sourcing. the smarter way.®

A Systems Plus Group Company

HYBRID SOC

UPDATED FEBRUARY 2021

MANAGING A SECURITY PROGRAM – A CIO PERSPECTIVE

A confusing environment of regulation, frameworks, security tools and services has created a situation where companies often don't know what direction to take

The security industry tells you….

1. "Buy our tools"
2. "Hire our services"

"And everything will be OK"

What they don't tell you: Execution is more important - An effective security program involves more than tools.

- **Watching the pane of glass is the easy part** – effective incident, or observation, response takes time and effort
- **An effective security foundation starts with solid processes and a few tools:** (a) Endpoint management, (b) a network log and event management SEIM tool, and (c) threat intelligence service
- **It's possible to spend a lot of money on things that you don't need or can't prove the value of.** But you don't have to. Multiple tools often lead to overlapping capabilities. Instead, first master the basics with process and basic tools
- **End Points and Agent Management is important**. Keeping all device agents configured and reporting correctly is a lot of work, if you have a distributed environment
- **Vulnerability management is an on-going effort**. Vulnerability scanning, patch management, and remediation is a lot of work
- **Access and Identity Management involves many tasks**. Account provisioning and deprovisioning, rights management, and privileged account control need constant attention
- **Change is the only constant**. Configuration tuning, and strengthening the security processes in response to other changes in technology is an ongoing process

A "HYBRID SOC" IS AN EFFECTIVE AND AFFORDABLE WAY FOR MANY COMPANIES TO ADDRESS AND MATURE THEIR SECURITY NEEDS

A "Hybrid SOC" is a cross-skilled, and multi-function security Virtual Captive team. A Hybrid SOC is capable of handling all security operations tasks a company needs in today's modern "defend from within" security approaches

Program Domain

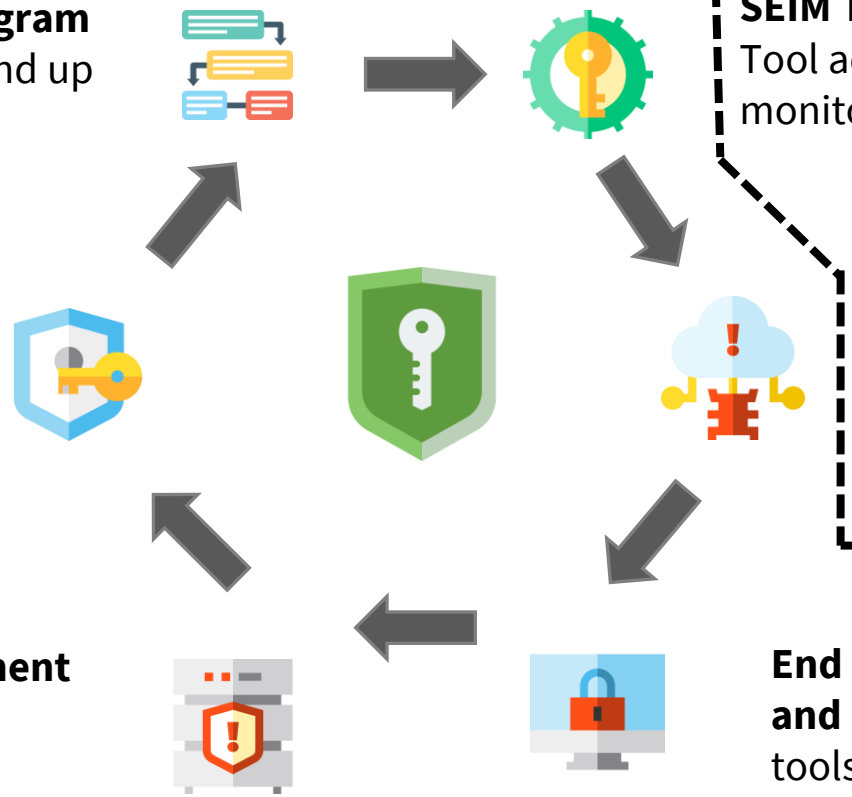
Risk Management Program keeps things healthy, and up to date

Identity Domain

User provisioning and identity management handles the details of access control and management (SOX requirement)

Patching/ Infra Domain

Vulnerability management and patching. Conduct scans, monitor status of vulnerabilities, and patch devices as needed. Also Firewall Mgmt



SEIM Tool management - Tool administration, tuning, monitoring, management

Network Domain

Incident evaluation and response – identify and respond to threats and alerts with detailed level 2 and 3 research and analysis

End Point management and health keep security tools on-line, agents reporting, and devices updated

Device Domain

A WAY TO THINK ABOUT HYBRID SOC

A *Hybrid SOC team* is a Virtual Captive team with both security and infrastructure skills that can administer security tools, and operate ALL security processes

Our security philosophy is *"Execute the basics really well."*

= Identity Mgmt components highlighted

① Define key policies

- Information security and risk management policy
- Anti virus/ anti malware
- Acceptable use
- Information classification
- Email policy
- Network security policy
- Access control and passwords
- Device management
- Event response
- Change management
- IT Exception policy
- Disaster recovery and Business continuity

② Buy Good Tools, but use then well (no need for Best in Class)

- End point protection
- Privileged account and password mgmt
- Next gen firewall
- IPS/ IDS
- SEIM event mgmt/ log correlation

③ Use targeted services for independent verification

- 3rd party vulnerability scanning
- 3rd party penetration testing
- Ethical Phishing
- PCI QSA (if applicable)

④ Use a Virtual Captive Team to perform Hybrid SOC processes

- Patching & Vulnerability remediation
- User provisioning and access control management
- Monitoring and SEIM management
- Incident investigation & response
- Firewall, IPS, IDS management
- Security tool agent deployment and health
- Program reporting and metrics

POSSIBLE TEAM STRUCTURE

Network Domain

SEIM Tool skills +
Incident evaluation and response - Can be 24 x 7 depending upon client needs

SOC Lead
Mid Tool Admin
Mid + Junior Incident evaluation and response

Device Domain

End Point management team - Can be separate end point support team, but with dotted line to security team for anti-virus/ anti-malware response and agent management

Infra Domain

Infrastructure Team – Handles infrastructure vulnerability scanning, server patching, firewall rules management and patching, incident response

Identity Domain

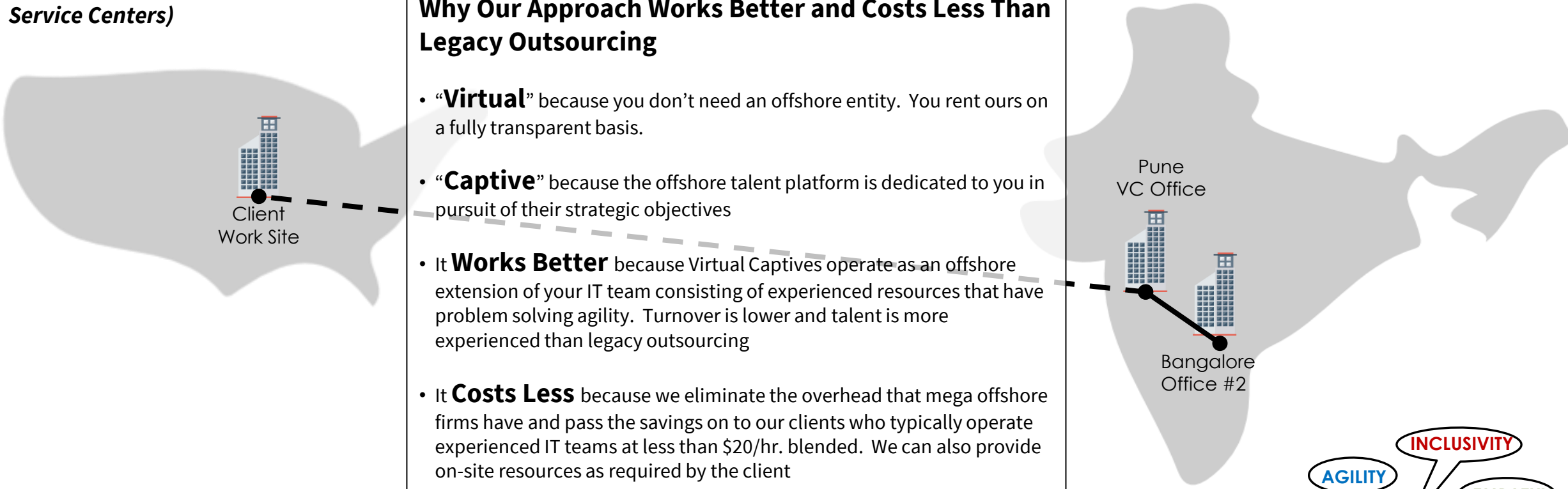
User provisioning and identity management handles the details of access control, identity management and compliance (SOX requirement)

Program Domain

Risk Management Program – Likely internal client team with responsibility for Hybrid SOC team

A VIRTUAL CAPTIVE FUNCTIONS AS AN EXTENSION OF YOUR ORGANIZATION AND MAKES OUTSOURCING WORK BETTER, AND COST LESS

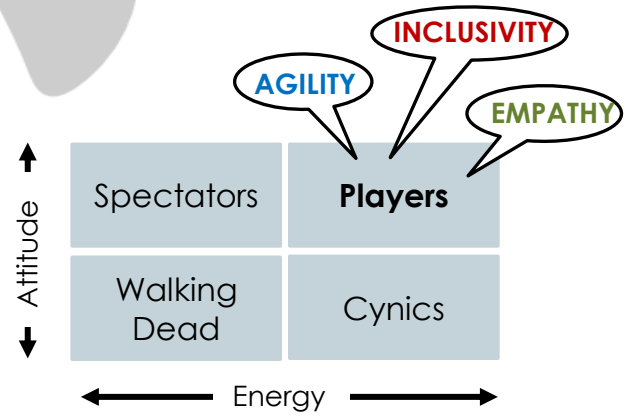
The approach and benefits are the same as with captive GSCs (Global Service Centers)



Why Our Approach Works Better and Costs Less Than Legacy Outsourcing

- "**Virtual**" because you don't need an offshore entity. You rent ours on a fully transparent basis.
- "**Captive**" because the offshore talent platform is dedicated to you in pursuit of their strategic objectives
- It **Works Better** because Virtual Captives operate as an offshore extension of your IT team consisting of experienced resources that have problem solving agility. Turnover is lower and talent is more experienced than legacy outsourcing
- It **Costs Less** because we eliminate the overhead that mega offshore firms have and pass the savings on to our clients who typically operate experienced IT teams at less than $20/hr. blended. We can also provide on-site resources as required by the client
- It's **Easy to Operate** because our experience and "Design to Operate" methodology guide you every step of the way.

Our Approach is a "People First" remote talent management strategy



WE RECOMMEND LAYERING THE RIGHT TALENT WITH THE RIGHT TASKS AT THE RIGHT COSTS

Most Expensive

Layer 3 - Flex

(Think "Contractor")

FOR: Temporary resources used for specialty project work, extra capacity, or only as needed tasks linked to business cases

DO: Limit use of "Flex" resources to focused, targeted tasks. Get them in, then get them out when done

Layer 2 - Internal

(Think "Leader/Driver")

FOR: Owner, driver, architect, business relationship, and IT leadership roles

DO: Put only as many roles as needed to engage the business, and lead the Layer 1 execution teams

Least Expensive

Layer 1 - Baseline

(Think "Virtual Captive")

FOR: Ongoing baseline support tasks, app dev, QA, infrastructure COE teams, Data Analytics, ERP Support

DO: Put as many FTE roles, and as much tasking, and workload as possible into this bucket

EXAMPLE CONFIGURATION FOR AN ACTUAL CLIENT

Layer 3 - Flex

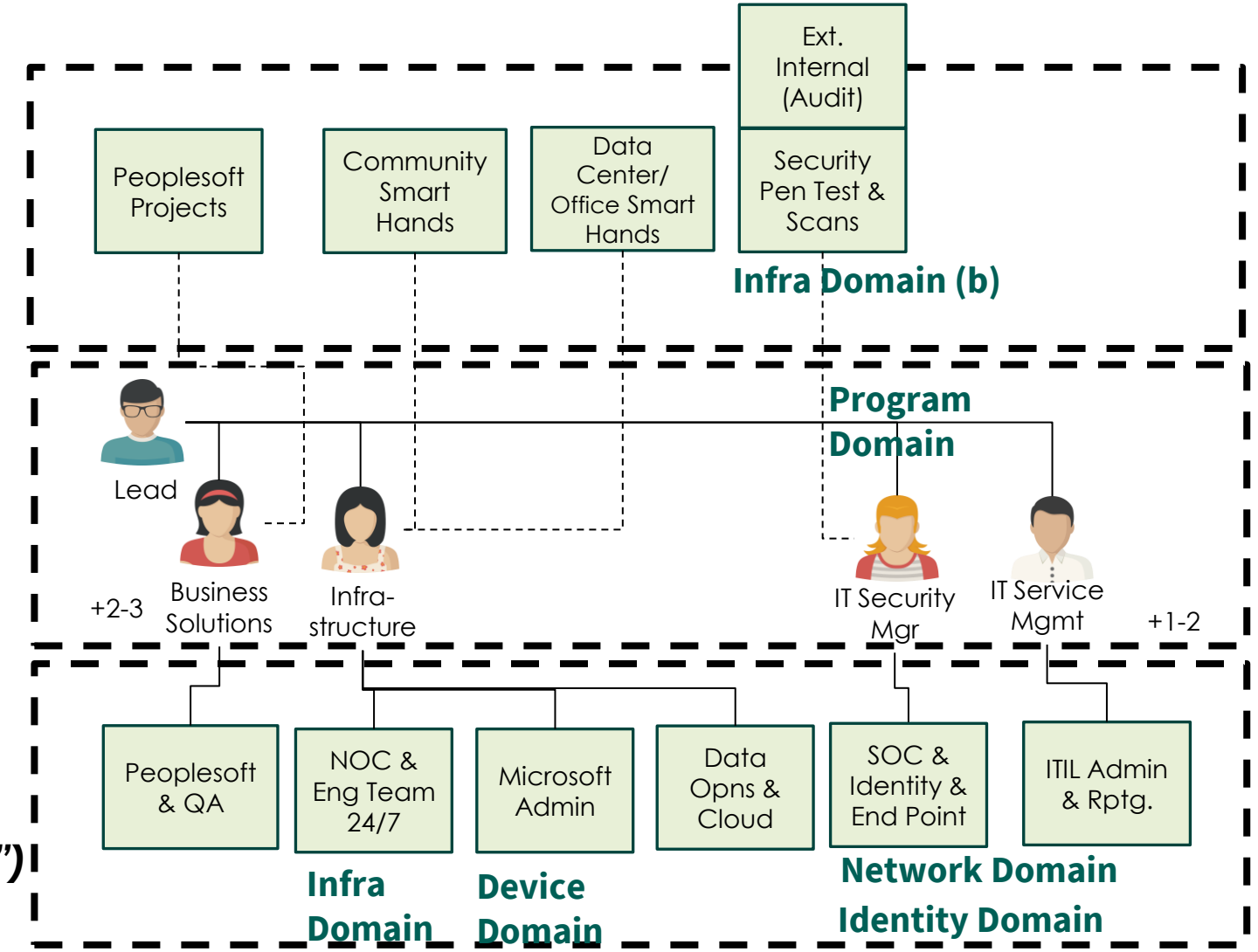
(Think "Contractor")

Layer 2 - Internal

(Think "Leader/Driver")

Layer 1 - Baseline

(Think "Virtual Captive")



*This configuration is **50-60% cheaper** than the cost of an internal-heavy configuration*

BUSINESS CASE ILLUSTRATION OF HOW A VIRTUAL CAPTIVE TEAM CAN BE DESIGNED TO DELIVER AN AGILE, HIGH VALUE SOC AT THE LOWEST TOTAL COST OF OWNERSHIP

1. The Requirement

Company requires a security operations team (SOC) to monitor and manage incident response 24x7, run vulnerability management program, patching, user provisioning, and tool administration

2. The Options

The company has several options for how to build teams to handle the workload:

(A) Staff an entirely internal team,
(B) Use a combination of specialty vendors, including some legacy off-shore service providers
(C) Use a Virtual Captive as an off-shore extension of the internal team

Conclusions

1. Internal teams and the Virtual Captive are by far the most agile, and flexible solutions, but come at different costs.
2. Option B will always be most expensive, rigid, and require the most oversight
3. Option C delivers the best results, most agility, and the least cost

3. The Solutions Compared

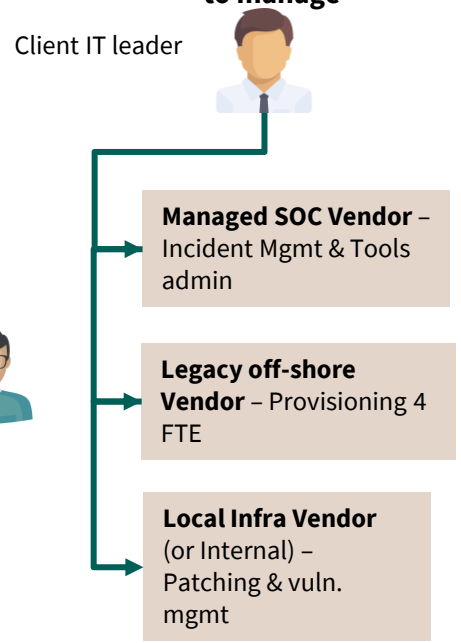
Option A – Internal Teams - Good, but expensive

Team makeup – 2 PT Leads plus
9 FTE – 24x7 monitoring, response, tool administration
2 FTE – Windows engineers for patching and device admin
2 FTE – user provisioning including off-hour support

Assume that internal teams are more productive and can get by with fewer resources, but still require 9 to cover 24x7.

Total cost (excluding Client IT Leader but including benefits) is **$1.2M-$1.5M/yr.**

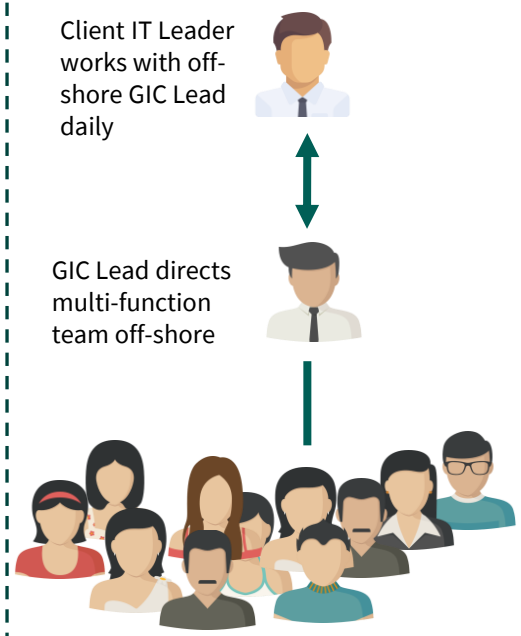
Option B – Mixture of Vendors is the most expensive and hardest to manage



Assume that SOC vendor handles L1-L2 incidents. Some internal help required (not incl.)

Total cost (excluding Client IT Leader) is **$1.4M-$1.8M/yr.**

Option C – Virtual Captive – Best results, lowest cost



Team makeup – 1 Lead plus
9 FTE – 24x7 monitoring, incident response, tool administration
3 FTE – Windows engineers for patching and device admin
3 FTE – user provisioning including off-hour support

Total cost (excluding Client IT Leader) is **$400-500K/yr.**

A HYBRID SOC CAN DO MORE FOR YOU

	Hybrid SOC	Managed SOC Service
Cost	$	$$$$
Rigid Vendor Processes		✓
Adaptable to changing environment	✓	
Retained knowledge and intellectual property	✓	
Incident management	✓	✓
Security tool configuration and management	✓	✓
Security agent health management	✓	
Vulnerability management	✓	
Device patching	✓	
User provisioning	✓	
Privileged account management	✓	
Continuous improvement	✓	

EXAMPLE OF TEAM STRUCTURES – HERE, WE COMPARE A SMALL CORE SOC TEAM AND IDENTITY MANGEMENT

Security Operations

Outsource Model

Resource	Years of Experience	# of Resources	Base Salary $/Hr	Recurring Overhead $/Hr	Management Overhead $/Hr	Total $/Hr Rate	Total $/Year
SOC Lead	7-10 yrs	1	$ -	$ -	$ -	$ 32.00	$ 66,560
SOC Sr. Engineer	7-8 yrs	1	$ -	$ -	$ -	$ 29.00	$ 60,320
SOC L2 Analyst	5-7 yrs	2	$ -	$ -	$ -	$ 25.00	$ 104,000
SOC L1 Analyst	3-5 yrs	5	$ -	$ -	$ -	$ 21.00	$ 218,400
			Grand Total				$ 449,280

BLENDED RATE $ 24.00

9 FTE VC SOC

Resource	Years of Experience	# of Resources	Base Salary $/Hr	Recurring Overhead $/Hr	Management Overhead $/Hr	Total $/Hr Rate	Total $/Year	One Time Setup Cost
SOC Lead	7-10 yrs	1	$ 14.35	$ 2.88	$ 4.31	$ 21.54	$ 44,798	
SOC Sr. Engineer	7-8 yrs	1	$ 12.15	$ 2.88	$ 3.76	$ 18.79	$ 39,078	$ 29,745
SOC L2 Analyst	5-7 yrs	2	$ 9.25	$ 2.88	$ 3.03	$ 15.16	$ 63,076	
SOC L1 Analyst	3-5 yrs	5	$ 7.00	$ 2.88	$ 2.47	$ 12.35	$ 128,440	
			Grand Total				$ 275,392	

BLENDED RATE $ 14.71

Savings (Blended $/Hr)	$ 9.29	39%
Savings (Total $/yr)	$ 173,888	39%
Savings (Total $/yr - 1 time setup)	$ 144,143	32%

- Small teams – probably the minimum for these functions
- Multi skilled resources capable of handling tool administration, agent deployment
- Identity management team handles all account administration and privileged account management
- To this team, we can add patch management, and network support

EXAMPLE OF TEAM STRUCTURES – HERE, WE COMPARE A SMALL CORE SOC TEAM AND IDENTITY MANGEMENT

Provisioning Team

Outsource Model

Resource	Years of Experience	# of Resources	Base Salary $/Hr	Recurring Overhead $/Hr	Management Overhead $/Hr	Total $/Hr Rate	Total $/Year
Provisioning Lead	7-10 yrs	1	$ -	$ -	$ -	$ 32.00	$ 66,560
SOC Sr. Engineer	7-8 yrs	1	$ -	$ -	$ -	$ 29.00	$ 60,320
L2 Engineer	5-7 yrs	3	$ -	$ -	$ -	$ 25.00	$ 156,000
L1 Engineer	3-5 yrs	4	$ -	$ -	$ -	$ 21.00	$ 174,720
			Grand Total				$ 457,600

BLENDED RATE $ 24.44

8 FTE Virtual Captive

Resource	Years of Experience	# of Resources	Base Salary $/Hr	Recurring Overhead $/Hr	Management Overhead $/Hr	Total $/Hr Rate	Total $/Year	One Time Setup Cost
Provisioning Lead	7-10 yrs	1	$ 13.25	$ 2.88	$ 4.03	$ 20.16	$ 41,938	
SOC Sr. Engineer	7-8 yrs	1	$ 11.21	$ 2.88	$ 3.52	$ 17.61	$ 36,634	$ 29,745
L2 Engineer	5-7 yrs	3	$ 8.75	$ 2.88	$ 2.91	$ 14.54	$ 90,714	
L1 Engineer	3-5 yrs	4	$ 7.25	$ 2.88	$ 2.53	$ 12.66	$ 105,352	
			Grand Total				$ 274,638	

BLENDED RATE $ 14.67

Savings (Blended $/Hr)	$ 9.77	40%
Savings (Total $/yr)	$ 182,962	40%
Savings (Total $/yr - 1 time setup)	$ 153,217	33%

- Combining the two teams you get an 18 person team handling all aspects of security operations
- Identity team is staffed to handle 18x7, but would be scaled to meet SLA requirements
- Using basic tools, can result in an entire IT security program costing between $600K-$800K

Thank You

Contact us at info@Versitae.com, or 817-662-7004 to learn how a Versitae ***Virtual Captive*** can add value to your business