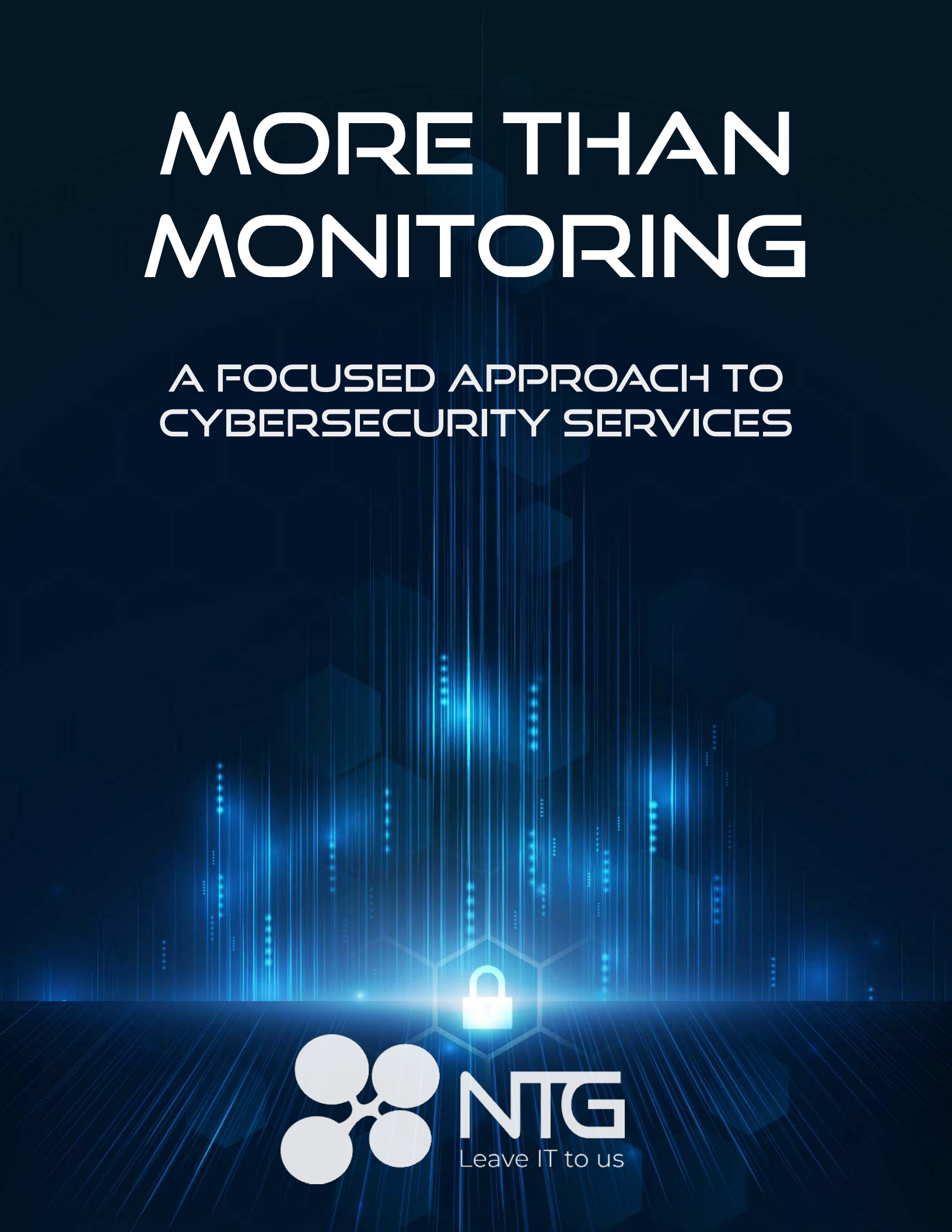
MORE THAN MONITORING

A FOCUSED APPROACH TO CYBERSECURITY SERVICES



NTG

Leave IT to us

INTRODUCTION

"The five most efficient cyber defenders are: anticipation, education, detection, reaction and resilience. Do remember: cybersecurity is much more than an IT topic."

-Stephane Nappo, Chief CISO for Société Générale International Banking

The need for enhanced cybersecurity has been making a lot of headlines lately. Frankly, it's frightening, especially for business owners, directors, and anyone with informational assets worth securing. Information is a significant component of most organizations' competitive strategy; either by collecting, managing, or retaining it. Any impact to that strategy should not be underestimated or neglected.

The pressure is on organizations' decision-makers to stay ahead of business-derailing impacts. Maybe that means extra training or recruitment for an existing IT department or hiring an in-house cybersecurity team. Maybe it means purchasing an expensive piece of software that purports to "do it all." These solutions are typically expensive, and funding for them isn't always available. Outsourced services aren't always reliable, either.

IT'S WHY WE BUILT A STATE-OF-THE-ART CYBERSECURITY OPERATIONS CENTER

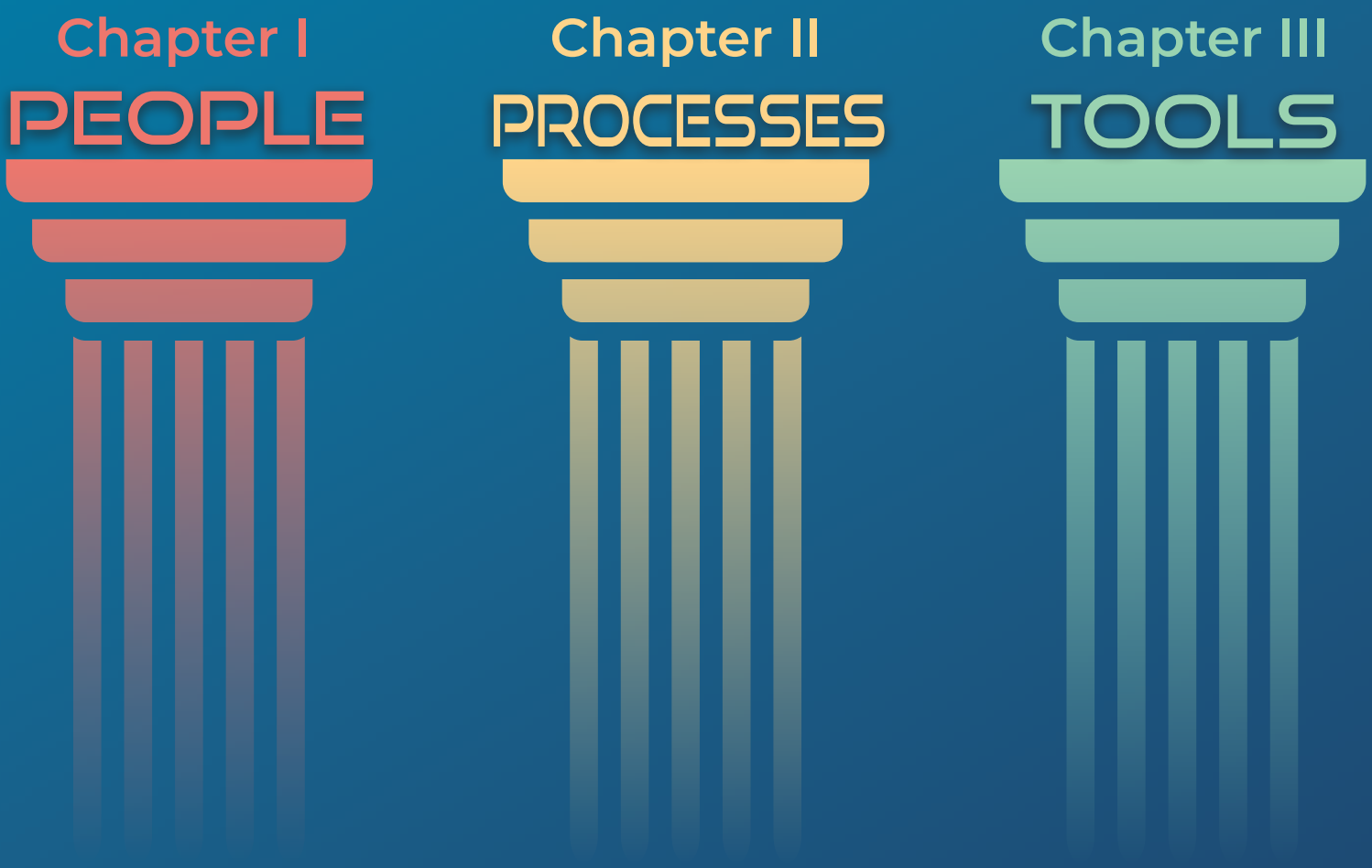
A typical security operations center monitors networks and alerts on threats. NTG's Cybersecurity Operations Center (CSOC) monitors, detects, contains, and remediates threats across applications, devices, systems, networks, and locations. It performs these functions and more, remotely, on a 24/7/365 basis.

We don't intend to stoke the fear factor too much in this book, but cybercrime is extremely prevalent at the time of this publication. Ransomware attacks are up over one thousand percent since 2020. Intrusive threats are more distributed and well-hidden than ever before, so it takes more than a single piece of software or layer of security to effectively monitor and protect an environment. Cybersecurity has evolved beyond the confines of IT. As our world transforms—as we rely more and more on digital resources—cybersecurity has become a social responsibility for all of us.

It's why today's cybersecurity solutions call for **more than monitoring**.

The rest of this e-book explains the foundations and functions of the CSOC and what distinguishes NTG's cybersecurity services from the rest.

CONTENTS



Together, these pillars form the essential structure of NTG's CSOC. An effective cybersecurity operation requires a team of experts, proven processes and methodology, and a modern suite of customizable tools capable of scaling with evolving technology. If just one pillar is neglected, the rest crumble with it. We continually strengthen this foundation against the growing tide of cybercrime. Our staff of analysts and engineers stays current in certifying and continuing their education. We refine our processes to stay up to date with industry regulations and compliance requirements. And we consistently improve our suite of tools, and even develop new ones sometimes. It's what makes NTG's CSOC truly state-of-the-art.

Chapter I

PEOPLE

Our people are passionate about what they do. Some of us have been working in the IT sector since before the advent of the Internet. Most of us can talk about the latest ransomware attack or a recently discovered firewall exploit for hours. We strive to stay up-to-date on the latest in IT and cybersecurity news and while we're all pretty knowledgeable, each of us has a specialization that separates us from the rest. As a collective, our people comprise a powerful cybersecurity operation.

It's the first pillar for a reason. An MSSP could have the greatest proprietary technology available. They could have documentation on every cybersecurity breach and emerging threat known to man. They could (in an alternate universe) have billions of dollars at their disposal. They could have it all, and it would all be useless without the right people in place to run the show.

Besides, technology and strategy changes all the time in our world. The only thing that remains constant is the human element. Cybercriminals usually don't have to perform technical wizardry to pull off an attack. More often, they count on innocent mistakes (like willingness to click a link) to do what they do. And nobody is completely infallible.

The human element is simultaneously the strongest cybersecurity defense and the weakest cybersecurity link.

That's a good thing. The more we learn about ourselves and our tendencies, the more we can contribute to a more robust cybersecurity culture for all.

Our CSOC staff doesn't just monitor networks for anomalies. We understand specific business requirements. We have been involved in a variety of IT environments—from networks deployed and used by the US military to those used by local non-profit organizations. Moreover, we understand that, just like cybersecurity teams, a "one-size-fits-all" solution is not the most effective one.

Next up: How are those specializations organized? Most operations centers utilize a tiered system for escalating an issue to the appropriate role.

ROLE	SKILLS	RESPONSIBILITIES
 **Tier 1** **Security Analyst**	Sysadmin skills (cross-platform); Basic programming skills; Security skills (CISSP, GCIH, GCFA, GCFE, etc.)	Reviews latest CSOC alerts to determined relevancy and urgency. Creates tickets for alerts that require an elevated response or review (Tier 2). Runs vulnerability scans and assesses scan reports. Responsible for monitoring the monitoring tools.
 **Tier 2** **Incident Responder**	Skills in previous tier + a few years of experience and natural ability; Hacking knowledge; Capable of handling pressure and stressful situations	Reviews tickets initiated by Tier 1. Tier 2 can be considered the “first responder” as they begin the path towards remediation in the event of an incident. Identifies the scope of an attack and all impacted systems.
 **Tier 3** **Threat Hunter**	Skills in previous tiers + keen understanding of data visualization tools and penetration testing; Advanced deductive skills	Responsible for reviewing vulnerability assessment reports generated at Tier 1. Leverages threat intelligence to determine vulnerabilities to emerging threats. Conducts penetration tests to validate resiliency and explore areas to improve.
 **Tier 4** **Management**	All of the above skills + excellent leadership and communication skills; Extensive experience in previous cybersecurity roles	Manages the activity of the CSOC. Responsbile for staff recruitment, hiring, and training. Continually refines the operational function and effectiveness of the CSOC based on best practices and established metrics.

SPOTLIGHT

THREAT INTELLIGENCE

Threat Intelligence is evidence-based knowledge about existing or emerging hazards to assets. Our CSOC team collects, analyzes, and uses threat intelligence data to fortify against and hunt down threats. It's like criminal investigation—evidence has to be extracted from mountains of data, patterns identified—only, cybercriminals are arguably better at maintaining anonymity than regular crooks.

CSOC analysts look for inidicators of compromise (IOCs) across all assets, devices, and networks. Common IOCs are spikes of unusual outbound network traffic or anomalies in privileged user account activity. On their own, IOCs may be evidence of an intrusion, but real threat intelligence calls for context. IOC data is matched against threat intelligence reports from numerous sources to build profiles of the tactics, techniques, and procedures (TTPs) of cybercriminals. Knowing who is behind a threat is key to knowing how to respond.

> **"If you know the enemy and know yourself, you need not fear the result of a hundred battles."**
>
> **-Sun Tzu, The Art of War**

Traditionally, cybersecurity investigations begin when the CSOC's tools alert to malicious activity. But what happens when the activity is stealthy and doesn't raise any alarms? Threat Hunters excel at finding and rooting out these sort of cyberattacks. In doing so, their findings actively contribute to the body of existing threat intelligence. Threat hunting is about venturing into the unknown. Threat intelligence is typically well-documented and publicly available, and cybercriminals adjust their TTPs quickly and accordingly. This isn't to say Threat Hunters are full-time detectives, but they do monitor the depths (like the Dark Web), and utilize existing threat intelligence to anticipate what certain adversarial groups or individuals will attempt in the future.

Next up: By now, you've likely ascertained that cybersecurity involves collecting and processing immense amounts of data and carrying out a long list of daily tasks. Let's take a closer look at the processes that keep the CSOC operating efficiently.

Chapter II

PROCESSES

Processes don't have to be complicated. In fact, it's better that they aren't. Consider the humble checklist. Checklists help us stay organized, collected, and sane. Even if you're not literally checking off a list of tasks, you probably have a basic idea of your daily objectives. It's natural for people to follow processes, whether consciously or not.

A simple checklist can help professionals like surgeons and pilots minimize errors that can be the difference between life and death. Minimizing errors from a cybersecurity professional's perspective can be just as dire. Consider the fact that cybersecurity is a critical element of the Department of Homeland Security's mission. One minor oversight—an open port on a firewall, or an easily guessed password—can lead to catastrophe for businesses, organizations, and governments.

NTG's CSOC is responsible for carrying out hundreds of tasks to ensure our partners' assets are protected and threats are detected and eliminated with minimal to zero impact. You can probably see where we're going with this: the CSOC team has a process for everything—from hardware inventory to event classification, to remediation and recovery. There's even a process for refining or changing a process, because the phrase "we've always done it this way" doesn't fly here. It's worth emphasizing again that the scope of cybersecurity is undergoing a revolution. Continual change means we have to adapt on a dime.

It's worth noting that business process enablement in general evolved rapidly with the advance of information technology a couple decades ago. Technology has made business process management easier, but it's also spawned an underworld of cybercriminals (who have processes of their own). Let's just say, it's a lot to account for. It's why the CSOC sticks to tried and true processes.

Next up: Detailing every CSOC process & procedure deserves a whole e-book on its own. We broke the next part down into categories. Let's take a closer look at the process framework the CSOC uses in its daily operations

> **"As a Global CISO, the best advice I can give is don't try to do something different for every part of the world. Pick and choose what you're going to use from a policy and procedure standpoint."**
>
> **-James Waters, Global CISO, Black & Veatch**

ASSET DISCOVERY

A complete inventory of assets in a network is usually the first step to securing it. Assets include hardware (computers, servers, routers, switches, etc.), software (applications, services, active ports, virtual machines, etc.), and their interactions and business functions.

We use a combination of active and passive asset discovery techniques during onboarding and throughout our partnerships. Our CSOC captures accurate and real-time information on all assets in a network and/or cloud environment. We'll go a little more in depth on this in the next chapter, but the takeaway is this: Some information environments are comprised of tens of thousands of assets, and using automation to keep track of them saves our partners (and us) a lot of time.

EVENT CLASSIFICATION

Once assets have been accounted for, the CSOC can begin collecting, correlating, and analyzing log data. Analysts sift through rapidly accumulating data for indicators of compromise (IOCs). We're talking thousands, sometimes millions of logs daily. It's a bit like looking for a needle in a haystack.

Tier 1 CSOC analysts review events and verify their criticality or severity. Sometimes there are false alarms. Once verified, Tier 2 takes over for further investigation. Documentation is paramount throughout all of these processes. We practice thorough notation and ticketing so all CSOC staff has a complete history of an event's discovery and detail. NTG's event taxonomy shows the sequence of actions an attacker uses to infiltrate a network, also contributing to threat intelligence.

Note: NTG's processes and procedures are adaptable. We consider any and all of our partners' business requirements whether we are assisting an in-house IT department or managing the whole environment.

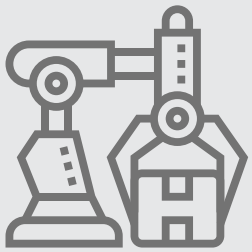
PRIORITIZATION & ANALYSIS

It's tricky to prioritize in today's cybersecurity culture. MSSPs can get bogged down by the sheer number of endpoints in any given network. Something is always alerting, and it's up to the CSOC analysts to determine which events are the most impactful to business continuity.

Automation helps, but the human element is still a necessity. To aid with prioritization, CSOC analysts use a set of directives applied against raw event log data to identify and escalate signs of malicious activity expeditiously. Keep in mind, adversaries are usually subtle at the outset of an infiltration. They probe slowly, careful not to raise red flags. Initial indicators might not look like indicators at all to a lot of monitoring tools. Prioritization and subsequent analysis of events also aids threat hunters in that they can focus on threats that may have advanced beyond primary defenses.

REMEDIATION & RECOVERY

Fastidious incident detection and response is imperative to containing damage and preventing similar incidents in the future. Of course, recovering any lost data and getting business back on track is the CSOC's primary objective post-attack. But we also specialize in forensic analysis "at the scene of the crime" to build on the existing body of threat intelligence.



The remediation and recovery process varies based on the type and scope of an attack (and it's a CSOC priority to limit that scope with preventative measures), but from a broad overview, the following steps are common:

- Patching and updating devices, applications, and operating systems
- Reconfiguring system access/retooling access management
- Reconfiguring network access (adjusting firewall rules, VPN access, etc.)
- Validating patching procedures and other security controls
- Re-imaging systems and restoring from backups
- Reviewing monitoring capabilities

Maintaining backups is essential to data recovery. We highly recommend keeping multiple, encrypted backups. Stay tuned to ntgit.com for backup best practices.

ASSESSMENT & REVIEW

Assessment is an ongoing process. We assess environments during onboarding, in the discovery phase, during and after an incident, and at scheduled intervals in between. An event or incident is revealing, but we prefer to take a proactive approach to find and fix vulnerabilities before they can be exploited.

We are big believers in transparency with our partners. NTG provides comprehensive reports compiled from assessment data which can be shared with auditors, consultants, and executive management to demonstrate effectiveness and compliance to regulatory standards. Our tools feed reporting dashboards which we also share, providing visibility into our operations (tickets, events, network traffic, user activity, and analysis).

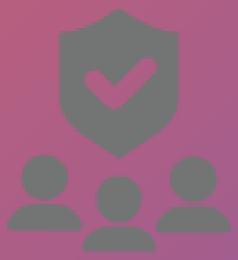
Assessment isn't just for our partners—we assess our own operations regularly.

BY THE BOOK

NTG's CSOC is unique, but we still operate in accordance to established frameworks and regulations. The processes and procedures we've developed over the years align with baselines detailed in the Information Technology Infrastructure Library (ITIL) and standards set by the National Institute of Standards and Technology (NIST).

We are keen observers of regulations and compliance standards, whether they're on the horizon, recently updated (see: Cybersecurity Maturity Model Certification 2.0 updates), or long-existing law (HIPAA). We see it as part of our duty to assist others in aligning their processes with established guidelines to create a stronger cybersecurity culture for all.

Next up: Nuts & bolts. The CSOC tool suite is a truly distinguishing factor among MSSPs and cybersecurity software developers. We have, at our command, the cybersecurity tools of the future.



Chapter III

TOOLS

There's no silver bullet in cybersecurity. Despite claims to the contrary, no singular, out-of-the-box solution covers all the bases. Don't get us wrong; a lot of security software suites are extremely proficient at what they propose to do, and there are many more in development, but a solid cybersecurity model is nuanced—there's a sense of engineering behind it.

Imagine purchasing the latest and greatest motion-sensing camera system for your home. It's got instant alerts, it functions offline, it even reads body language and facial expression in conjunction with AI to decide whether or not that guy approaching your porch with a box has criminal intent. "I'm finally at peace leaving my home unoccupied for the day," you think as you back your car out of your driveway. Still, you probably locked your front door on the way out. And that guy with the package? Just a regular delivery. But those drivers are easy to impersonate, and AI is not infallible.

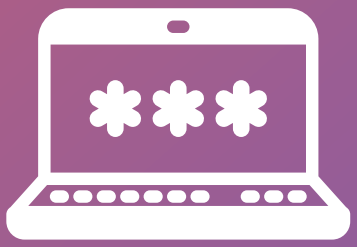
It's always been a cat and mouse game, and these days the mouse has titanium teeth. As you might have guessed, this chapter isn't simply an explanation of the tools NTG uses to gain the upperhand in a world rife with cybercrime—because it isn't just about the tools, it's how we use them.

Cybercriminals are using modern and sophisticated tools, too. And they're increasingly well organized, coordinated and funded. Their targets aren't as niche as they used to be, either. In the past, cybercriminals mostly went after valuable data. With the advent and subsequent prevalence of ransomware, the data itself isn't necessarily as valuable as the amount someone can demand for its decryption.

It makes sense for organizations with a track record for being targeted to take the necessary cybersecurity precautions. The pool has opened up, however. It's an opportune time for everyone to enhance their security.

Note: Not to boast, but there's a great deal of ingenuity and innovation behind the tools we use. The suite is decades in the making, and getting better all the time.

THE ESSENTIALS



Going with the analogy from the previous page, a whamadyne cybersecurity solution doesn't mean a thing if you don't implement the essentials first. So lock your doors.

Monitoring is great for indentifying incidents and managing them, but it also gives us insight into system's attack surface by mapping out devices and paths. Attack surface is comprised of all endpoints through which an unauthorized user may enter an environment. Keeping the attack surface small is a basic security measure, but it requires upkeep as an attack surface tends to fluctuate over time. It's something that's often overlooked in lieu of modern, all-in-one software solutions.

ATTACK SURFACE REDUCTION

Password Management

Defining password policies, scheduling password changes, and implementing single sign-on (SSO) and multifactor authentication (MFA) are excellent first steps. Beware of using common, short, and easily guessed passwords.

Security Awareness Training

Educating users on threats and ways to protect against them. Security awareness training commonly involves learning to recognize phishing schemes and social engineering schemes, and other internet best practices.

Next Gen Antivirus

Viruses and malware are still going strong—and they tend to be sneakier than the poorly disguised .exe files of the early web. Installation and monitoring of a next generation antivirus is a critical attack surface reduction.

Patch Management

Frequent updates can be a hassle, but they're necessary for security. You may notice a lot of critical operating systems updates are vulnerability patches. Our tools help identify non-updated and legacy software.

Server Hardening

Servers, especially web servers, are typically at the edge of any given network making them particularly vulnerable. Hardening makes sure servers aren't operating with default configurations, among other things.

Remote Employees

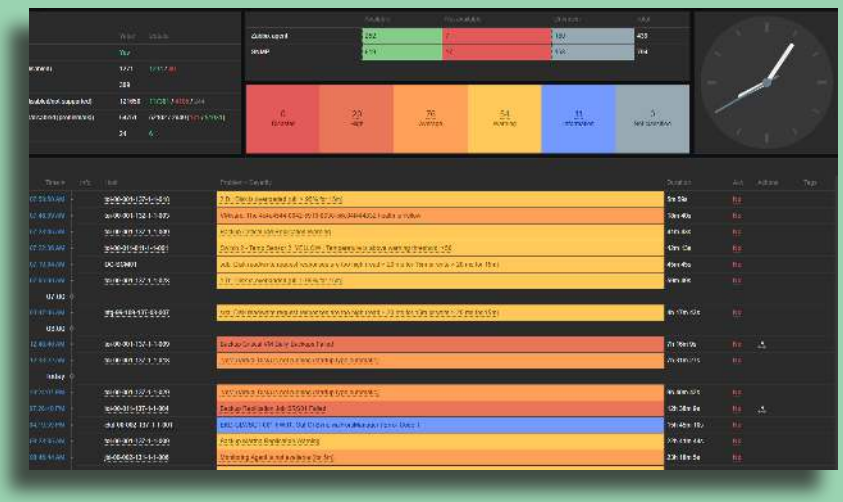
Remote work is increasingly popular these days. Special considerations for these employees include virtual firewalls and, crucially, virtual private network connection to their organization's network enabling traffic encryption.

Email Encryption

End-to-end encryption is a necessity for protecting the immense flow of communication via email. We make sure only senders and receivers with the proper decryption key can view the contents and attachments of sensitive emails.

Vulnerability Scanning

Vulnerability scanning is sort of the core of attack surface reduction. NTG utilizes continuous vulnerability scanning to monitor the status of software, hardware, network traffic, user activity, and our own security tools.



ROUND THE CLOCK OPERATIONS

Attacks happen at all hours of the day so our CSOC operates 24/7, 365 days a year. And there's always at least a couple analysts monitoring the tools. We're swift responders—our partners don't wait days for resolution. NTG is available when you need us to be.

THE METHOD

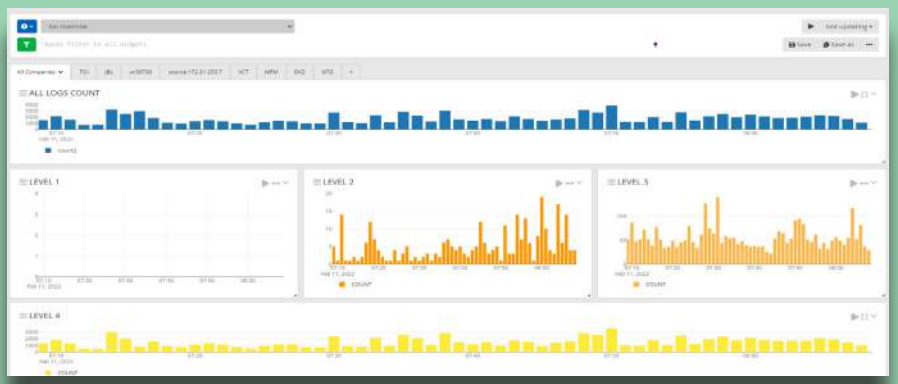
There's a rising concern that managed service providers and cybersecurity service providers are becoming prime targets for cybercriminals. "Buffalo jumping" is used by attackers to not only hold MSPs and MSSPs for ransom, but their customers as well.

We avoid the potential propagation of an attack by using proxy servers, virtual machines, and fine-tuned privileged access management. With this "jump box" method, our tools effectively monitor and alert to incidents without being **in** our partners' environments. If that sounds complicated, well...it is. Our engineers can give you the granular details. But at the end of the day, our partners will not be victims if NTG is targeted with a hard-hitting attack.

PROACTIVE APPROACH

Our tools collect and analyze millions of data logs on a daily basis. The majority of that data may appear mundane on the surface; device fan speed or chassis temperature, for example. But complete diagnostic capabilities help our CSOC analysts identify the most covert IOCs well before fullscale infiltration happens.

We aim to stop intruders at the gate. Intrusion Detection Systems (IDS) use AI to scan for anomalous network activity. IDS actively learns the normal day-to-day pattern of an organization's activity and alerts when something out of the ordinary (e.g. rogue processes or file modifications) occurs.



SIEM TOOLS

Security information and event management (SIEM) is a core element of most cybersecurity solutions. SIEM tools aggregate and analyze activity from network devices, domain controllers, servers, and so on across an entire IT infrastructure. Depending on the complexity of the infrastructure, SIEM tools need the capability to analyze several terabytes of data per day. There are dozens of SIEM tools on the market with excellent features but none of them have all the features cybersecurity professionals dream of.

Correlation, especially dynamic correlation, is a much desired SIEM feature. Correlation directives allow us to find the latest threats in a huge amount of disparate and varied event log data. Legacy SIEM tools don't always have the best correlation capabilities, which renders them useless in this time of constantly evolving threats.

As a vendor agnostic company, we've used several SIEM tools, incorporating the best features from all over the years. Now we're building a SIEM tool of our own:

Omniscient
Realtime
Correlating
Analyzer

THE ULTIMATE SIEM TOOL

Admittedly, omniscience in cybersecurity is an impossibility. We're getting close though.

ORCA incorporates AI, customizable correlation rules, and thorough analysis capabilities in realtime, delivering the ultimate SIEM solution for organizations of all sizes.

This is a SIEM tool created with years of experience in the most demanding sectors.

ORCA is being developed with adaptability in mind. The foremost predator of the depths stays ready at all times.

Bonus

CSOC SAVES THE DAY

You've learned about NTG's approach to cybersecurity operations—how our people, processes and tools comprise a formidable defense against the rising tide of anonymous and subversive attackers. You've also seen the headlines: billion dollar corporations hit with ransomware, Silicon Valley IP theft, sensitive data leaks from high-profile users, whole governments being taken offline. If these powerhouses can't stop an infiltration, how will NTG?

"Cybersecurity is a social responsibility. We all have a role to play."

-Magda Chelly, CISO, Cybersecurity Author

Larger organizations, especially in tech, retail, and government, have long been favorite targets for cybercriminals. They're also well equipped to deal with breaches (for the most part). Attacks do happen, and they do make headlines, but they rarely wipe out the organization entirely. For every million-dollar breach a Fortune500 company or state government experiences, a hundred small-to-medium sized businesses (SMBs) are hit hard with similar attacks. Attackers often test their methods on a small scale before going big.

To answer the question, nobody can stop all infiltrations, but we help our partners prepare defenses across more vectors than your average MSSP. In the event of a breach, our average time from detection to elimination is about 20 minutes. Attacks happen, but under our guidance, they'd make pretty boring stories.

"Local SMB falls victim to latest cryptolocker ransomware! (Detected, quarantined, systems restored from backup in twenty minutes. Minor emotional trauma reported among executive members)."

With NTG, guidance surpasses a basic "break/fix" or "detect/eliminate" methodology. We believe we're evolving the field of cybersecurity, and you're invited to join us in that endeavor.

CYBERSECURITY STATS

SINCE COVID-19, THE FBI REPORTED A 400% INCREASE IN REPORTED CYBERCRIMES

43% OF CYBER ATTACKS TARGET SMALL BUSINESS (FEWER THAN 500 EMPLOYEES)

95% OF CYBERSECURITY BREACHES CAN BE ATTRIBUTED TO HUMAN ERROR

CYBERATTACK FREQUENCY

- 14% SOCIAL ENGINEERING
- 10% ADVANCED PERSISTENT THREAT
- 9% RANSOMWARE
- 9% UNPATCHED SYSTEM
- 8% DENIAL OF SERVICE
- 8% SECURITY MISCONFIGURATION

Sources: Cybint, ISACA's State of Cybersecurity 2021

Nobody wants to be a part of these statistics. NTG's CSOC can save the day.

THANK YOU FOR READING

ABOUT NTG

NTG is a minority woman owned business located in beautiful Tampa, Florida since 2002. In the last two years, NTG has tripled its customer base by providing superior service in the IT Managed Services and Cybersecurity space. We are proud to work with a variety of organizations locally and abroad, including government agencies, healthcare facilities, and financial institutions. Give us a call, visit our website, or stop by our office and find out what NTG can do for you.

14413 N Nebraska Ave
Tampa, FL 33613

(813) 885-7500

ntgit.com

NTG
Leave IT to us