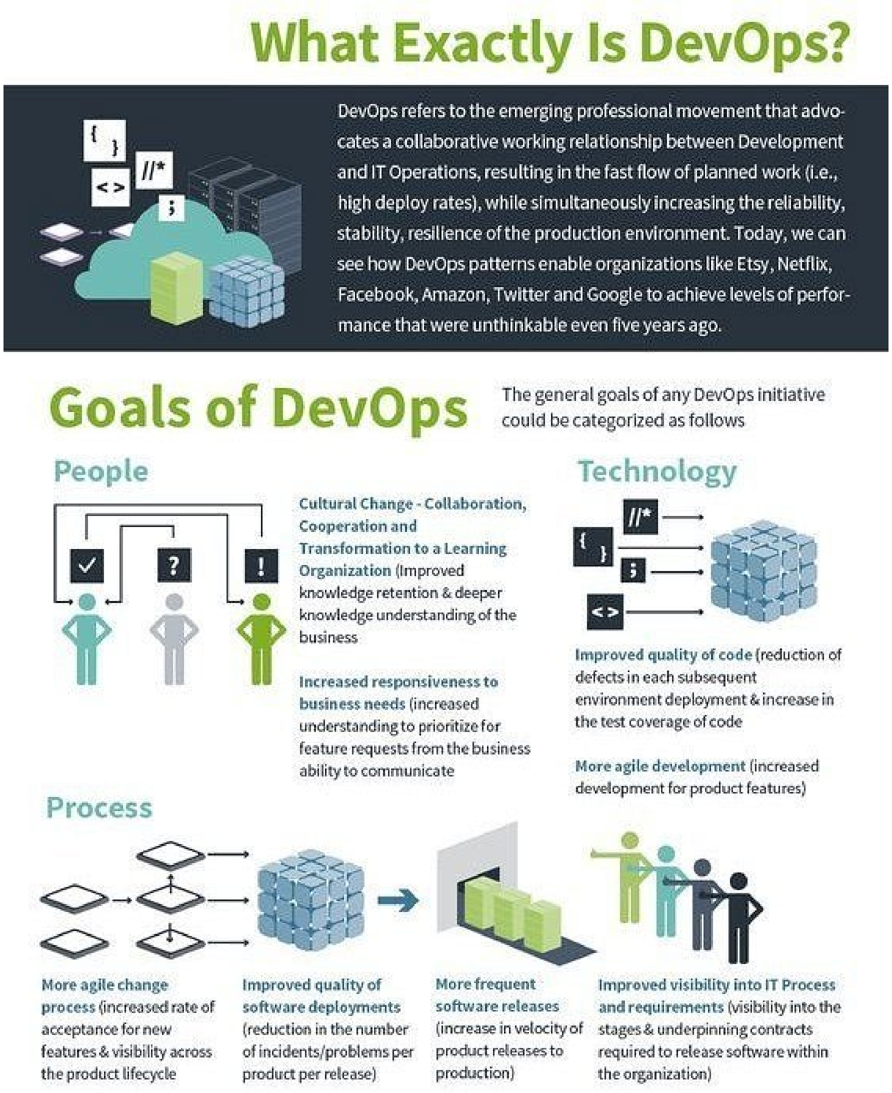
There is not enough historical data to display risk trend.

The audit was performed on 2 systems, 2 of which were found to be active and were scanned.

There were 138 vulnerabilities found during this scan. Of these, 92 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 44 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 2 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 2 of the systems, making them most susceptible to attack. 2 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 2 systems. No systems were free of vulnerabilities.

Source: https://www.nsiserv.com/blog/vulnerability-assessment-checklist-for-small-businesses

Exhibit 15: What is DevOps?



What Exactly Is DevOps?

DevOps refers to the emerging professional movement that advocates a collaborative working relationship between Development and IT Operations, resulting in the fast flow of planned work (i.e., high deploy rates), while simultaneously increasing the reliability, stability, resilience of the production environment. Today, we can see how DevOps patterns enable organizations like Etsy, Netflix, Facebook, Amazon, Twitter and Google to achieve levels of performance that were unthinkable even five years ago.

Goals of DevOps

The general goals of any DevOps initiative could be categorized as follows

People

Cultural Change - Collaboration, Cooperation and Transformation to a Learning Organization (Improved knowledge retention & deeper knowledge understanding of the business

Increased responsiveness to business needs (increased understanding to prioritize for feature requests from the business ability to communicate

Technology

Improved quality of code (reduction of defects in each subsequent environment deployment & increase in the test coverage of code

More agile development (increased development for product features)

Process

More agile change process (increased rate of acceptance for new features & visibility across the product lifecycle

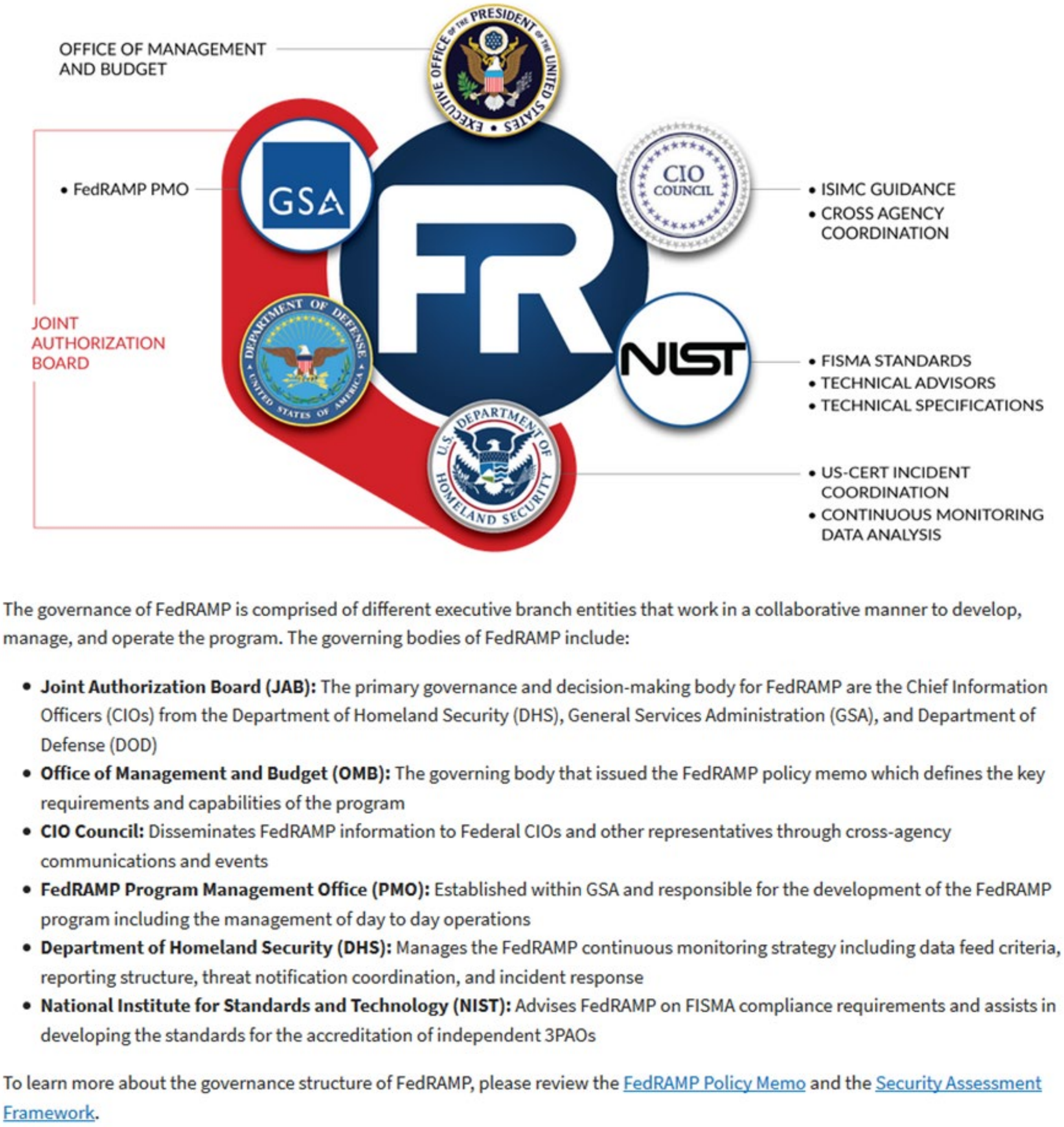
Improved quality of software deployments (reduction in the number of incidents/problems per product per release)

More frequent software releases (increase in velocity of product releases to production)

Improved visibility into IT Process and requirements (visibility into the stages & underpinning contracts required to release software within the organization)

Source: https://scontent.cdninstagram.com/t51.2885-15/e35/20686896_2036789379680513_5272951295127322624_n.jpg

Exhibit 16: FedRamp


OFFICE OF MANAGEMENT AND BUDGET
• FedRAMP PMO
GSA
JOINT AUTHORIZATION BOARD
FR
CIO COUNCIL
• ISIMC GUIDANCE
• CROSS AGENCY COORDINATION
NIST
• FISMA STANDARDS
• TECHNICAL ADVISORS
• TECHNICAL SPECIFICATIONS
• US-CERT INCIDENT COORDINATION
• CONTINUOUS MONITORING DATA ANALYSIS

The governance of FedRAMP is comprised of different executive branch entities that work in a collaborative manner to develop, manage, and operate the program. The governing bodies of FedRAMP include:

- **Joint Authorization Board (JAB):** The primary governance and decision-making body for FedRAMP are the Chief Information Officers (CIOs) from the Department of Homeland Security (DHS), General Services Administration (GSA), and Department of Defense (DOD)
- **Office of Management and Budget (OMB):** The governing body that issued the FedRAMP policy memo which defines the key requirements and capabilities of the program
- **CIO Council:** Disseminates FedRAMP information to Federal CIOs and other representatives through cross-agency communications and events
- **FedRAMP Program Management Office (PMO):** Established within GSA and responsible for the development of the FedRAMP program including the management of day to day operations
- **Department of Homeland Security (DHS):** Manages the FedRAMP continuous monitoring strategy including data feed criteria, reporting structure, threat notification coordination, and incident response
- **National Institute for Standards and Technology (NIST):** Advises FedRAMP on FISMA compliance requirements and assists in developing the standards for the accreditation of independent 3PAOs

To learn more about the governance structure of FedRAMP, please review the FedRAMP Policy Memo and the Security Assessment Framework.

Source: https://www.fedramp.gov/governance/