



INTRODUCING  
3HUE VIRTUAL  
CIO-ISC  
SERVICES



# **BUSINESS JUSTIFICATION PACKAGE**

## Virtual CIO-ISG Solutions | Introduction

As your organization grows, your technology infrastructure and information security posture become increasingly complex. It can be challenging to keep up with emerging technology trends, regulatory compliance requirements, and the constantly evolving threat landscape. This is where a 3HUE Virtual CIO-ISG services come in. Our ISG services provides a platform for continuous strategic guidance and technical expertise required to help your organization achieve its goals while maintaining a strong security posture.

---



## Statistics & Trends

---

Use the statistics & trends in this section to define the business problem requiring management consideration for justification of budgeted Information Security Initiatives

## DID YOU KNOW?

### 3.5 million unfilled cybersecurity roles

Unfilled global cybersecurity roles expected in 2023. Seen as a leading risk to US-based organizations.

### 49% increase in SMB data breaches in 2021

The rate of SMB companies experiencing a data breach in the U.S. and Canada from 2020 to 2021.

### Remote work makes security more demanding

61% of US-based organizations feel under scrutiny to prove the business takes information security seriously, with 57% feeling more likely to experience a data breach.

## The Impact to your business

### 92.4% of consumers want improved privacy

Of 1,939 respondents surveyed, 92.4% considered it important to have more control over their personal data and how it is shared.

### Breakout time from Initial Access to lateral movement decreasing

Length of time it took for malicious adversaries to move from initial access to lateral movement decreased from 98 minutes to 84 minutes. Adversary tactics are improving

### Key threat indicators on the rise since the start of the pandemic

**667%**  
increase

Email Scams

**2000%**  
increase

Malicious files  
named Zoom

**40%**  
increase

Unsecure  
Desktops

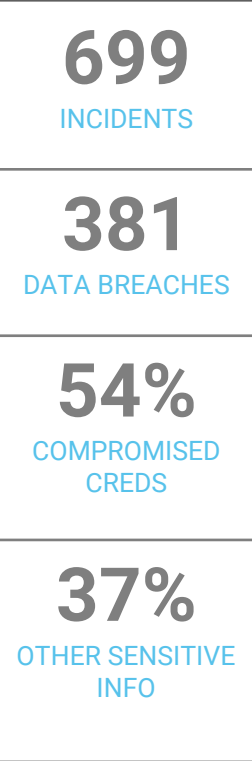
# 2022-23 Review of the Cybersecurity Landscape for Small, Midmarket and Large US-based Organizations

### Small businesses (less than 1,000 employees)

<b>Frequency</b>	699 incidents, 381 with confirmed data disclosure
<b>Top patterns</b>	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
<b>Threat actors</b>	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)
<b>Actor motives</b>	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)
<b>Data compromised</b>	Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches)

Table 3. At a glance for SMB

### Key Statistics

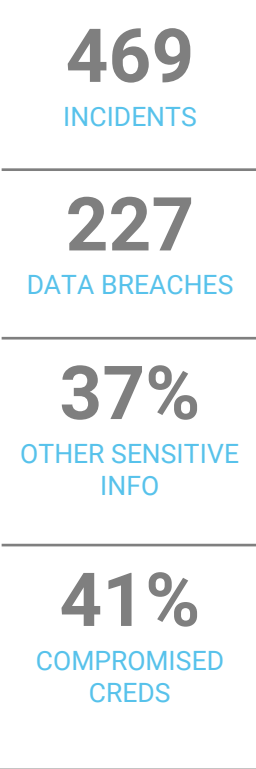


### Large businesses (more than 1,000 employees)

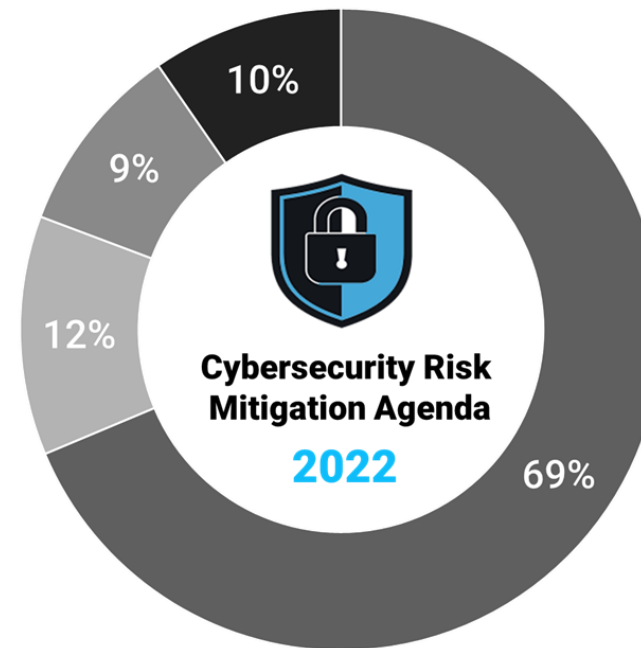
<b>Frequency</b>	496 incidents, 227 with confirmed data disclosure
<b>Top patterns</b>	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
<b>Threat actors</b>	External (89%), Internal (13%), Multiple (2%), Partner (2%) (breaches)
<b>Actor motives</b>	Financial (97%), Espionage (3%), Ideology (2%), Convenience (1%), Fun (1%) (breaches)
<b>Data compromised</b>	Internal (41%), Credentials (37%), Other (30%), System (22%) (breaches)

Table 4. At a glance for large organizations

### Key Statistics



# Most important cybersecurity risks perceived by CIOs in the United States in 2022



- 69% ■ Ransomware attack
- 12% ■ Compromises to the software supply chain
- 9% ■ Agency use of shadow IT solutions or products
- 10% ■ Stolen identities /fraudulent claims for benefits (UI, SNAP, etc.)



# Most important cybersecurity risks perceived by CIOs in the United States in 2022

## Adversaries Continued to Move Beyond Malware to Gain Initial Access and Persistence

There was a continued shift away from malware use, with malware-free activity accounting for 71% of all detections in 2022 (up from 62% in 2021). This was partly related to adversaries' prolific abuse of valid credentials to facilitate access and persistence in victim environments. Another contributing factor was the rate at which new vulnerabilities were disclosed and the speed with which adversaries were able to operationalize exploits.

**ADVERSARY TACTICS** ■ Malware-Free

**71%** 2022

62% 2021

51% 2020

40% 2019

39% 2018



**Shift in Adversary Tactics:** There has been a noticeable move away from the use of malware by adversaries.

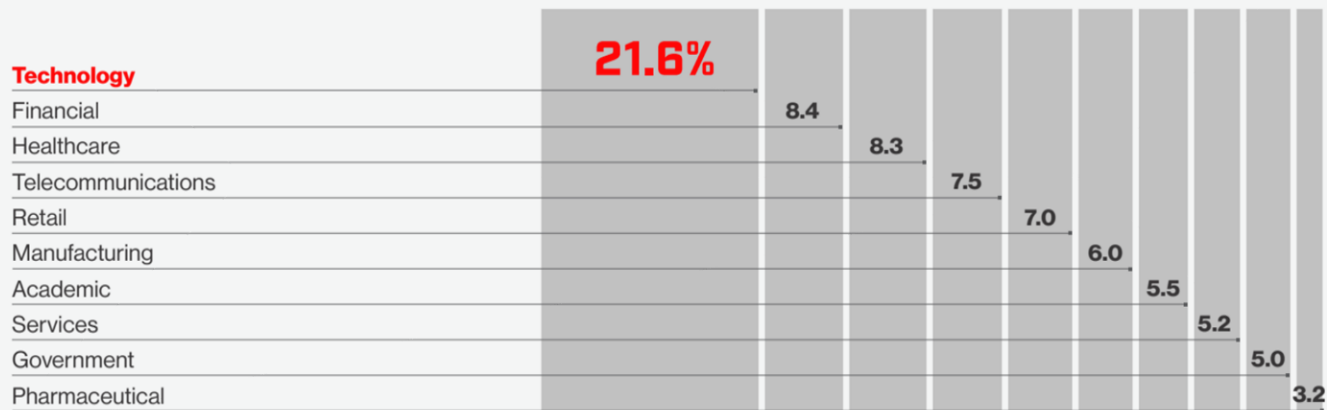
**Malware-Free Activity:** In 2022, 71% of all detections were malware-free, showing a rise from 62% in 2021.

**Use of Valid Credentials:** A significant factor in this shift is the adversaries' widespread use of valid credentials. This allows them to gain initial access and maintain persistence in victim environments.

**Vulnerability Disclosure Rate:** The rate at which new vulnerabilities are being disclosed and the speed of adversaries capitalizing on these vulnerabilities are also notable contributing factors.

# Top 10 Verticals by Intrusion Type during 2022 – 2023 across US-based entities

TOP 10 VERTICALS BY INTRUSION FREQUENCY



## Summary of Action on Objectives for Top 3 Vectors

### Technology sector (21.6%):

- Threats from hackers seeking proprietary technology.
- State-sponsored attacks targeting technological advancements.
- Insider threats compromising systems and data.

### Financial (8.4%):

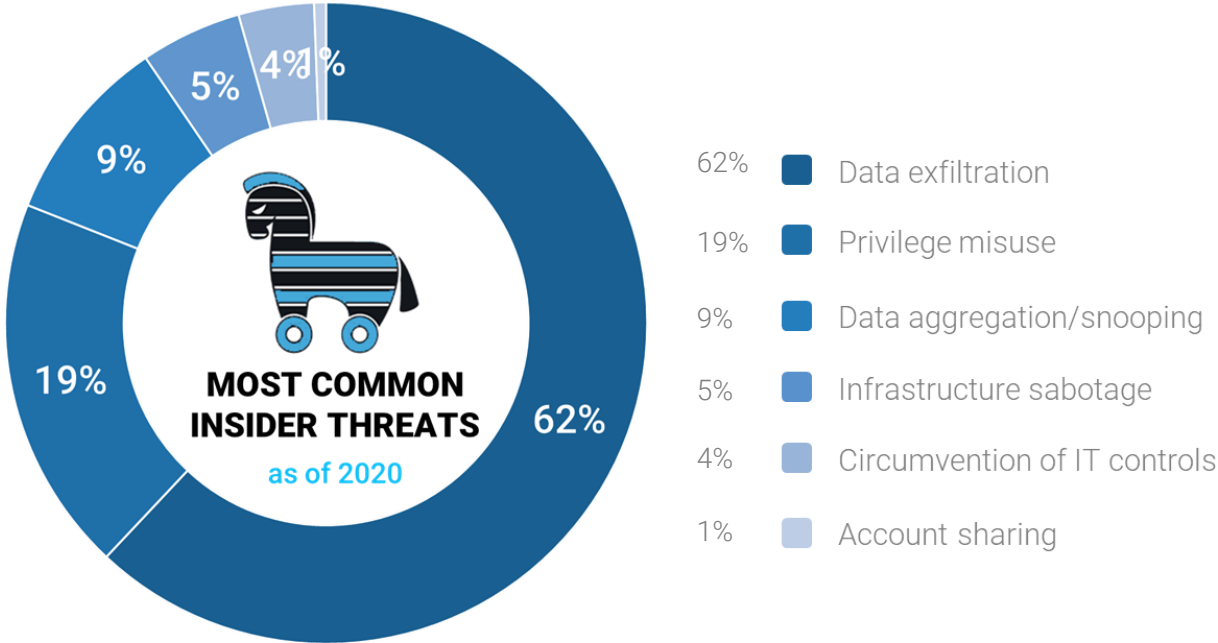
- Attacks targeting online banking and transactions.
- Phishing attempts to gain customer credentials.
- Insider trading and fraudulent schemes.

### Healthcare (8.3%):

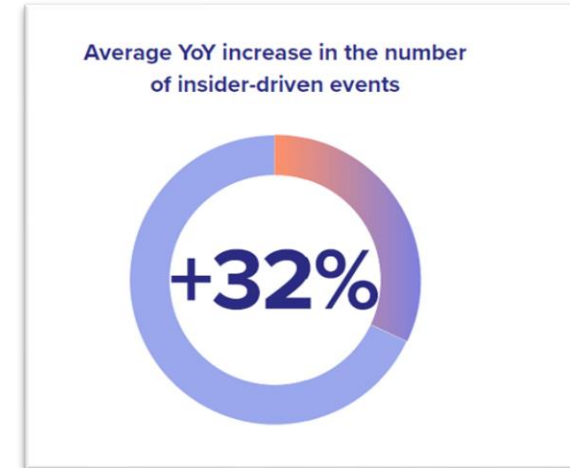
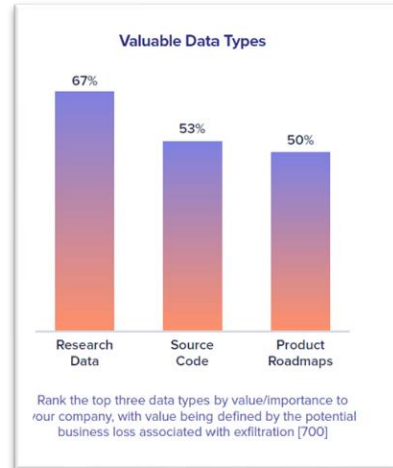
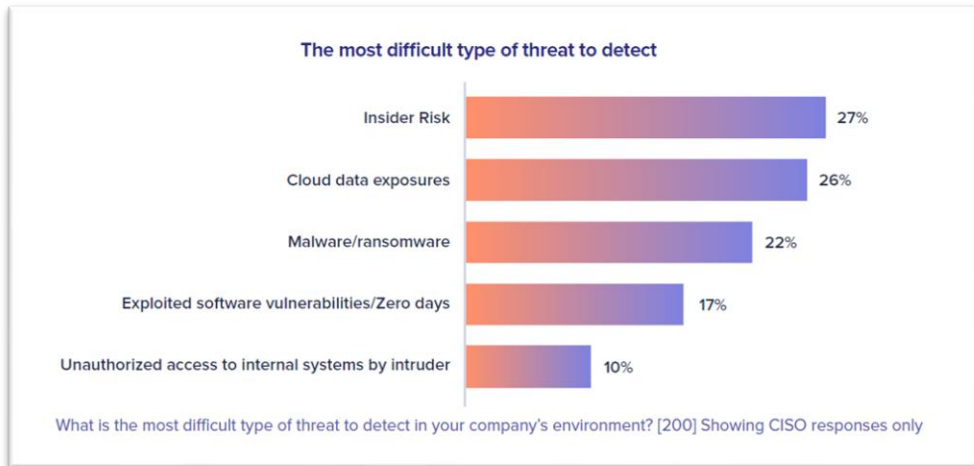
- Ransomware attacks targeting critical health data.
- Unauthorized access to patient records.
- Medical device vulnerabilities.



# Most common types of insider threats in the United States in 2020



# Analyzing the Insider Threat in 2023 as a top data exfiltration vector. Organizations need to do more to mitigate!



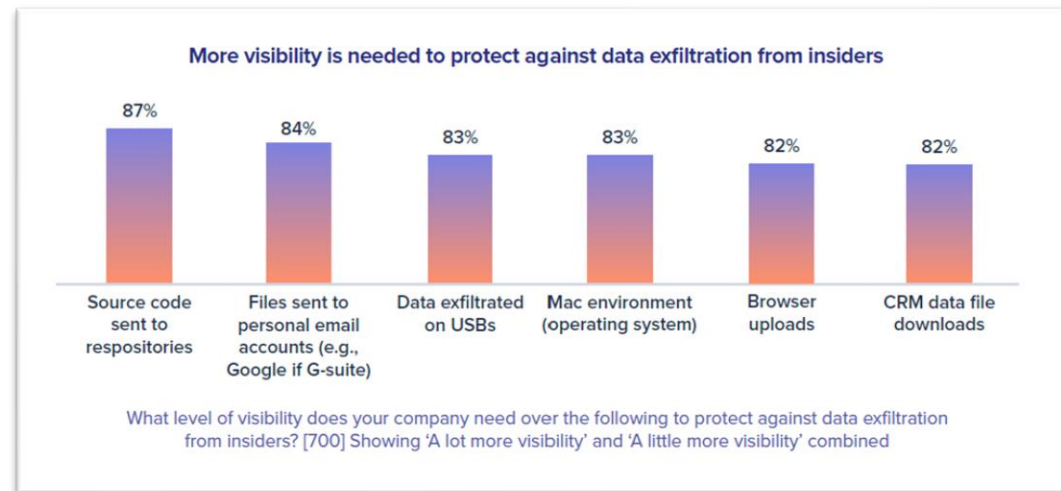
Data loss from insiders is a growing problem despite 72% of organizations having a program dedicated to Insider Risk

**32%**

The average year-over-year increase in the estimated monthly number of insider-driven data exposure, loss, leak and theft events

**\$16M**

Insider-driven data exposure, loss, leak and theft events could cost companies \$16 million per incident, on average.





## Self-Managed Comparative TCO

---

This sections presents an Total Cost of Ownership (TCO) analysis which compares the self-managed approach to using 3HUE Virtual CIO-ISG Managed Programs and Managed SOC Services

# ISG Solutions | Economics of Establishing Strong GRC Management

Software	QTY	Unit Price	Ext Price
Full-time CISO	1	\$ 235,000	\$ 235,000
Security Architect - US-based	1	\$ 185,000	\$ 185,000
Senior GRC Analyst - US-based	2	\$ 160,000	\$ 320,000
Senior Risk Analyst - US-based	1	\$ 182,000	\$ 182,000
Staffing Fringe Benefits	4	\$ 25,763	\$ 103,052
<b>STAFFING TOTAL</b>		<b>\$</b>	<b>\$ 1,025,052</b>
GRC Management System Licenses	12	\$ 7,000	\$ 84,000
KnowBe4 Security Awareness & Training	100	\$ 21.95	\$ 21,950
<b>TOTAL ANNUAL RECURRING COST</b>		<b>\$</b>	<b>\$ 105,950</b>

## Compared to ISG-OPS



## For 100 Users

- GRC Management System
- Policies, Standards, Procedures and Plans
- Manage Control Catalog
- Annual Controls & Risk Assessment
- Periodic Controls Review
- Risk Register and POA&M Management
- Semi-annual Firewall Security Review
- Annual Internal Compliance Assessment
- Vendor Security Certification
- Third-party Risk Management
- Supply-chain Risk Management
- PCI-DSS Third-party Audit Support
- SOC 2 Type II Audit Support
- Security Operations Oversight, Advisory & Architecture Support

Staffing Spend:

**\$ 1,025,052**

Technology Spend:

**\$ 105,950**

**Annual Total  
Cost of Ownership (TCO)**

**\$1,131,002**

**3HUE-ISG Estimated Total  
Cost of Ownership (TCO)**

**\$ 192,850.00**

Based on an enterprise with less than 1000 assets, 500 controls, and no more than 60 vendors with access to sensitive data. Managed programs include ISP, RMP, SCS, VCP and CIRP.

# ISG Solutions | Economics of building your own Security Operations

Software	GB/Day	Unit Price	Ext Price
Splunk Cloud	24	\$ 1,200	\$ 28,296
DarkTrace		\$ 50,000	\$ 50,000
Nessus Professional		\$ 2,390	\$ 2,390
Incident Response Retainer		\$ 10,000	\$ 10,000
Crowdstrike Complete		\$ 120	\$ 13,200
Umbrella Advantage		\$ 52	\$ 5,720
KnowBe4 Diamond		\$ 30	\$ 3,300
Proofpoint Email Security Essentials Pro		\$ 54	\$ 5,720
Network Performance Monitor		\$ 2,995	\$ 3,594
Network Topology Mapper		\$ 1,495	\$ 1,1794
Network Configuration Manager		\$ 4,195	\$ 5,034
IP Address Manager (up to 1024 Ips)		\$ 1,995	\$ 2,394
Illumio Core		\$ 354	\$ 3,540

**SOFTWARE TOTAL** \$ 145,162

Staff	Qty	Price	Extended Price
SOC Manager	1	\$ 90,000	\$ 90,000
SOC Analyst	4	\$ 60,000	\$ 240,000
Fringe Benefits		25%	82,500

**TOTAL ANNUAL RECURRING COST** \$ 547,702

## Compared to ISG-OPS

**5x**  
Staffing Costs

**1.7x**  
Technology Costs

## For 100 Users

- SIEM
- Network anomaly detection
- Vulnerability Scanning
- Incident Response Retainer
- Endpoint Security
- DNS Security
- Security Awareness Training
- Email Security
- Network Monitoring
- Micro-segmentation
- N-SOC Staffing

Software Spend:

**\$ 145,162**

Staffing Spend:

**\$ 547,702**

**Annual Total  
Cost of Ownership (TCO)**

**\$547,702**

**3HUE-ISG Estimated Total  
Cost of Ownership (TCO)**

**\$ 89,520.00**

Based on an enterprise with 105 users, using XDR Complete and ZTNA Premium for all users.





# ISG-GRC Managed Programs

---

This section summarizes key details about the 3HUE  
Virtual CIO-ISG Managed programs

# 3HUE Solutions | Our Managed Service Modules

Service Mark	Service Reference	Description	Use Cases	Key benefits
	<b>ITG Services</b> Become more efficient, agile, and competitive.	Our ITG module helps organizations assess its current technology landscape, identify gaps and opportunities for improvement, prioritize technology initiatives, develop, and implement a roadmap for achieving digital transformation goals, and provide ongoing support for technology initiatives.	<ul style="list-style-type: none"><li>• Strategic IT Planning</li><li>• IT Modernization</li><li>• Digital Transformation</li><li>• Digital Product Development</li></ul>	<ul style="list-style-type: none"><li>• Improved productivity and efficiency</li><li>• Increased agility and flexibility</li><li>• Enhanced customer experience</li><li>• Competitive advantage</li></ul>
	<b>ISG Services</b> Protect assets, maintain regulatory compliance, and reduce the risk of cyberattacks.	Our ISG module helps your organization assess its current security posture, identify vulnerabilities and risks, develop and implement policies and procedures to ensure system and data security, monitor and manage security posture, and provide employee training and awareness programs. This module can help your organization protect its assets, maintain regulatory compliance, and reduce the risk of cyberattacks.	<ul style="list-style-type: none"><li>• Information Security Management</li><li>• Enterprise Information Security Risk Management</li><li>• Vendor Security &amp; Privacy Compliance Management</li><li>• Incident Response operations planning and support</li></ul>	<ul style="list-style-type: none"><li>• Reduced risk of cyberattacks and data breaches</li><li>• Compliance with regulatory requirements</li><li>• Protection of assets and intellectual property</li><li>• Better financial planning and risk management</li><li>• Enhanced reputation and customer trust</li><li>• Avoidance of legal and financial penalties</li><li>• Enhanced business continuity and disaster recovery capabilities</li></ul>



# ISG-GRC | Our Managed Programs



## Virtual CISO

Pairs our experienced CISO-level professionals with your in-house CIO, CISO or head of information security to provide advisory and mentorship for the management of Information Security

3HUE-ISG Analysts, Architects & Engineers reporting to the vCISO



### ISP

Information Security Program

Sets Policies, Standards, Controls for Information Security



### RMP

Risk Management Program

Annual Risk Assessment with Continuous Operational Risk Reviews



### VCP

Vendor Compliance Program

Sets Minimum Security Requirements for Vendors and Certifies their Posture at onboarding and annually



### CIRP

Incident Response Planning

Cyber-Incident Response Planning & Operations to include annual simulations & table-top exercises



### SCS

Security Compliance Services

Continuous Security & Privacy Compliance Management to include automated Change Detection



## vCISO

Virtual CISO Management

### Virtual CISO - CISO Support

Benefit from our recommended strategy, which pairs our experienced CISO professionals with your in-house CIO or CISO to provide coaching and mentorship. This collaboration empowers them to lead your organization's information security strategy, architecture, and operations effectively. Our comprehensive 3HUE ISG Programs and dedicated ISG team support this partnership for optimal results.

### Key Benefits

- Bi-weekly CISO Coaching Sessions (90 Minutes)
- Weekly Operational Alignment w/ Cyber-Risk Advisory (90 Minutes)
- Quarterly Board Communications Update Package development (3 hours)
- Security Audit Support





Virtual CISO Management

## Virtual CISO – Fractional CISO

Discover our Fractional CISO service, perfect for organizations that don't require a full-time CISO. With flexible time commitment options, our vCISO offering is customized to fit your organization's specific needs. Enjoy expert guidance and strategic security leadership while avoiding the costs associated with a full-time role.

## Key Benefits

- CISO Staff Augmentation
- Information Security Strategy Development
- Enterprise Roadmap Development
- Board of Directors Update
- Monthly IT Leadership Alignment meeting
- Annual Security Budget Planning w/ one reforecast
- IS Staff Documented Talent Review
- Prospect Interviews
- Analysis of Customers Trust & Perceptions
- M & A Due Diligence
- Weekly Operational Alignment (90 Minutes)
- Quarterly Board Communications Update Package development (3 hours)
- Provide periodic project status and risk posture reporting to senior management and the board of directors.
- Provide information security support to business stakeholders as required.
- Security representation for change management processes
- Talent assessment, selection, and leadership of security staff and service providers
- Facilitate training opportunities and provide guidance to corporate staff on security issues



Information Security Program

## Information Security Program Management

Enhance your organization's information security with our expert services, designed to align with your business goals and risk tolerance. We specialize in creating secure network and system architectures, implementing industry-leading security controls and configurations. Trust us to safeguard your digital assets and maintain operational efficiency.

## Key Benefits

- Scoped Internal Control baseline using the Secure Control Framework for alignment to all in-scope frameworks and standards
- Development of information security policies and standards aligned with your risk posture
- Annual Reviews and updates to meet evolving regulatory requirements and risk tolerances
- Security Exceptions Request and Management process
- Security Awareness Training Program Architecture
- Annual Reviews & Updates for Information Security polices & standards
- Maintenance of the Business Process Inventory



## Operational Risk Management

The GRC Operational Risk Management service offers a comprehensive approach to managing operational risks, with continuous tracking and insightful reporting of potential risks through the development of risk intelligence reports with data from platforms such as AV, EDR, Vulnerability & Patch Management, Cloud Security Posture Management, SIEM, backup/restore, and incident response. This all-inclusive solution streamlines risk mitigation, ensuring timely identification, prioritization, and resolution of security concerns, fostering a proactive and resilient security posture.

(up to 500 Controls)

## Key Benefits

- Establishment or Alignment with objectives of the organizations Risk Committee or Information Security Steering Committee
- Month over Month (MoM), Quarter over Quarter (QoQ), Year over Year (YoY) performance analysis and reporting across all in-scope security programs
- Risk Register & POA&M Management
- Weekly Cyber-Risk Leadership Advisory Meetings (90-minutes)
- Weekly Operational Risk Team Meetings



## Business Impact Analysis

The Business Impact Analysis service provides a structured methodology for assessing the potential consequences of disruptions to critical business processes. By identifying vulnerabilities and prioritizing recovery strategies, this service enables organizations to enhance their resilience and minimize downtime in the face of unforeseen events.

(Up to 50 Business Processes)

## Key Benefits

- Interview key stakeholders, such as business leaders, IT staff, and relevant personnel, to identify and prioritize critical business functions.
- Identify dependencies between critical business functions and IT systems, applications, and data.
- Determine maximum allowable downtime for each critical business function and IT system, application, or data.
- Assess potential impact of disruption or outage on critical business functions and IT systems, applications, and data.
- Develop mitigation strategies to reduce disruption or outage impact on critical business functions and IT systems, applications, and data.
- Create recovery strategies for restoring critical business functions and IT systems, applications, and data in case of disruption or outage.
- Prioritize recovery of critical business functions and IT systems, applications, and data based on importance to organizational operations and mission.
- Conduct annual review and update of BIA to ensure alignment with current state of organization's critical business functions and IT systems.
- Provide ongoing support for implementing or modifying business continuity and disaster recovery contingency plans during disruptions or outages.



## Privacy Protection Services

Privacy Protection Services provide a comprehensive solution for managing sensitive data, encompassing data mapping, discovery, and impact assessments. By identifying and mitigating potential privacy risks, this service ensures compliance with privacy regulations and fosters trust in an organization's responsible handling of personal and sensitive information.

(Up to 25 Systems)

## Key Benefits

- Identify DPIA scope, covering systems, networks, data, and processes handling personal information.
- Determine applicable data protection laws and regulations and their requirements.
- Identify data flows, including personal data types, data subjects, sources, and recipients.
- Recognize potential risks and threats to data subjects, such as unauthorized access, use, disclosure, and destruction.
- Evaluate necessity and proportionality of personal data processing, including legal basis, purposes, and benefits.
- Assess potential impact on data subjects, considering their rights, freedoms, and interests.
- Develop mitigation strategies and plans to address risks and threats, incorporating technical and administrative controls.
- Prioritize recommendations based on potential impact and implementation feasibility.
- Create an action plan outlining procedures and resources needed for implementing recommendations and enhancing data protection and privacy compliance.
- Provide ongoing support to assist with action plan implementation.





Vendor Compliance Program

## Periodic Vendor Security Due Diligence

Establish and maintain processes for securely onboarding and offboarding vendors, including conducting background checks, access management, and data transfer protocols.

(up to 10 Vendors)

## Key Benefits

- Identify vendors with access to organization's systems, networks, data, or facilities.
- Request vendor documentation, such as security policies, procedures, and controls, to evaluate their security posture.
- Review vendor documentation for compliance with organization's minimum-security requirements.
- Conduct on-site visits to validate vendor security controls and adherence to organization's minimum-security requirements.
- Perform vulnerability assessments on vendor's systems and networks to identify potential weaknesses.
- Assess risks and threats related to vendor access to organization's systems, networks, data, or facilities.
- Review vendor's incident response procedures for alignment with organization's minimum-security requirements.
- Develop recommendations to improve vendor's security posture based on assessment findings.
- Prioritize recommendations considering potential impact and implementation feasibility.
- Create a remediation plan outlining procedures and resources needed for implementing recommendations and enhancing vendor's security posture.
- Regularly review and update vendor security compliance due diligence process to reflect changes in minimum-security requirements, technology, and business operations.
- Provide ongoing support to ensure vendor compliance with minimum security requirements and assist with remediation plan implementation.



Vendor Compliance Program

## Vendor Performance Monitoring

Monitor vendors' security performance metrics and service level agreements (SLAs) to ensure they are meeting the required security and compliance standards.

(up to 10 Vendors)

## Key Benefits

- Establish vendor performance metrics, including quality, timeliness, and accuracy.
- Monitor vendor performance against metrics, covering goods/services delivery, timeline adherence, and work quality.
- Conduct regular vendor check-ins to review performance and discuss concerns or issues.
- Document vendor performance, maintaining records of issues, concerns, or successes.
- Address performance issues collaboratively, developing improvement plans with the vendor.
- Escalate unresolved performance issues to relevant parties within the organization or vendor's management.
- Collaborate with the vendor to create improvement plans addressing performance issues and setting future expectations.
- Conduct periodic reviews assessing vendor performance and adherence to organization's minimum-security requirements.
- Review vendor contracts for alignment with organization's minimum-security requirements and monitor compliance.
- Provide ongoing support to ensure vendor compliance with security requirements and assist with implementing improvement plans or performance metrics.



## IRO Operations Management

Provide ongoing support for maintaining and updating the incident response operations program, procedures, playbooks, and remediation plans based on technological, business, and regulatory changes.

## Key Benefits

- Ongoing evaluation of incident response plan effectiveness in addressing security incidents and meeting organizational objectives.
- Analyze incident data for trends and improvement opportunities in response procedures and processes.
- Formation of incident response teams with assigned roles and responsibilities.
- Train employees on incident response procedures, roles, and responsibilities to ensure understanding and compliance.
- Conduct incident response drills to assess procedure and playbook effectiveness.
- Integrate Key Service Provider Incident Response Simulation and Testing.
- Develop remediation plans addressing weaknesses or non-compliance found during drills or evaluations.
- Review incident response team performance and pinpoint improvement areas.
- Provide ongoing support for maintaining post-incident reporting, lessons learned processes, and process improvement implementation.



## Incident Response Command

Our Incident Command Service provides organizations with a structured, efficient, and coordinated approach to manage and resolve security incidents. Our expert team of professionals leverages industry-standard frameworks and best practices to ensure swift incident identification, containment, eradication, and recovery. This service includes incident response planning, communication, and coordination among various stakeholders to minimize potential damage, reduce recovery time, and maintain business continuity. With ongoing support, proactive monitoring, and post-incident analysis, our Incident Command Service helps organizations build resilience and continually improve their security posture.

## Key Benefits

- Investigate security incidents to determine nature, extent, affected systems, and data.
- Collaborate with Security Service Providers for incident containment by isolating affected systems and networks.
- Collect incident data for post-incident reporting and lessons learned.
- Conduct incident debriefs with response teams and stakeholders to identify improvement areas in procedures and processes.
- Communicate incident details to key stakeholders, such as management, legal, and communications staff.
- Perform after-action reviews to pinpoint areas for improvement in response procedures and processes.
- Create & share lessons learned reports with response teams and stakeholders for procedure and process enhancement.
- Develop process improvement plans addressing weaknesses or non-compliance found in debriefs and lessons learned reports.
- Conduct security incident after-action reviews to identify improvement areas in response plans and procedures.



## BCDR Planning & Implementation Support

Outsourced services assist organizations in developing and maintaining business continuity and disaster recovery plans to ensure resilience in the face of security incidents or other disruptions.

## Key Benefits

- Define BCDR plan objectives, including recovery time objectives (RTO) and recovery point objectives (RPO).
- Identify critical business functions for maintenance during disasters or disruptions.
- Develop recovery strategies for critical functions and systems based on BIA findings.
- Integrate Service Provider BCDR Testing.
- Create recovery plans for critical functions and systems with detailed procedures and processes.
- Develop communication plans for employees, customers, and stakeholders during disasters or disruptions.
- Create training and testing plans to prepare employees and ensure recovery plan effectiveness.
- Implement the BCDR plan, including recovery, communication, and training/testing plans.
- Monitor and maintain the BCDR plan, updating recovery plans and testing procedures as needed.
- Regularly review and update the BCDR plan for continued effectiveness in disaster or disruption events.



## Incident Response Forensics

External teams provide incident response support, digital forensics, and investigation services to help organizations effectively respond to and recover from security incidents.

## Key Benefits

- Gather and preserve security incident evidence, such as logs, system images, and related data.
- Analyze incident data to determine cause, damage extent, and potential vulnerabilities.
- Create remediation plans addressing security vulnerabilities or weaknesses found during incident response and forensics.
- Offer continuous support for maintaining incident response and forensics processes, as well as assisting with updates and remediation plan implementation.



## Compliance Audits & Assessments

Perform periodic audits and assessments to verify compliance with internal policies, industry standards, and regulatory requirements (e.g., GDPR, HIPAA, CCPA, etc.).

## Key Benefits

- Establish compliance objectives that align with the organization's business goals, regulatory requirements, and industry best practices.
- Develop audit plans that outline the scope, methodology, and timeline for the compliance audits and assessments.
- Conduct compliance assessments to evaluate the organization's compliance with applicable laws, regulations, and industry standards.
- Review the organization's policies and procedures to ensure they are in compliance with applicable laws, regulations, and industry standards.
- Identify compliance gaps or deficiencies in the organization's policies, procedures, and controls.
- Develop remediation plans to address any areas of non-compliance or deficiencies identified through the compliance audits and assessments.
- Monitor compliance with applicable laws, regulations, and industry standards, and track progress in implementing remediation plans.
- Report compliance findings to senior management and the board of directors, including any areas of non-compliance, potential risks and threats, and remediation plans.
- Respond to audit findings and recommendations and develop corrective action plans to address any identified deficiencies or non-compliance.
- Regularly review and update the compliance program to reflect changes in technology, business operations, and regulatory requirements.
- Provide ongoing support to ensure the compliance program remains up-to-date and effective, and to assist with the implementation of remediation plans and corrective actions.





## Regulatory Monitoring

Stay informed about changes in data protection laws, regulations, and standards to ensure ongoing compliance and alignment with industry best practices.

## Key Benefits

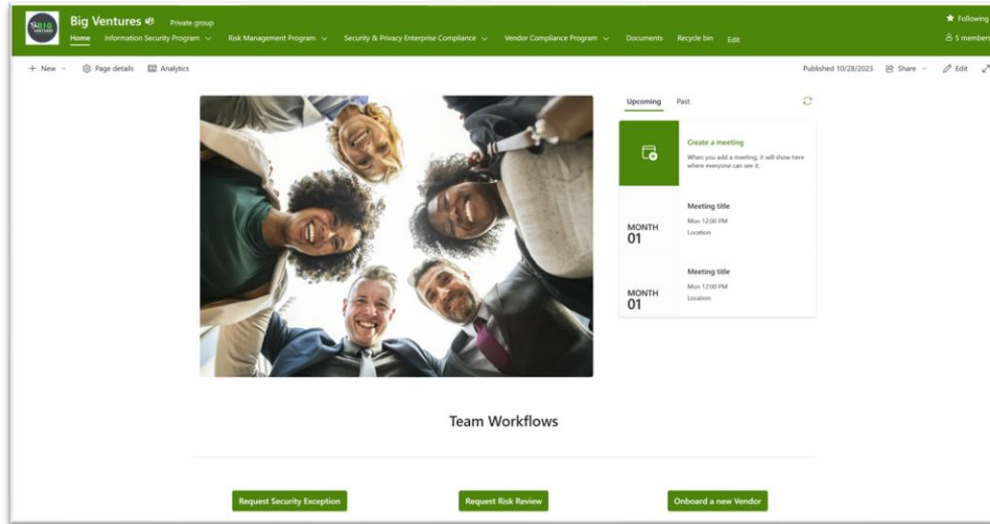
- Identify the regulations that apply to the organization based on its industry, location, and business operations.
- Monitor regulatory changes and updates to ensure the organization remains compliant with applicable regulations.
- Analyze the impact of regulatory changes on the organization's operations, policies, and procedures.
- Develop regulatory compliance plans to address any changes or updates to applicable regulations.
- Train employees on new or updated regulatory requirements, including changes to policies and procedures.
- Conduct compliance assessments to evaluate the organization's compliance with applicable regulations.
- Identify compliance gaps or deficiencies in the organization's policies, procedures, and controls.
- Develop remediation plans to address any areas of non-compliance or deficiencies identified through compliance assessments.
- Monitor compliance with applicable regulations, and track progress in implementing remediation plans.
- Report regulatory changes and updates to senior management and the board of directors and communicate any required changes to policies and procedures.
- Regularly review and update the regulatory monitoring program to reflect changes in technology, business operations, and regulatory requirements.
- Provide ongoing support to ensure the regulatory monitoring program remains up-to-date and effective, and to assist with the implementation of remediation plans and corrective actions.



# ISG-GRC Management Systems

---

This section includes the systems used by the ISG-GRC team to implement and operationalize your Managed Programs



## M365 GRC Platform Implementation

Instead of investing in a costly GRC system, consider our tailored solution that harnesses the power of Microsoft 365, SharePoint, Power Automate, Power Apps, PowerBI, and other M365 services. Our approach streamlines your organization's GRC processes, centralizes vital information, and enhances collaboration, all while offering a cost-effective alternative to traditional GRC systems.

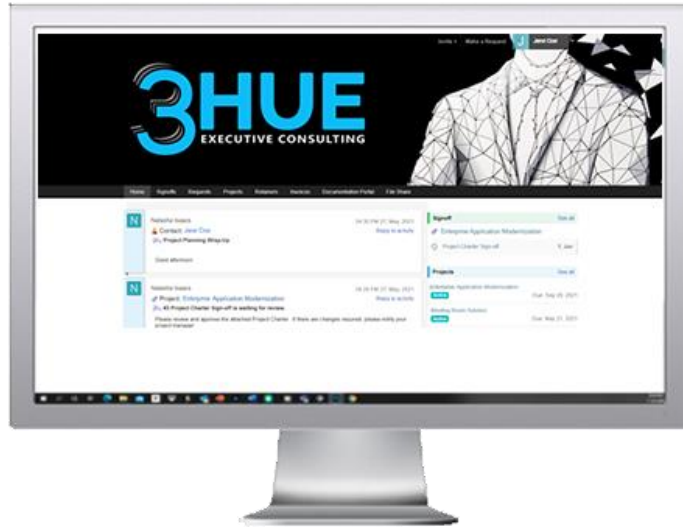
## Key Benefits

ISO SharePoint Intranet Site which includes:

- Program Information Page (e.g., ISP, RMP, VCP)
- Security Blogs for threat awareness and staff support
- Published Policies and Standards with automatic change notification for constant awareness
- Enterprise-wide security news, updates, and initiatives

MS SharePoint/Teams GRC Management System which includes:

- Risk Register
- Plan of Actions & Milestones
- IT Asset Manager
- Vendor Security DB
- Risk Assessment DB
- Business Process Inventory
- Policies & Procedures
- Attestation Assessments
- Security Exceptions
- Security Control Catalog
- Security Intelligence Dashboards



## IT Project Management Office (IT-PMO)

Discover the advantages of our IT Project Management Office (IT-PMO) service, providing a cohesive, structured strategy for managing projects throughout all 3HUE ISG services. With efficient processes, specialized guidance, and a focus on aligning with business goals, our IT-PMO service empowers organizations to successfully carry out IT projects. Optimize your resources, reduce risk, and boost project success rates with our tailored approach.

## Key Benefits

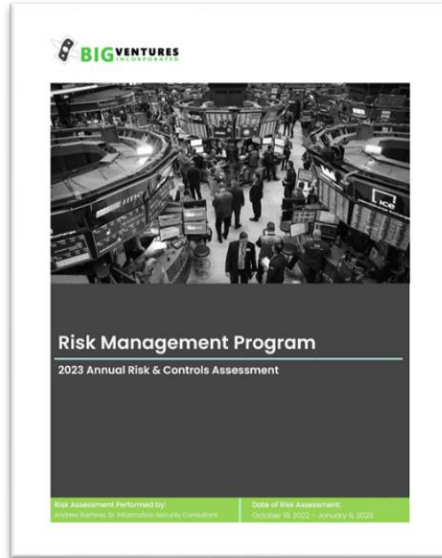
- Development and management of Project Charters
- Formalize and establish Project Teams
- Development and management of Project Plans
- Full project lifecycle management
- Project Budget Management
- Weekly project update meetings
- Security integration for security by design projects



## **ISG-GRC Key Artifacts**

---

This section includes key artifacts typically required by most information security programs and used by the 3HUE-ISG team for ongoing management of security risks



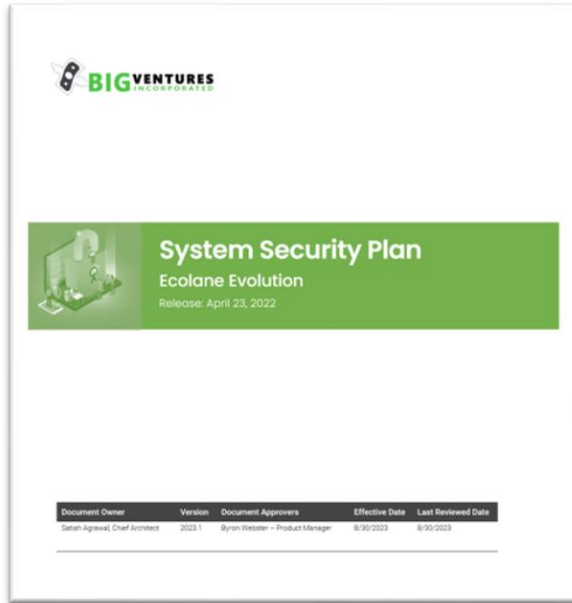
## Controls & Risk Posture Assessment (CCRPA)

The Controls & Risk Assessment (CRA) service offers a systematic approach to evaluating an organization's security controls and identifying potential risks. By aligning with industry best practices and regulatory requirements, this service enables organizations to strengthen their security posture and effectively manage risk in an increasingly complex threat environment.

(up to 1000 Assets)

## Key Benefits

- Assessment Scoping & Profiling
- Assessment Observations, Interviews, Demos and Document Reviews
- Review of Penetration Tests, Systems & Application Vulnerability Scans, Cloud Security Posture scans performed in the past 12-months
- External Analysis of the cybersecurity threat & compliance landscape, industry vertical trends for information security management, market opportunity analysis and more
- Control compliance gap review (baselined against ISG Scoped control set using Secure Control Framework (SCF) or an optimized NIST Cybersecurity Framework, or other control framework)
- Threat Modelling and Risk Analysis
- Risk and Controls Posture Reporting
- Recommended Strategic and Tactical risk Mitigation Initiatives
- Characterization of Key Systems
- Security Portfolio Review and Recommendations
- Updated risk register & plan of actions and milestones (POA&M)



## System Security & Privacy Plans (SSP)

The System Security & Privacy Plan service provides a concise, tailored solution for DoD contractors handling CUI, ensuring compliance with regulations like NIST 800-171. The service includes risk assessments, strategic planning, and continuous monitoring, empowering contractors to maintain robust security and privacy measures while staying aligned with evolving DoD requirements.

(up to 500 Controls)

## Key Benefits

- Information System level risk assessment
- Definition of Information Types processed by system
- Definition of all system related physical and logical assets
- Establish control baseline with the definition of a scoped control set required for compliant cybersecurity protection
- System specific Incident Response Guidelines
- System specific Contingency Planning Guidelines
- Development and Publication of a NIST compliant System Security Plan



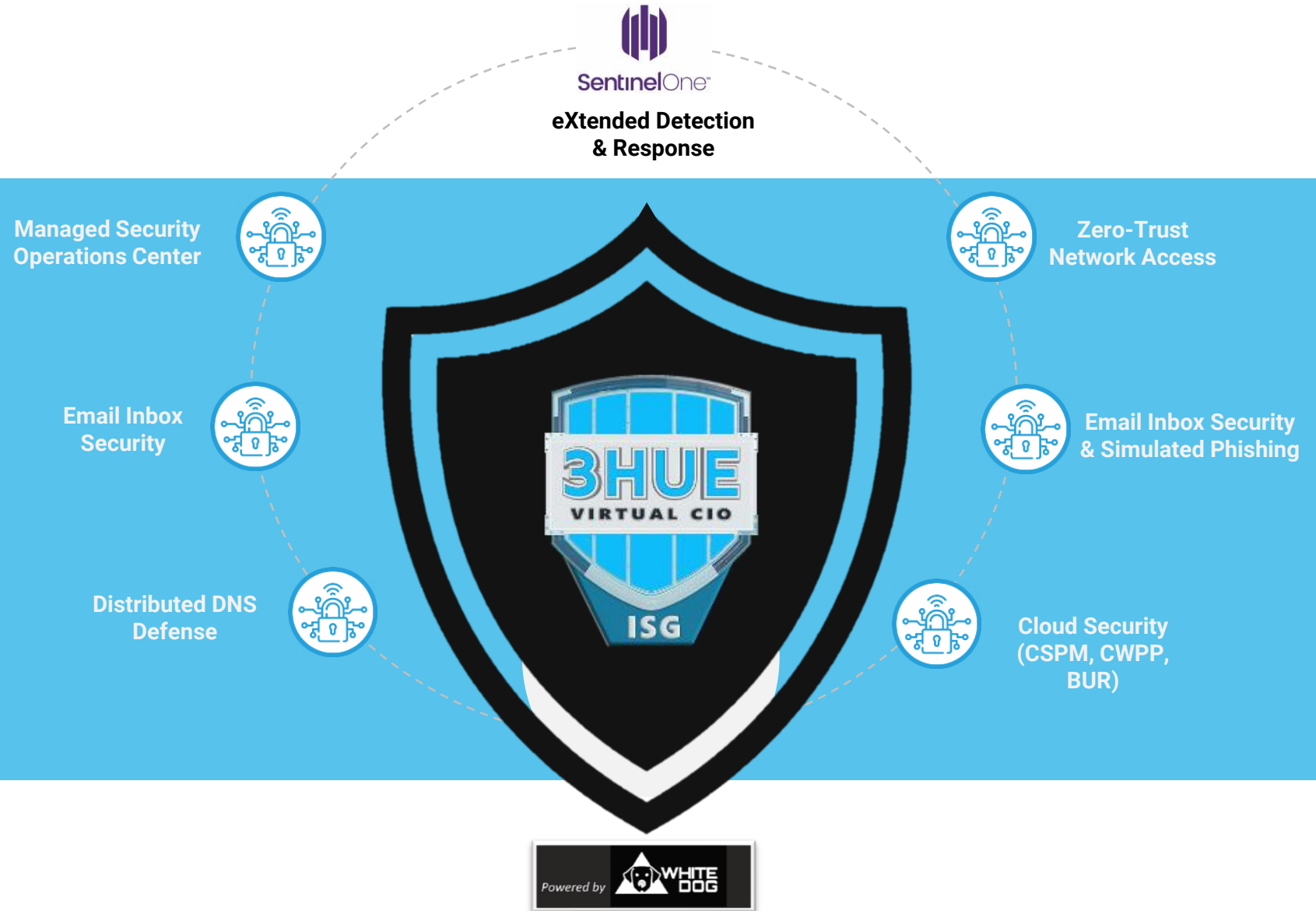
# ISG-OPS Managed Security Services

---

This sections explores the 3HUE ISG-OPS Managed SOC security services managed by the 3HUE-ISG team and powered by our partners WhiteDog.



# ISG Solutions | Protection against the modern adverstary





## Managed Security Operations Center (24x7x365)

Stay informed about changes in data protection laws, regulations, and standards to ensure ongoing compliance and alignment with industry best practices.

## Key Benefits

- Managed Detection & Response
- Active & Passive Asset Discovery (NTA)
- Continuous Incident Response
- User & Entity Behavioral Analysis (UEBA)
- Continuous Network Vulnerability Scanning
- Internal Security Controls Validation based on MITRE ATT&CK TTPS
- Dark Web Monitoring
- Attack Surface Vulnerability Monitoring (Purple Teaming)



## Endpoint Protection Security

Stay informed about changes in data protection laws, regulations, and standards to ensure ongoing compliance and alignment with industry best practices.

## Key Benefits

- Deep Visibility, Storylines, hunt ATT&CK technique
- Manual/Auto file fetch (Windows, MAC, Linux)
- Deep Visibility Mark benign finding as Threat enforcement response
- Secure Remote Shell (Windows PowerShell, Mac & Linux bash)
- Autonomous Threat Response
- Static Behavioral AI for file-based or fileless attack detection & prevention
- Incident Analysis (MITRE ATT&CK, timeline, explorer, team annotations)
- Quarantine/Isolate devices from the network
- OS & Third-party applications inventory & vulnerability (Win, Mac)

## COMPATABILITY

				
<b>Windows Desktop</b> Windows 7 SP1 Windows 10 Windows 11	<b>MacOS</b> Ventura Monterey Cataline Mojave High Sierra	<b>Windows Server</b> 2008 R2, SP1 2012 2016 2019 2022	<b>Linux Distributions</b> Ubuntu Redhat (RHEL) CentOS Oracle Amazon SUSE Fedora Debian Virtuozzo Scientific	<b>Cloud &amp; Virtual</b> Kubernetes Self-Managed AWS Kubernetes Azure Kubernetes Citrix XenApp Citrix ZenDesktop Oracle VirtualBox VMWare vSphere VMWare Workstation VMWare Fusion VMWare Horizon Microsoft Hyper-V



## Cloud Security

Stay informed about changes in data protection laws, regulations, and standards to ensure ongoing compliance and alignment with industry best practices.

## Key Benefits

- M365 File-level protection
- Google G-Suite file-level protection

### COMPATABILITY



#### Windows Desktop

Windows 7 SP1  
Windows 10  
Windows 11

#### Legacy Windows

Windows XP  
Windows Server 2003  
Windows Server 2008



#### MacOS

Ventura  
Monterey  
Cataline  
Mojave  
High Sierra



#### Windows Server

2008 R2, SP1  
2012  
2016  
2019  
2022



#### Linux Distributions

Ubuntu  
Redhat (RHEL)  
CentOS  
Oracle  
Amazon  
SUSE  
Fedora  
Debian  
Virtuozzo  
Scientific



#### Cloud & Virtual

Kubernetes Self-Managed  
AWS Kubernetes  
Azure Kubernetes  
Citrix XenApp  
Citrix ZenDesktop  
Oracle VirtualBox  
VMWare vSphere  
VMWare Workstation  
VMWare Fusion  
VMWare Horizon  
Microsoft Hyper-V



## Distributed DNS Defense

Stay informed about changes in data protection laws, regulations, and standards to ensure ongoing compliance and alignment with industry best practices.

## Key Benefits

### Essential Protection

- Block domains associated with Phishing, malware, botnets, etc.
- Create custom block/allow list
- Discover and Block shadow IT, with App Discovery report
- Enable web filtering

### Advanced Protection

- Block direct-to-IP traffic for C2 callbacks that bypass DNS
- Proxy web traffic for inspection



## Email Inbox Security

Stay informed about changes in data protection laws, regulations, and standards to ensure ongoing compliance and alignment with industry best practices.

## Key Benefits

- Real-time defense against business email compromise
- Protection against account takeover and insider risk
- Brand & Domain fraud protection
- Account Takeover Protection



## Security Awareness Training

Stay informed about changes in data protection laws, regulations, and standards to ensure ongoing compliance and alignment with industry best practices.

## Key Benefits

- Monthly end-user training
- Advanced Simulated Phishing
- Advanced Threat Simulation
- Phish Reporting Button for Outlook integration w/ gamification engine



# Customizing Virtual CIO Modules

---

Use the information in this section to understand how 3HUE bills for our services and manage our relationships



# ISG Solutions | How we structure our sales engagements

## Managed Program

- Best for continuous program management and outsourcing of information security functions
- Requires a signed Master Services Agreement
- 24- and 36-month term commitments
- Each module has a commitment of hours based on size and complexity of the Client organization
- Our Managed Programs are Billed Annually

## Retainer-Based

- Best for engagement with loosely defined deliverables
- Allows for quick start without establishing terms
- Minimum commitment of 100-hours
- Renewals sent when balance of hours falls below 20 hours.

## SOW-Based

- Best for precisely scoped engagements with clear success criteria
- Includes specific set of Terms & Conditions for 3HUE & Customer deliverables
- Uses a milestone payment model, requiring payment for a milestone when all success criteria is met.

# ISG Solutions | Service Components customized to your needs

**STEP 1:** Select your **ISG Leadership** Option

**ISG Services**  
**Virtual CISO Support**  
For organizations with an internal resource in the CISO role

**ISG Services**  
**Fractional CISO**  
For organizations requiring CISO staff augmentation

**STEP 2:** Select your **ISG GRC** Managed Services

**ISP** Information Security Program

**RMP** Risk Management Program

**VCP** Vendor Compliance Program

**SCS** Security Compliance Services

**CIRP** Cybersecurity Incident Response Program

**SEA** Secure Engineering & Architecture

**STEP 3:** Select your **ISG OPS** Managed Services

**MDR** Managed Detection & Response

**NDR** Network Detection & Response

**EDR** Endpoint Detection & Response

**EDRm** EDR for Mobile Devices

**IDM** Identity Management

**DSB** SaaS Backup

**D3** Distributed DNS Defense

**ZTNA** Zero-trust Network Access

**APP** Advanced Phishing Protection

**PROFESSIONAL SERVICES & PROCUREMENT**

# ISG Solutions | Service Components customized to your needs



\$15/user      \$38/user      \$43/user

Managed Detection & Response	Essentials	Premium	Complete
Managed Security Operations Center (24x7x365)	X	X	X
Endpoint Protection Security	X	X	X
Distributed DNS Defense – Foundations	X	X	X
Distributed DNS Defense – Advanced		X	X
Email Inbox Security		X	X
Cloud Security		X	X
Security Awareness Training			X

Virtual CIO-ISG Services		STD Rate
<b>VCISO</b>	Virtual CISO	\$ 315/hr.
<b>ISP</b>	Information Security Program	\$ 285/hr.
<b>RMP</b>	Risk Management Program	\$ 285/hr.
<b>VCP</b>	Vendor Compliance Program	\$ 285/hr.
<b>SPECS</b>	Security & Privacy Enterprise Compliance	\$ 265/hr.
<b>CIRP</b>	Cyber-Incident Response Planning	\$ 315/hr.
<b>IT-PMO</b>	IT Project Management Office	\$ 250/hr.