



UnderDefense

Security Monitoring



39

Security
engineers



28

Publications



19

Certified
experts



4

Products
launched for
our clients

Enhancing
your
capabilities

Leaders Matrix

Top Cybersecurity Consulting Companies

15 Leaders

Reviews

Leaders Matrix



Clutch Leaders Matrix

Rollover to see company insights or click a company below for more details.

- 1 ScaleFocus
- 2 Fluid Attacks
- 3 UnderDefense
- 4 FRSecure
- 5 Silent Break Security
- 6 Switchfast Technologies
- 7 Fidelis Cybersecurity
- 8 Dhound
- 9 TechMD
- 10 Berezha Security
- 11 A1QA
- 12 The Vietnam Security Network
- 13 UkrinSoft
- 14 TestArmy
- 15 Bit by Bit Computer Consultant

Recognitions, Awards & Partnerships



splunk> partner+

UnderDefense is [Splunk partner](#) and our team is holding the following Splunk certifications:

- Splunk Certified Consultant I
- Splunk Administrator
- Splunk Power User
- Splunk Sales engineer 1
- Splunk User
- Splunk Sales Rep 1
- Splunk Sales Rep 2
- Splunk Sales IT & App
- Splunk UBA User

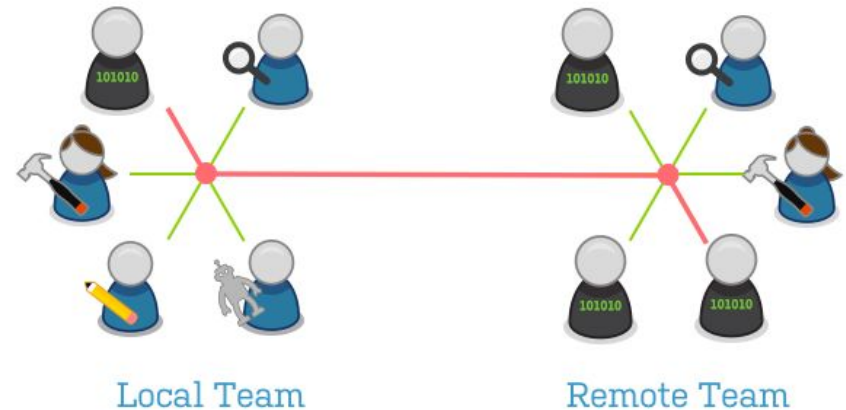


Security Monitoring Advantages

- You spend less, but get more with Cloud deployed co-managed Splunk SIEM
- Your costs are predictable with fixed scale of payment
- The hours of on non-operational running cost much more than the quote for security monitoring for half a year
- The SOC team consists of certified experts in SecOps and SIEM tools
- Visibility and measurability of security is enabled
- You define the time and scope of SOC: 8x5, 12x5 or 24x7 security monitoring
- Legal protected Service Layer Agreement
- Tier 1 through 3 Analysts
- Monitoring team scalability
- Incident Response is in real time with the least consequences
- IT Forensics

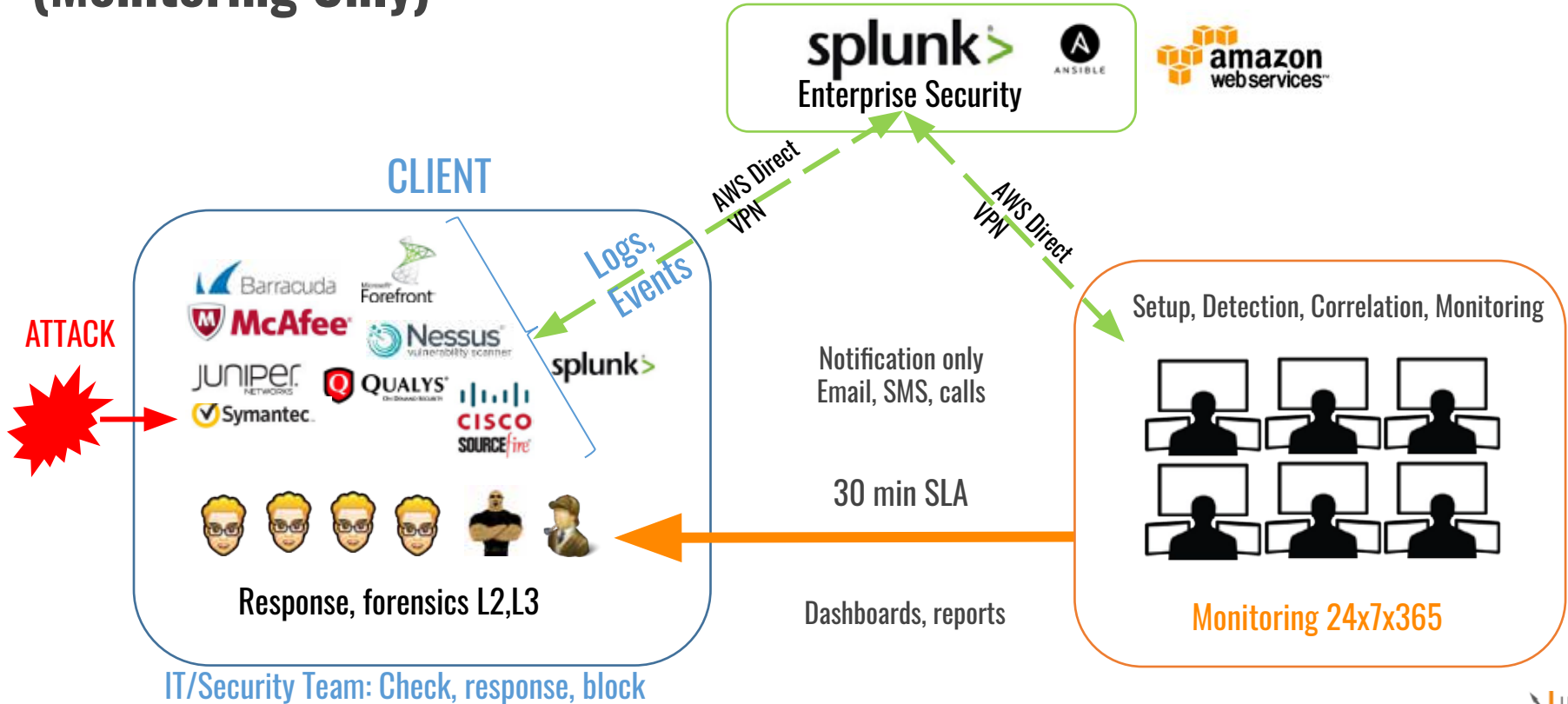
Security Monitoring for existing IT Security Team

- Our Managed Security Services & SOC are designed to serve as a remote extension of your security staff
- Our cost and location model are optimized to reduce costs, increase efficiency, provide 24x7x365 coverage from multiple locations
- Our team serves supplements your staff allowing you to focus on core business needs. Allow your Security and IT to do more value added services like:
 - Red Teaming / Offensive Security
 - Education
 - Trainings
 - Certifications
 - Forensics
 - Completing compliance



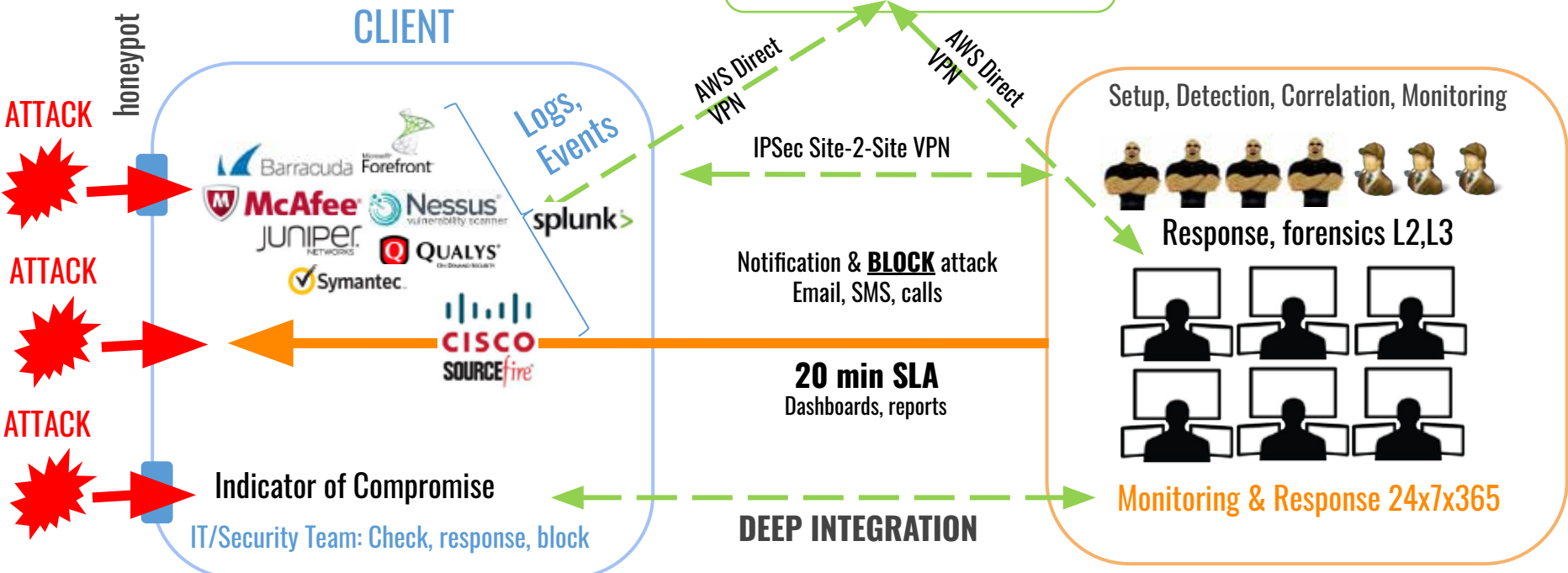
Co-managed security monitoring for SMB

(Monitoring Only)



Co-managed security monitoring for SMB

(Monitoring & Management)



What is included?

Incident Management and reporting



- Security logs monitoring methodology
- Real-time incident handling
- Trend analysis

Development and adaptation



- Changes to log sources and formats
- Changes in search criteria
- Create reports and dashboards
- Create and change alarm structures

Operations



- NOC/SOC-delivery
- Service monitoring
- SLA
- SIEM management

Compliance reporting

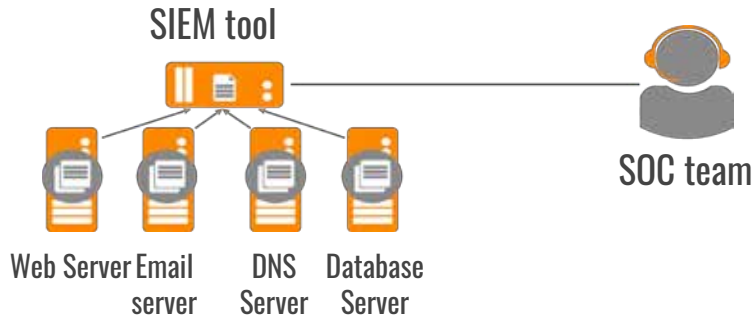


- Compliances reports
- Deviation reports

How this works:

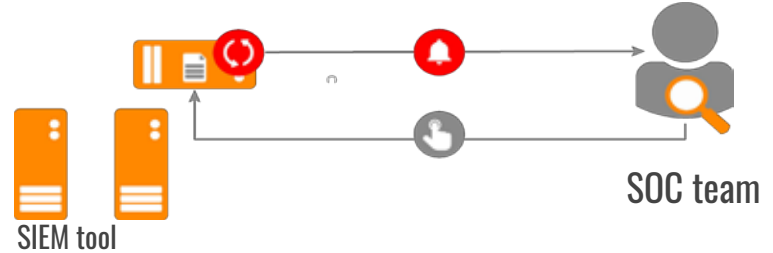
Stage 1 - Configuration phase

The SIEM is installed and logs are collected from log sources



Stage 2 - Monitoring phase

They are analysed using SIEM alert system due to their urgency



Stage 3 - Incident Response

Security Analysts consult the customer IR plan and send the Incident Report



PREPARE

Improve Organizational Readiness

- Invite team members
- Fine-tune response policies and procedures
- Run simulations (firedrills / table tops)



REPORT

Document Results & Improve Performance

- Generate reports for management, auditors, and authorities
- Document results
- Conduct post-mortem
- Update policies and procedures
- Track evidence
- Evaluate historical performance



ASSESS

Identify and Evaluate Incidents

- Engage appropriate team members
- Evaluate precursors and indicators
- Track incidents, maintain logbook
- Automatically prioritize activities based on criticality
- Log evidence
- Generate assessment summaries

MANAGE

Contain, Eradicate, and Recover

- Generate real-time IR plan
- Coordinate team response
- Choose appropriate containment strategy
- Isolate and remediate cause
- Instruct evidence gathering and handling



Thank you for your trust

V2 Version 2 | 二版
www.version-2.com
Hong Kong | Taiwan | Singapore | Macau | Mainland China

Hong Kong & Macau
Tel: (852) 2893 8860
Email: sales@version-2.com.hk

Taiwan
Tel: (886) 02 7722 6899
Email: sales@version-2.com.tw

Singapore, Malaysia & SEA
Tel: (65) 6296 4268
Email: sales@version-2.com.sg