digitalhands

Digital Hands Whitepaper

What Drives the Need for SOC Maturity?

Copyright 2019 Digital Hands LLC

The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency.

Bill Gates

About Digital Hands

Digital Hands is an award-winning managed security services provider with a difference. We are AGILE, INNOVATIVE and PROACTIVE. Our adaptive security architecture is designed to prevent, detect and respond to cyber security threats with unparalleled velocity.

We are agile because in this business, we must be. We have nearly two decades of experience which allows us to predict where we need to go. We are continuously looking ahead and preparing for the next thing. The threat landscape demands that you move quickly and since our inception, we have risen to that challenge.

We are innovative because of our strong leadership in service development. We are challenging the rules and pioneering new approaches for a more secure world.

We are proactive because of our deep commitment to customer service. In our work, every minute counts which is why we work 24 x 7 to keep your business secure and operating without disruption.

QUICK FACTS ABOUT US

MSSP PURE-PLAY

- Security focused organization, dedicated to delivering high touch services, innovative solutions to security use cases, and rapid adoption of emerging technologies in our space

TRUSTED & SECURITY FOCUSED

- Partnership DNA with a reputation for innovation, speed to market, and channel loyalty

PARTNER FRIENDLY

- Partnership DNA with a reputation for innovation, speed to market, and channel loyalty

CERTIFIED AND COMPLIANT

- ISO 27001 certified, PCI Audited, SAE16 SOC II, US DoD Secret Facilities Clearance

100% US BASED ON SHORE MODEL

- US citizens, US Infrastructure, 24x7x365 GLOBAL Support

Prologue

“The perspective in this white paper is that of a enterprise CISO whose corporation is growing amidst the current industry trends. They have a defined need for better security, but they don’t really know what “better” means. They are also experiencing the pains of the differences between a growing staff and a maturing one.

The account is drawn from actual and anecdotal experiences of Digital Hands and its customers, including partners.

The account is fictional, but the experiences are very real.

OVERWHELMED

Escaping the constant Alarm Bells

I was burdened by over 10,000 security alerts per day. This burden was worsened by the fact that my SOC had a shortage of critical cybersecurity talent, and I struggled to train and retain the staff I did have because there is a zero percent unemployment rate among cybersecurity personnel.

Threats Hidden in the Noise

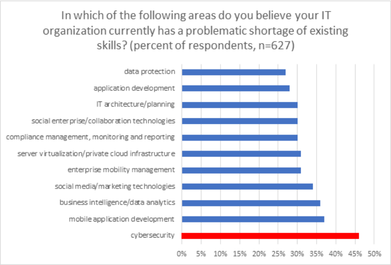
My team's processes, as is the case for 28% of SOCs, were either manual or informal, which made it difficult to train new incoming staff. Because of the volume of noise and the constant turn-over, it often took my SOC on average approximately 197 days to find the real threats.

197
days
the amount of time it takes for an average organization to detect an advanced exploit in their environment.

Like 58% of other cybersecurity executives, I expect to feel even more increased pressure over last year because the organization places enormous expectations on the analysts and administrators working for me, which leads to my employees burning out, leaving enormous skills gaps.

Growing vs. Maturing

The act of scaling and growing my SOC versus maturing it were not necessarily one in the same. An expanding business typically results in an increased attack landscape, which in turn mandates increasing headcount to manage additional security controls required to protect the organization. This naturally increased my cybersecurity budget, which is great, but a larger budget did not yield process optimization along with creating scalable, repeatable best practices. Quite the opposite; bringing more talent into a largely tribal-knowledge environment expanded the problem.



Business compliance requirements may also encourage establishment of measurable outcomes, but compliance is not the equivalence of security. Just providing this quarter's metrics for PCI or HIPAA can sometimes feel like it is distracting analysts from their "day job." The time they spent compiling metrics often left critical systems unpatched for hours or days and essential projects got their deadline pushed back.

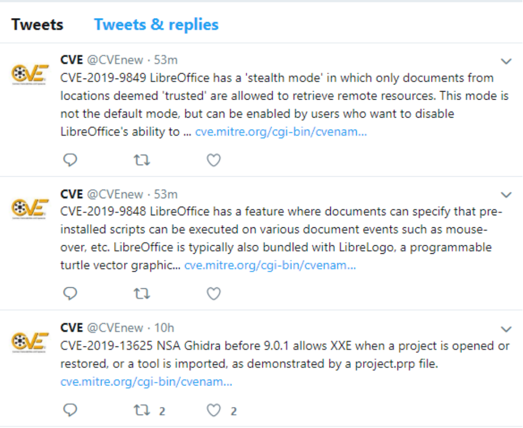
4 to 9

average number of months a job remains open before engaging with an external recuriting firm

https://www.cybersn.com/cyber-security-resources/Salary-Research-Rep-3.pdf, p.12

Constantly Repairing the Wall

The constant emergence of zero-day exploits, release of CVEs more frequently than daily, and unending need for critical patches required my SOC personnel to constantly be on their toes, leaving very little time for the sort of synoptic vision required to optimize, gain efficiency or eliminate waste. SOC personnel take the job of preventing intrusions very seriously, and any time spent on other projects can be difficult to fit into the daily grind of stopping the bad guys. This pain is felt more when new security technologies are introduced to the SOC because people must now spend the time training and learning how to integrate it into existing systems; time not spent working alerts or patching systems.



CVE @CVEnew · 53m
CVE-2019-9849 LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote resources. This mode is not the default mode, but can be enabled by users who want to disable LibreOffice's ability to ... cve.mitre.org/cgi-bin/cvenam...

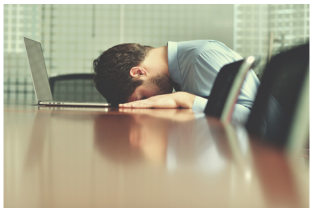
CVE @CVEnew · 53m
CVE-2019-9848 LibreOffice has a feature where documents can specify that pre-installed scripts can be executed on various document events such as mouse-over, etc. LibreOffice is typically also bundled with LibreLogo, a programmable turtle vector graphic... cve.mitre.org/cgi-bin/cvenam...

CVE @CVEnew · 10h
CVE-2019-13625 NSA Ghidra before 9.0.1 allows XXE when a project is opened or restored, or a tool is imported, as demonstrated by a project.prp file. cve.mitre.org/cgi-bin/cvenam...

As if those weren't enough problems, the C-suite was breathing down my neck to demonstrate a return on their investment into improved cyber security and they want to see the metrics that prove it was worth their time. Asking my analysts to step away from the alarms and patches felt like time not spent hardening infrastructure or responding to potential threats and is a tough sell to already tired employees.

DIGGING OUT

The Pain of Scaling



My early-stage SOC found it challenging to keep up with the constant barrage of machine generated alerts. Scaling-up enough analysts to have 24/7 coverage was challenging, if not downright impossible, and having bench depth to cover PTO, sick days, training and turnover felt almost herculean. Carving out blocks of time to identify misconfigurations that generate false positives, spot thresholds that are too low or re-writing SIEM rules to exclude unnecessary devices was sometimes the difference between drowning and succeeding.

Document, Document, Document

I asked six analysts on my incident response team how they perform investigations, and I got six different responses. Does it matter whether an analyst begins with data manipulation and then recording observations or vice versa? Should analysts reduce before they expand or is the reverse true? It turns out that order of operations matters quite a bit and even veteran analysts can have old and outdated habits that die hard. Taking the time to document and identify what it means to perform this work correctly ended up saving massive FTEs down the line while simultaneously improving quality.

One of the side effects of a well-documented and established set of processes for incident handling and change control was repeatability and scalability. Even if all the members of my team are equally skilled, if they perform their work radically differently, it can be difficult, if not downright impossible for newcomers to identify which process to follow. In the worst-case scenarios, the wild-west approach of “anything goes” can create confusion, disinformation and dropped hand-offs right when I need it to go smoothly: during an actual intrusion event.

The Light at the End of the Tunnel

Establishing a commitment to SOC maturity by identifying waste in current processes brought its own rewards: optimization begets efficiency. SOC budgets were tight and reducing the mean-time-to-detect allowed analysts to touch more alarms, perform root-cause-analysis on more problems and exit the reactive mindset that caused every new incident to be the hottest fire. Documenting lessons learned and using this information to optimize and improve current process to prevent future problems yielded precisely the sort of returns the board was seeking.

Obtain, Retrain, Retain

One of the single greatest pain points of every maturing SOC is losing top talent. The national average ratio of job seekers to jobs for all jobs at **5.8**, while the national average for cybersecurity jobs is even worse at only **2.3**.

2.3 very low

average ratio of cyber security workers available compared to the total number of job openings

Accordingly, losing our most valued employees left a hole in the team without anyone on staff able to perform the work that needed doing. Leveraging documented processes and practices to create an internal training team helped straddle otherwise daunting blank spots in the org chart but it often took me 4-9 months to fill open positions, with a 90-day ramp-up period before they were fully function. It was extremely painful having to wait almost a year to back-fill positions when I only received two weeks' notice before they left .

IN THE CLEAR

Build it or Buy it?

When maturing my SOC, it was important to identify what strengths and weaknesses existed within my organization. If I had individuals on my team that are utility players, able to work across the various silos of my SOC and flatten processes to identify where time is wasted, then I needed to be optimizing my own internal processes by leveraging those employees. However, doing so often required they work with precisely the individuals that were already burdened with too much work.

Early on, I had enough individuals at the management level, but found it difficult to maintain staffing levels on my technical employees. I remember with dread when my system administrator, with that specialized skill-set, put in their two weeks' notice. I had already been unable to fill that 3rd shift weekend shift for my incident response team and had been operating on a skeleton staff for months, even though I've been authorized to backfill the recently vacated positions.

To complicate matters further, I had just expanded my defenses to include a new technology. It seemed that reaching the next SOC maturity level would require hundreds of hours of training and dozens of new employees to be obtainable. How could my obstacles be rapidly overcome? I had to identify whether it is less expensive, faster, or higher quality to try and build these capabilities myself or whether it is time to seek outside assistance.

To Built or Not to Build?

If I built it myself, I had three options before me: (1) hire already skilled workers, (2) retrain existing workers or (3) upskill new hires. Hiring already skilled employees suffered from an even longer lag time to hire, not to mention finding the quality employee among the applicants rather than settling for a warm body. Retraining my existing workers took one or more of my remaining essential personnel away from their critical tasks, and the training usually only covered procedure; they still had to perform lengthy discovery-based learning to understand what had to be done in their new role, because far too little of it had been documented by the previous employee and now I had to backfill their position. Finally, upskilling new hires required I find individuals with the right temperament, then pay for costly training and then hope they acquire the tribal knowledge needed to perform in my SOC. All three options took valuable time and energy away from my already overworked staff that I just couldn't afford, and required I somehow continue to retain staff I already had. After reviewing my options, I had to partner with an MSSP.

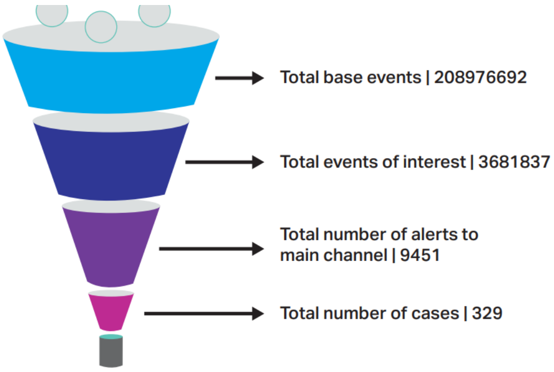
The Right Fit

But finding the right security service provider can be a challenge in itself! I had to identify which systems I needed to be managed internally and which ones to outsource; I had to decide which capabilities I wanted my team to keep once I lightened their load. Many internal employees felt threatened when I brought an MSSP in because they feared the service provider was there to replace them. It was important to reassure internal security personnel that only the incident response triage, and the firewall MACDs will be performed by the MSSP.

I drew clear boundaries where internal staff would still be able to perform their job and clearly identify the scope of work the contract covers with the MSSP. The on-boarding process created additional work for my team in configuring devices, creating credentials and establishing new processes, but things significantly improved once the on-boarding was completed.

The Fruits of Labor

When the day arrived that my SOC had finally matured, I knew it because where once I had over ten thousand alarms per day, now I have less than twelve high value incidents to investigate per analyst per hour. With the MSSP performing initial triage, most false positives have already been weeded out. The remaining alarms have been contextualized with threat intelligence and correlated with appropriate devices to ensure that the wheat has been separated from the chaff.



Because of the orchestration and automation introduced into my SOC by my MSSP, I produce fast and measurable performance that generates KPIs my board members can understand and grasp. The measurable outputs of my SOC demonstrates security value to my larger organization as I identify threats and remediate them in a timely manner. My experienced and trained staff utilize standard procedures, so quality of investigations is normalized among my analysts. I can support a larger organization because of the efficiency and optimization I've achieved, and I can continue improving because my employees have available bandwidth to invest in process optimization.

Whichever route you take to mature your SOC, be aware that things often get messier before they get cleaner. Much like organizing the hall closet, sometimes laying out the current methods used to solve a problem can get mired in discussions around past incidents, emotional scars and previous conflicts between siloed members of your staff. Bringing in outsiders can solve many problems, often in a more timely and cheaper manner than could be done internally, but it has its own challenges. Perseverance and keeping the goal of SOC maturation clearly in mind can help you obtain a more highly structured and optimized SOC. If this story resonates with you, it's because it was drawn from our experiences maturing our customers. Real examples were adapted to coherently tell the story of a CISO's struggles maturing their SOC. If you are facing these same difficulties, an MSSP may be the right solution to your problems.

3.9m$

Global average cost of a data breach

Source: https://www.ibm.com/downloads/cas/ZBZLY7KL p.3

Security Operations Center Maturity Checklist

(based upon HP SOMM)

Level 1

- Can provide security monitoring
- Documentation of processes does not exist
- Processes are ad hoc

Level 2

- SOC meets business goals
- Can meet compliance requirements
- Operational tasks are repeatable
- Documentation of processes exists but are modified reactively

Level 3

- Processes are modified proactively
- Evaluation of operations is performed subjective

Level 4

- Processes are modified using performance metrics
- Evaluation of operations is performed using quantitative metrics
- Evaluation of operations is Reviewed consistently

Level 5

- Documentation of processes is rigid and inflexible
- Existence of an operational improvement program

References

[1] Page 5; https://www.imperva.com/blog/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/, p5“55% of CISOs, felt burdened by over 10,000 security alerts per day” p.2

[2] Page 5; https://www.csoonline.com/article/3307476/5-biggest-cybersecurity-challenges-at-smaller-organizations.html “Top Security Challenges at SMBs” “28% of SOC processes were either manual or informal”

[3] Page 5; https://www.esg-global.com/hubfs/ESG-Brief-Cybersecurity-Skills-Shortage-Feb-2016.pdf [Infographic]

[4] Page 5; http://www.level3.com/~/media/files/brochures/en_retail_eb_protecting_omnichannel_securitydefenses.pdf “on average approximately 197 days to find the real threats”

[5] Page 6; https://www.cybersn.com/cyber-security-resources/Salary-Research-Rep-3.pdf p. 12 “positions left open for 4-9 months before turning to recruiters ”

[6] Page 7; https://twitter.com/CVEnew/

[7] Page 9; https://www.cyberseek.org/heatmap.html “SUPPLY OF CYBERSECURITY WORKERS” “The national average ratio of job seekers to jobs for all jobs at 5.8, while the national average for cybersecurity jobs is even worse at only 2.3”

[8] Page 9; https://www.cybersn.com/cyber-security-resources/Salary-Research-Rep-3.pdf p. 12 “positions left open for 4-9 months before turning to recruiters ”

[9] Page 11; https://www.microfocus.com/media/white-paper/intelligent_security_operations_a_staffing_guide_wp.pdf p. 12 “Analysts should work 8–12 alerts per hour, which allows the analysts to triage and escalate events effectively.”

[10] Page 12; a. https://www.ibm.com/downloads/cas/ZBZLY7KL p. 3

Contact Us

Digital Hands
400 North Ashley Drive, Suite 900
Tampa, FL 33602
(877) 229-8020
sales@digitalhands.com
www.digitalhands.com