Secure IT

for middle market operations

What is **Secure IT**?

Secure IT is a CRAG-designed cybersecurity solution deployed to:

- prevent operational downtime from threats and disruption
- meet and support your compliance framework and liability requirements
- build digital trust your customers count on
- help move your organization from cyber awareness to true digital agility and alignment

Expect the best from CRAG **Secure IT**:

- 24×7×365 Security Operations Center (SOC) services
- Active prevention, detection, response, and threat hunting across all operating systems
- Leading-edge phishing and email defense
- Cyber compliance reporting (SOC 2, CMMC, HIPPA, etc.)
- Network scanning, security monitoring, and vulnerability management

- Cybersecurity awareness and simulation training for employees
- Microsoft 365 cloud infrastructure defense

Why we exist

CRAG exists to make the work lives of our clients easier and more secure.

How we work

Competence

Technically excellent work by self-starters who work together well

Empathy

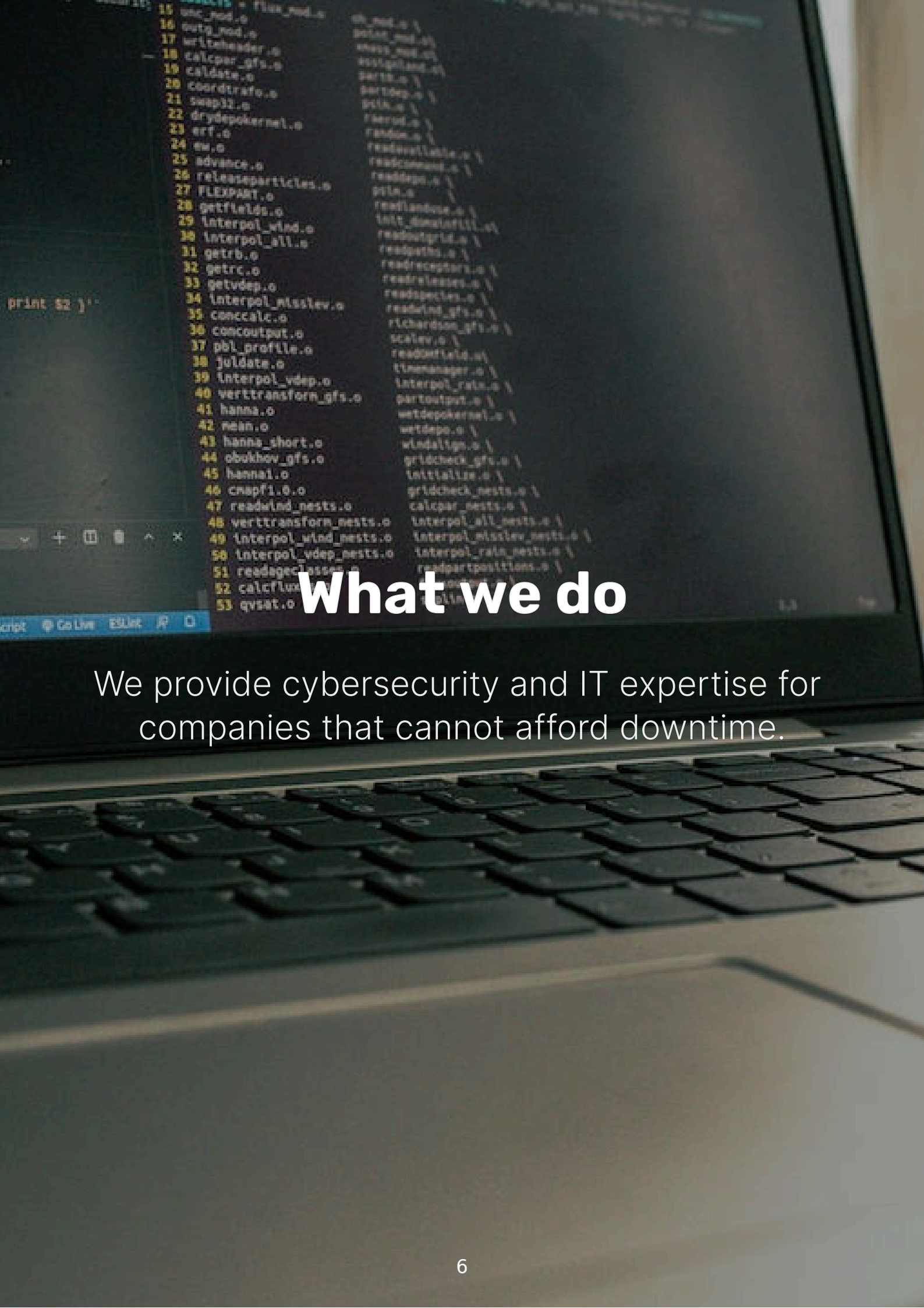
Professional, fun, low stress attitude that puts our clients' work first

Consistency

Predictable results and crazy-good automation

Vigilance

Constant awareness and proactive responses to the security threats that could otherwise disrupt your business



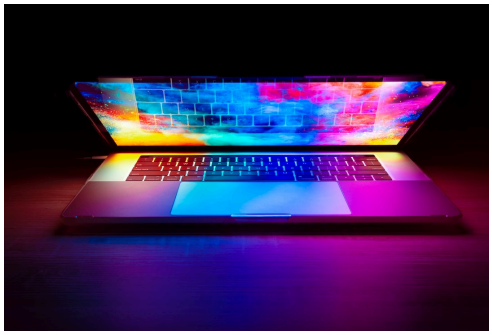
What we do

We provide cybersecurity and IT expertise for companies that cannot afford downtime.

How we succeed

Our People

- Technically competent and vigilant
- Work anywhere with an ownership mentality
- Integrity in all things



Our Systems

- Top of the line security tech stack
- Cyber compliance frameworks integrated into managed IT
- Active automation, bringing faster response times and consistent results
- Root cause analysis and problem solving. Like a dog with a bone until we find the root cause.

Our Alignment

- Long term partnerships over short term profit
- Clients who value excellent, total service
  delivery over lowest short-term cost
- Clients aligned with our values

Meet our industry leading Security Operations Center

With **Secure IT**, CRAG protects your infrastructure and ensures you remain compliant through our enterprise-level Security Operations Center.

Our SOC is an elite team of Cybersecurity Analysts who proactively hunt and investigate threat activity across your operational systems. Our SOC performs the triage of detections and works with our Network Operations Center (NOC) on the remediation when an actionable threat is discovered. Our SOC performs critical cybersecurity activities including:

- Security monitoring, threat analysis tool deployment (with security operations)
- Firewall and intrusion prevention system management and antivirus support
- Detection of malicious and suspicious activity across three critical attack vectors:
  - Endpoint
  - Network
  - Cloud

Key Roles

Our SOC is staffed by security veterans working on your behalf to prevent threat activity, disruption, and downtime. This level of expertise requires specialized education and training beyond IT generalists. CRAG hires for degrees rather than certifications.

Hiring a large team of cybersecurity experts with technical capabilities necessary to secure all your IT and keep it compliant is not feasible for most companies. Businesses with cyber compliance requirements hire CRAG to secure their information infrastructure and safeguard compliance performance.

SOC Design and Operations

Our SOC leverages a Threat Monitoring Platform to detect malicious and suspicious activity that evade traditional cyber defenses across three critical vectors: endpoint, network, and cloud. This platform is fueled by a multi-tenant cloud architecture with integrated threat intelligence and a built-in app store delivering 24/7 threat monitoring. **Why CRAG #1: 24×7×365 "real person" security monitoring with expert training and tools.**

Our endpoint defense is AI-powered with pre-execution protection for known and unknown file-based malware, plus behavioral monitoring that covers any attack vector, including unknown exploits and bypass attempts of traditional anti-virus. **Why CRAG #2: We're committed to only top-of-the-line security software and hardware so your digital reputation stays safe.**

Intrusion Monitoring offers real-time safeguarding against suspicious activity, protecting against threats from terrorist nations, unauthorized TCP/UDP services, and backdoor connections to C2 servers. For NextGen Malware, CRAG uses industry-leading malware prevention, backed up with a secondary line of defense using real person monitoring for malicious detection of files, tools, processes and more. **Why CRAG #3: Over 4,000 attacks blocked with 0 successful breaches.**

Our SOC maintains a risk assessment and remediation program aligned with your cybersecurity compliance framework. The risk management platform meets all requirements that are part of the IDENTIFY core function of the NIST cybersecurity framework. The scanning agent identifies risks and vulnerabilities aligned with SOC 2, CMMC 2.0, and HIPPA (examples) for our technicians to remediate. **Why CRAG #4: Robust, turnkey cybersecurity compliance management.**

SOC services require a 50-device minimum. Billing is processes per device, defined as any of the following types that communicate with the SOC during the monthly billing period:

- Windows OS device running Windows 7, 8, or 10
- Windows Server OS device running Windows Server 2008R2, or Windows Server 2012, 2016, or 2018.
- macOS device running macOS 10.14 or higher
- Firewalls from Barracuda, Cisco Meraki, Fortinet, PfSense, SonicWall, Sophos, WatchGuard, Ubiquiti, and Untangle.

Secure IT Plan Details

CRAG Managed SOC

- Our team of cybersecurity experts as your defense:
  - 24×7×365 continuous monitoring services
  - Always-on threat detection in real-time
  - No hardware required
  - SIEMless log monitoring
  - Threat intelligence, hunting, and remediation

- Breach detection and intrusion monitoring
- XDR malware protection integration
- PSA ticketing

CRAG Extended Detection & Response (XDR)

- Top-of-the-line endpoint defense
- Autonomous artificial intelligence
- Enterprise proved and easily scalable
- Certified and recognized as an industry-leading solution
- Helps eliminate notification fatigue
- Single, holistic agent for PC, Mac, Linus, VDI
- Multi-layered AI-powered endpoint protection
- Advanced Threat Hunting and device controls
- Policy-driven response to threats

CRAG MS 365 Cloud Backup + Email Archiving

- Exchange Online backup
- Gmail and Outlook backup
- Calendars, Tasks, and Attachments backup for Microsoft 365 & Google
- OneDrive / SharePoint backup and My Drive / Shared backup
- Microsoft Teams backup
- Insights email business intelligence
- Journaling-based email archiving for Exchange, Gmail, IMAP or POP protocols to preserve, search, hold and comply with GDPR, HIPPA, SOC2, ISO 27001, SSAE16

CRAG Phishing & Spam Defense Core

- Provides real-time email content scanning
- Prevents email spoofing and impersonation emails
- Reduces risk of financial loss
- Enables users to be part of the email phishing protection solution
- Reduces phishing click rates through continuous training
- URL/Link and attachments scanning
- Unique machine learning algorithms
- Sender fingerprinting
- Inbox behavioral analysis
- Automated phishing forensics, orchestration and remediation
- Account takeover detection and response

- Microsoft Teams protection
- SSO and application API support

CRAG Simulation & Training Premium

- Phishing simulations with immediate feedback and training
- Engaging and fun videos
- Improved user participation
- Participation tracking and reporting

CRAG Network Scanning & Security Monitoring

- Complete asset discovery
- Track end user VPN connections
- User behavior tracking

CRAG IT Vulnerability Management

- Vulnerability tracking across assets and groups
- Mitigates risks and shadow IT
- Lowers risk by security Active Directory
- Checks if routers are hackable

CRAG Compliance Reporting

- Based on the client's cybersecurity framework (SOC 2, HIPPA, CMMC 2.0)
- Risk assessment across an organization
- Users and clients stay compliant

Microsoft 365 defense for cloud files (optional)

- Guards against unknown and sophisticated attacks
- Protects Microsoft Teams, Word, Excel, PowerPoint, Visio, SharePoint, and OneDrive
- Allows for investigation of blocked messages
- Safe Attachments prevents threats from malicious email attachments
- Safe Links protects your environment when users click a link
- Advanced threat reporting

We make onboarding simple

...

STEP ONE

Complete our survey

1 Week

Satisfaction survey for current IT
"If you could fix 1 issue..."

STEP TWO

Deploy systems

2-4 Weeks

Support software
Monitoring and management software
Communication with your employees

STEP THREE

Complete onboarding

2-4 weeks

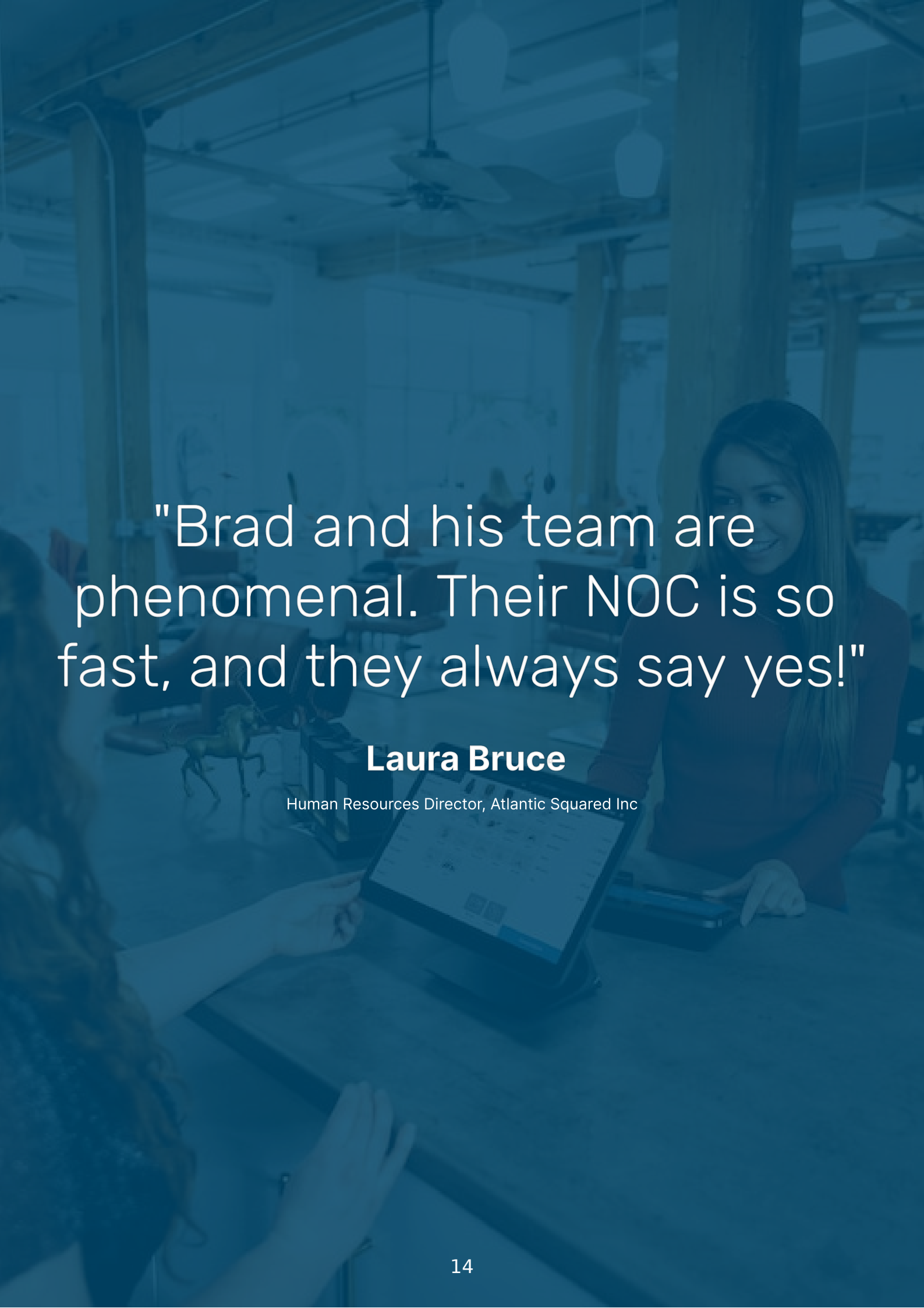
Outliers
Initial security scans & mapping
Communication with your employees

STEP FOUR

Continuous improvement

1+ years

Digital transformation
IT agility and alignment
Security landscape



"Brad and his team are phenomenal. Their NOC is so fast, and they always say yes!"

Laura Bruce

Human Resources Director, Atlantic Squared Inc

"You can't beat the customer service. Brad's staff is sharp and on top of it."

Matt Neely

Vice President, Multifamily Select Inc.

"CRAG migrated us to the cloud. They're very fast and responsive. Great MSP partner."

Steve Stradtman

CEO, International Consortium Inc

Have questions?

Get in touch →

CRAG
CYBER RISK ANALYSIS GROUP