



Managed Security Solutions Portfolio

Overview

Q4 2021

About Us



Partnerships:

Vertek distributes its Managed Threat Detection & Response services into the market through a national network of MSPs, VARs, Solution Providers, Master Agents, supporting customers with 50 - 2,000 employees (on average), that operate within, or provide goods and services to heavily regulated industries.

Est in 1988

- 110 Employees
- HQ in Colchester, VT, Offices in New Providence, NJ

3 Business Units:

- Telecom Operations
- Custom Software Development
- **Managed Cybersecurity**

Managed Security Services

- Small & Medium Business: *Managed Detection and Response*
- Mid Market & Enterprise: *Managed Threat Intelligence*
- Security Operations: *Team of Industry Experts*
- AT&T Cybersecurity Platinum MSSP Partner: *Master MSSP, Product Advisory Board*

Committed to Customer Success

- Highest Industry Client Retention Rate
- Ongoing Research, Development, Innovation
- Facility Clearance, NIST 800-171, CMMC L3 (In progress)

Capabilities & Industries

Industries Served:

- Financial Services
- Healthcare
- Automotive
- IT Solution Provider
- Retail
- Manufacturing
- Utility
- Public Sector
- Business Services
- Construction
- Legal
- Telecom
- Transportation

Certifications

- *CISSP, CEH, CPT, CIH, CYSA+ Security+, Network+, AlienVault, AWS, Cisco, VMware, Microsoft, ITIL, PMP, and Java*

Competencies

- *Managed Detection and Response, Security Information Event Management, Threat Hunting, Malware Analysis, Threat Research, Forensics, Security Operation Process Design, Custom Coding & DevSecOps, Reporting and Analytics, Compliance*

Compliance

- *NIST CSF/800-171, CMMC, ISO 27002/1, FFIEC/GLBA, SEC/OCIE, 23 NYCRR PART 500, SANS CIS, PCI, HIPAA, and SOC2*

Custom threat intel

- *Vertek labs team manages and maintains private threat pulses of Phishing, FS-ISAC, ES-ISAC, NCCIC and US-CERT threat indicators. These custom indicators are pushed real-time to your appliance.*

Managed Security Services (MSS) Portfolio



MDR - Managed Detection & Response

MTI - Managed Threat Intelligence

MDR + MTI Custom

Solutions designed around AT&T Cybersecurity Unified Security Management (USM) Anywhere Platform

Managed Detection & Response



What's included:

Security Tools:

AT&T's Unified Security Management Anywhere (USM-A) Product
Vertek Client Portal, Ticketing Platform and SOC Tools (e.g.,
forensics, malware, reconnaissance, analytics, etc.)

Security Operations:

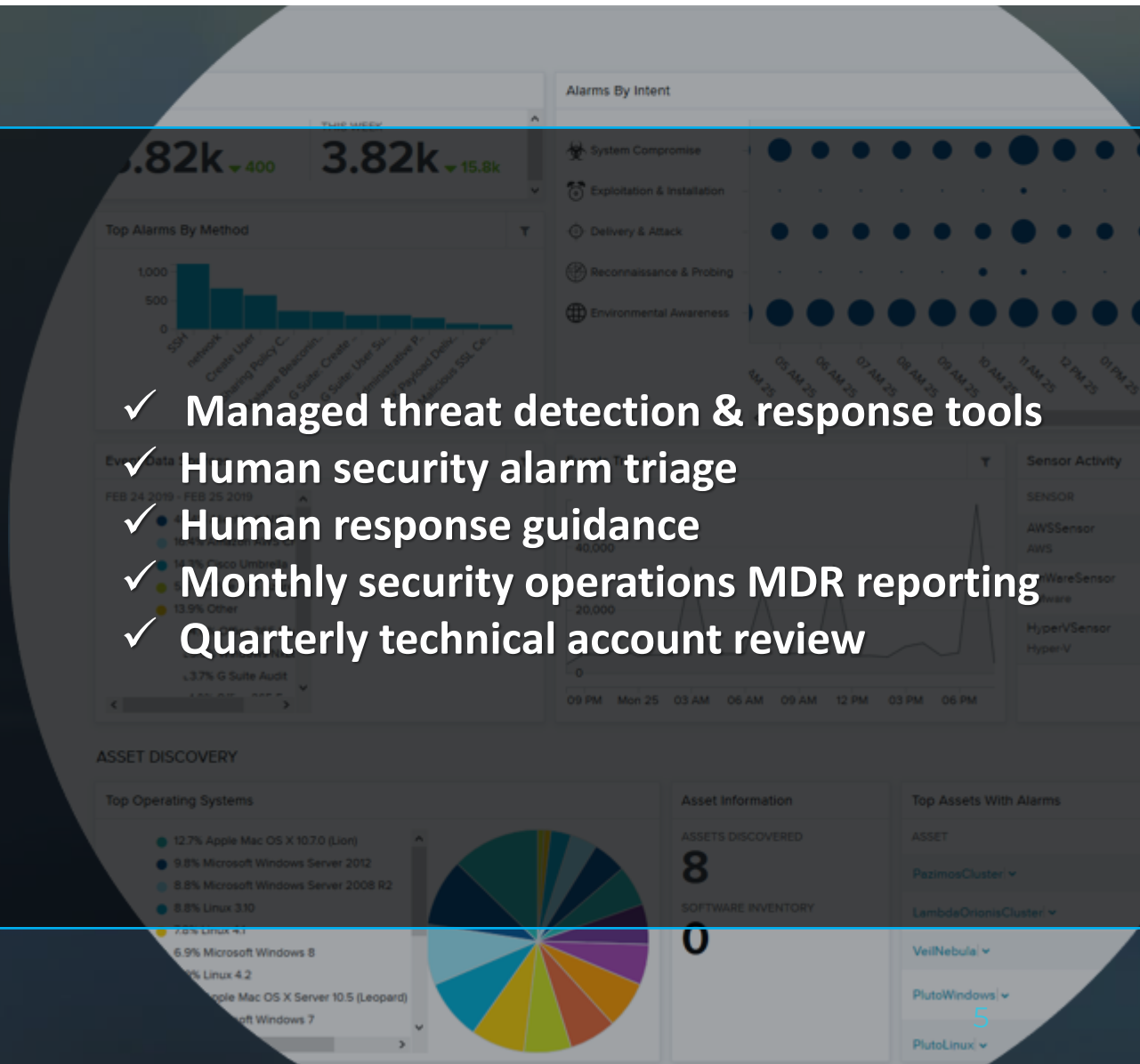
Vertek 24/7 Security Operations Center

Service Analytics:

Vertek Monthly MDR Reporting

Account Management:

Vertek Quarterly account review

- 
- ✓ Managed threat detection & response tools
 - ✓ Human security alarm triage
 - ✓ Human response guidance
 - ✓ Monthly security operations MDR reporting
 - ✓ Quarterly technical account review

Security Tools: Simplifying the Security Stack

As Required By Regulators = *Providing a Layered Approach to Cybersecurity* *Included in Vertek MDR

Vertek MDR Asset discovery
Know who and what is connected to your environment



Vertek MDR Vulnerability assessment
Know where the vulnerabilities are on your assets to avoid compromise



Vertek MDR Intrusion detection
Know when suspicious activities happen in your environment



Vertek MDR Endpoint detection & response
Continuously monitor your endpoints in the cloud and on premises to detect threats and changes to critical files.



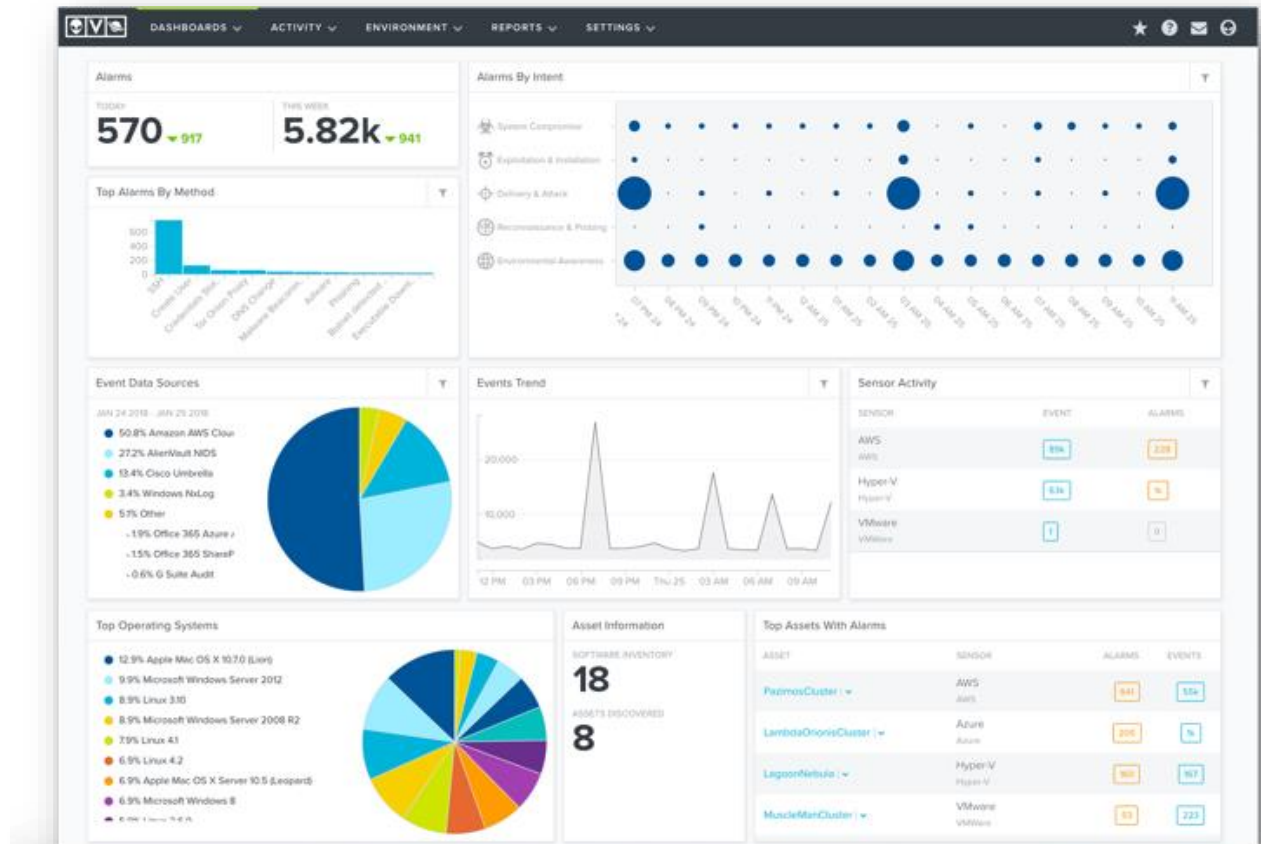
Vertek MDR Behavioral monitoring
Identify suspicious behavior and potentially compromised systems



Vertek MDR SIEM & log management
Correlate and analyze security event data from across your network and respond



Vertek MTI Security & compliance reporting
Pre-built, customizable reports for regulation standards and compliance frameworks

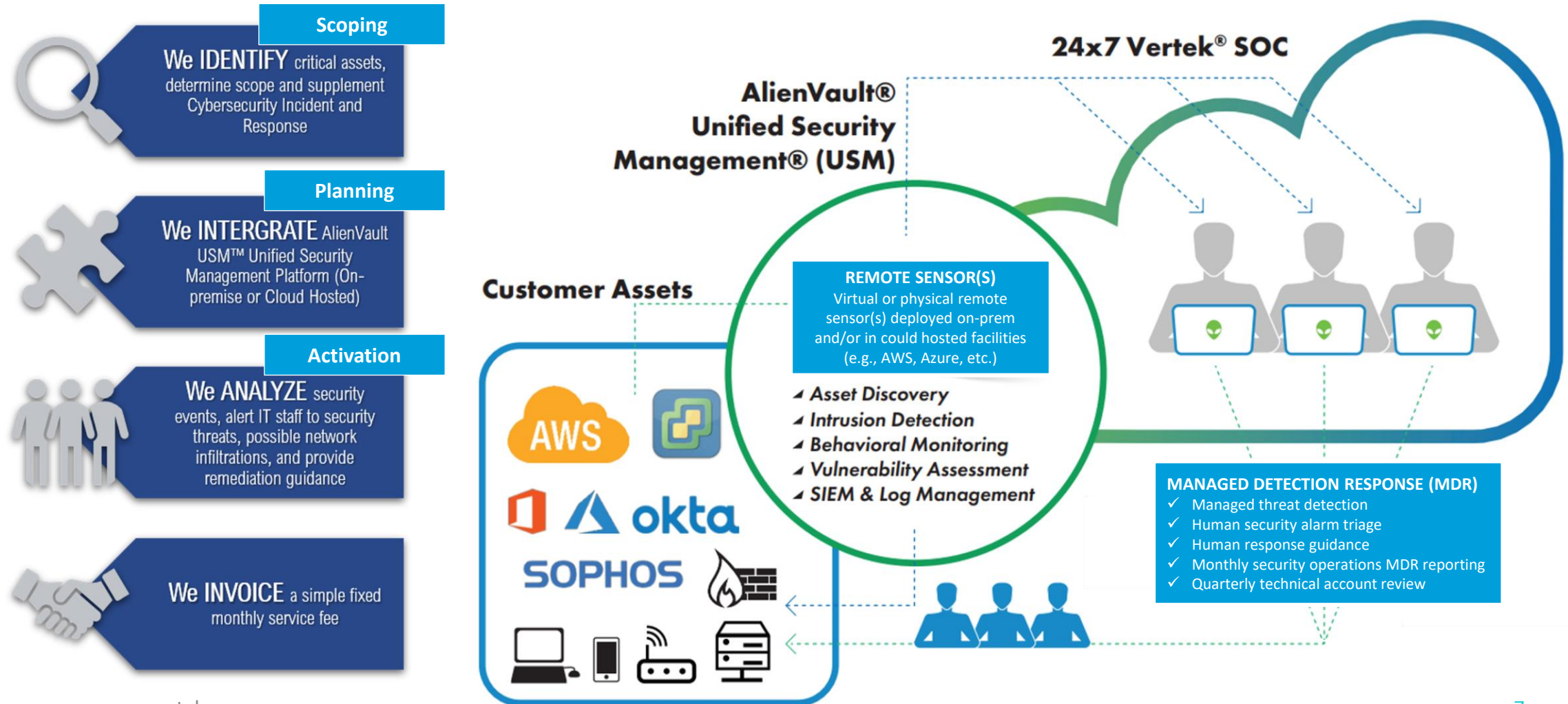


A unified security platform for threat detection, incident response & compliance

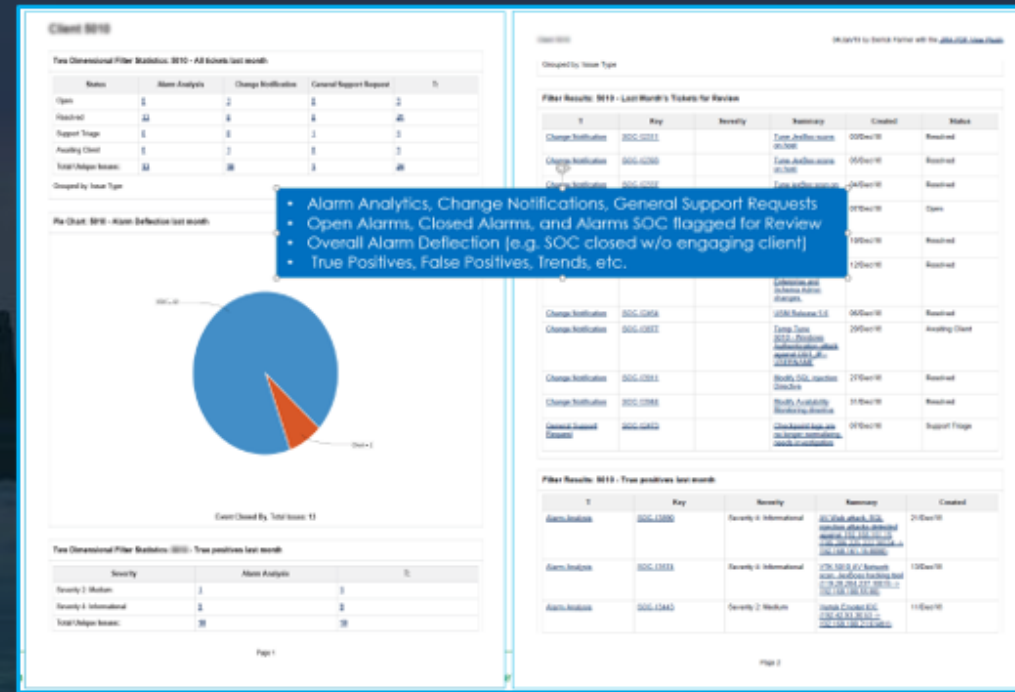
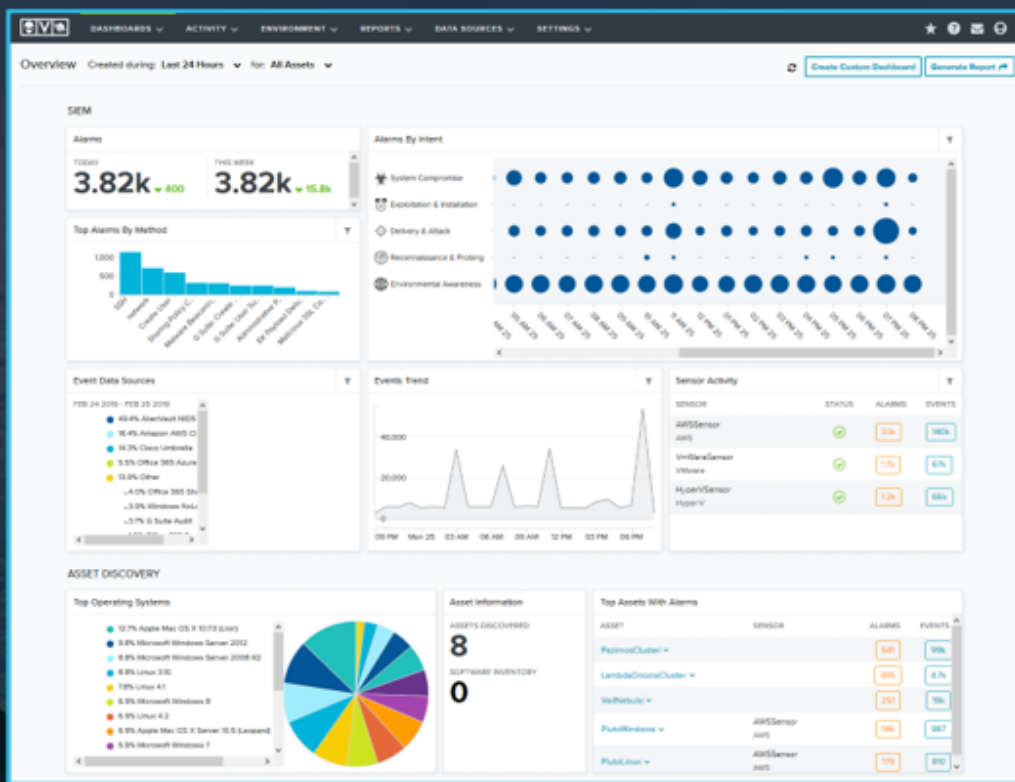
Vertek MDR Service Scoping to Activation



No need to set up a 24/7 Security Operations Center (SOC), we've done it for you



MDR: SIEM Based 24x7 Detection & Response



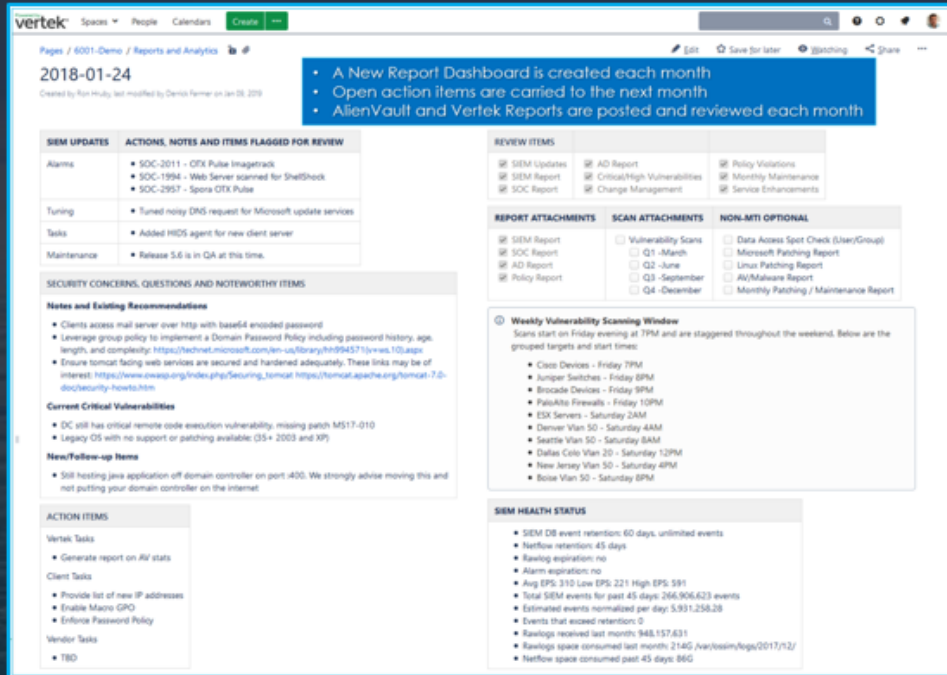
SIEM Health and Real-Time Security Metrics

- Asset Reports
- Alarm Reports
- Threat Reports
- Policy Reports
- Event Reports
- Security Reports
- Vulnerability Reports

Monthly Alarm Status Reports

- Active Alarms, Assignment and Status
- Total Alarms (SOC Deflected vs. Client Interaction)
- True Positive Alarms sorted by severity
- False Positive Alarms

MTI: MDR + Advanced Analytics, Intelligence, Reporting



Monthly Incident and Action Dashboard

- Deployment Status & Environmental Changes
- Outstanding and Important Alarms, Vulnerabilities
- Service Tuning and Maintenance Tickets
- SIEM Total Events and Statistics
- Document Network Changes | Critical Vulnerabilities
- Generate and Track Client & Vertek Action Items
- Critical Prioritization and Remediation Guidance
- Track Client Signoff on SIEM Filtering and Suppression

www.vertek.com

Security Operations Management Visibility

Answer key questions stakeholders are asking:

- How secure is our organization?
- Are our security investments paying off?
- Are cybersecurity services delivered in a fashion that meet the business needs?
- Are our IR capabilities adequately managing the impact of incidents to the organization?

MDR, MTI Feature Comparison



Managed Security Solution Features	MDR	MDR+MTI
Baseline inventory scanning and asset registration	Included	Included
Baseline vulnerability environment scanning	Included	Included
Baseline event correlation, tuning and alarm trimming	Included	Included
Basic threat dashboard and report creation	Advanced	Advanced
SIEM tuning	Continuously	Continuously
Vulnerability scanning	Weekly	Weekly
Network IDS and endpoint monitoring	Included	Included
Security Orchestration, Automation and Response (SOAR)	Included	Included
SIEM alarm monitoring and analysis	Included	Included
Remediation guidance	Included	Included
Quarterly service/relationship review with TAM	Included	Included
Lifecycle and compliance report management	NA	Included
Monthly service/technical security review with analyst	NA	Monthly
Advanced analytics/dashboard reviews	NA	Quarterly

Managed Reports and Advanced Analytics



Tactical MONTHLY – Immediate Security Alarms Items and Action Tracking

- Inform management of relevant details, risks, current status and progress, tasks to be completed, and expected outcomes and dates – supporting regulatory compliance requirements, audits.

Client Dashboard

- Client Specific IR Playbook and Escalation Matrix
- RSS feeds related to industry and Vertek OIX
- Request or Review Alarm or Platform Tickets
- System Maintenance Notifications
- Link to Report and Analytics

MDR

2018-01-24

- A New Report Dashboard is created each month
- Open action items are carried to the next month
- AlienVault and Vertek Reports are posted and reviewed each month

MTI

Client 6010

Alarm Analytics, Change Notifications, General Support Requests

- Open Alarms, Closed Alarms, and Alarms SOC flagged for Review
- Overall Alarm Deflection (e.g. SOC closed w/o engaging client)
- True Positives, False Positives, Trends, etc.

MDR

Client Portal

Monthly Incident & Action Dashboard

Monthly Alarm Status Report – Last 30 days



- A New Report Dashboard is created each month
- Open action items are carried to the next month
- AlienVault and Vertek Reports are posted and reviewed each month

SIEM UPDATES	ACTIONS, NOTES AND ITEMS FLAGGED FOR REVIEW
Alarms	<ul style="list-style-type: none"> • SOC-2011 - OTX Pulse Imagertrack • SOC-1994 - Web Server scanned for ShellShock • SOC-2957 - Spora OTX Pulse
Tuning	<ul style="list-style-type: none"> • Tuned noisy DNS request for Microsoft update services
Tasks	<ul style="list-style-type: none"> • Added HIDS agent for new client server
Maintenance	<ul style="list-style-type: none"> • Release 5.6 is in QA at this time.

REVIEW ITEMS		
<input checked="" type="checkbox"/> SIEM Updates	<input checked="" type="checkbox"/> AD Report	<input checked="" type="checkbox"/> Policy Violations
<input checked="" type="checkbox"/> SIEM Report	<input checked="" type="checkbox"/> Critical/High Vulnerabilities	<input checked="" type="checkbox"/> Monthly Maintenance
<input checked="" type="checkbox"/> SOC Report	<input checked="" type="checkbox"/> Change Management	<input checked="" type="checkbox"/> Service Enhancements

REPORT ATTACHMENTS	SCAN ATTACHMENTS	NON-MTI OPTIONAL
<input checked="" type="checkbox"/> SIEM Report	<input type="checkbox"/> Vulnerability Scans	<input type="checkbox"/> Data Access Spot Check (U
<input checked="" type="checkbox"/> SOC Report	<input type="checkbox"/> Q1 -March	<input type="checkbox"/> Microsoft Patching Report
<input checked="" type="checkbox"/> AD Report	<input type="checkbox"/> Q2 -June	<input type="checkbox"/> Linux Patching Report
<input checked="" type="checkbox"/> Policy Report	<input type="checkbox"/> Q3 -September	<input type="checkbox"/> AV/Malware Report
	<input type="checkbox"/> Q4 -December	<input type="checkbox"/> Monthly Patching / Maint

SECURITY CONCERNS, QUESTIONS AND NOTEWORTHY ITEMS

Notes and Existing Recommendations

- Clients access mail server over http with base64 encoded password
- Leverage group policy to implement a Domain Password Policy including password history, age, length, and complexity: [https://technet.microsoft.com/en-us/library/hh994571\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/hh994571(v=ws.10).aspx)
- Ensure tomcat facing web services are secured and hardened adequately. These links may be of interest: https://www.owasp.org/index.php/Securing_tomcat <https://tomcat.apache.org/tomcat-7.0-doc/security-howto.htm>

Current Critical Vulnerabilities

- DC still has critical remote code execution vulnerability, missing patch MS17-010
- Legacy OS with no support or patching available: (35+ 2003 and XP)

New/Follow-up Items

- Still hosting java application off domain controller on port :400. We strongly advise moving this and not putting your domain controller on the internet

Weekly Vulnerability Scanning Window

Scans start on Friday evening at 7PM and are staggered throughout the weekend. E grouped targets and start times:

- Cisco Devices - Friday 7PM
- Juniper Switches - Friday 8PM
- Brocade Devices - Friday 9PM
- PaloAlto Firewalls - Friday 10PM
- ESX Servers - Saturday 2AM
- Denver Vlan 50 - Saturday 4AM
- Seattle Vlan 50 - Saturday 8AM
- Dallas Colo Vlan 20 - Saturday 12PM
- New Jersey Vlan 50 - Saturday 4PM
- Boise Vlan 50 - Saturday 8PM

ACTION ITEMS
Vertek Tasks
<ul style="list-style-type: none"> • Generate report on AV stats
Client Tasks
<ul style="list-style-type: none"> • Provide list of new IP addresses • Enable Macro GPO • Enforce Password Policy
Vendor Tasks
<ul style="list-style-type: none"> • TBD

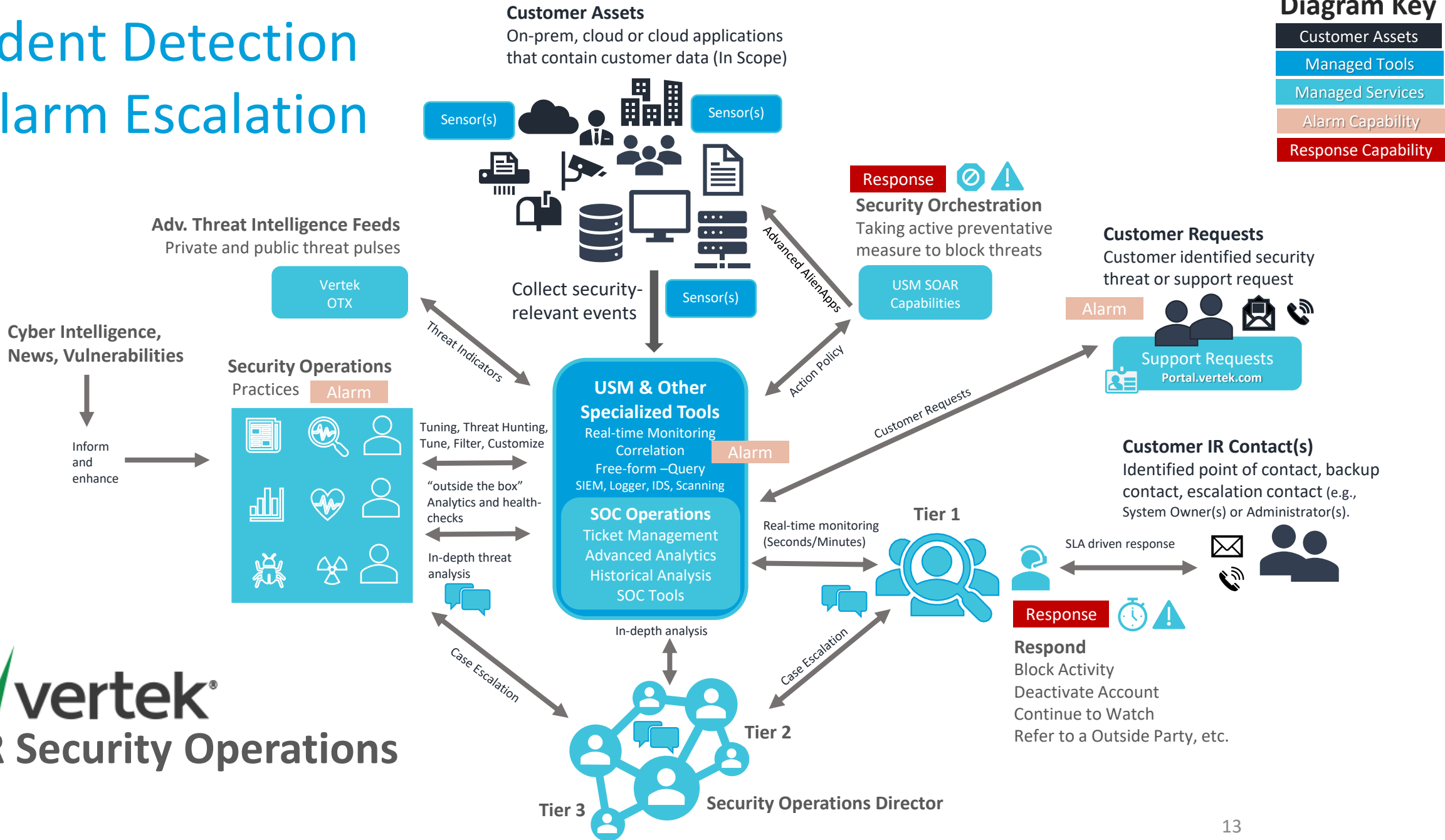
SIEM HEALTH STATUS
<ul style="list-style-type: none"> • SIEM DB event retention: 60 days, unlimited events • Netflow retention: 45 days • Rawlog expiration: no • Alarm expiration: no • Avg EPS: 310 Low EPS: 221 High EPS: 591 • Total SIEM events for past 45 days: 266,906,623 events • Estimated events normalized per day: 5,931,258.28 • Events that exceed retention: 0 • Rawlogs received last month: 948,157,631 • Rawlogs space consumed last month: 214G /var/ossim/logs/2017/12/ • Netflow space consumed past 45 days: 86G

- ## MTI: Monthly Incident & Action Dashboard
- Discuss Outstanding and Important Alarms, Vulnerabilities
 - Provide Critical Prioritization and Remediation Guidance
 - Review Tuning and Maintenance Tickets
 - Provides SIEM Total Events and Statistics
 - Discuss Standard and Custom Reports
 - Track Current Deployment Status and Environmental Changes
 - Follow-Up on Network Changes and Critical Vulnerabilities
 - Generate and Track Action Items for Client and Vertek
 - Track Client Signoff on SIEM Filtering and Suppression

Incident Detection & Alarm Escalation

Diagram Key

Customer Assets
Managed Tools
Managed Services
Alarm Capability
Response Capability



Security Operations Incident Escalation

Tier 3+

Security Operations Director
VP Cybersecurity



Qualifications:

- Cleared to work (e.g., drug and background checks, etc.)
- 2-5 years of experience in IT related work. Active mentor program in place.
- Experience with security tools, ticketing systems and compliance frameworks, CIA Triad
- Required Certification: ACSE/AVSE
- Industry Certifications: Security +, Network+, Linux+, CYSA, MTA

Core Competencies:

- Demonstrated understanding adversary tactics and techniques (threat models and methodologies used)
- Demonstrated ability to apply security knowledge to identify and respond to threats
- Demonstrated ability to identify and escalate security incidents to appropriate resources
- Demonstrated ability to make decisions and solve problems while working under pressure
- Demonstrated ability to troubleshoot and problem solve with thoroughness and attention to detail
- Demonstrated ability to communicate with all levels of management and company personnel

Qualifications:

- 5-10 years of experience in IT security related work
- 2-5 years of IT networking related experience
- Industry Certifications: CEH, Pentest+, CASP, MTA, MCSA

Core Competencies:

- Demonstrated ability to understand client networks and support a broad range of security technologies
- Demonstrated understanding of risk management and industry compliance frameworks
- Demonstrated ability to proactively identify and communicate client satisfaction issues
- Demonstrated ability to provide security thought-leadership to clients

Qualifications:

- DevSecOps experience, coding, and automation experience
- 10+ years of IT security experience
- 10+ years of IT networking experience
- Industry Certifications: OSCP, CISSP, CISA, CCNP, MCSA, MCSE, MCSA

Core Competencies:

- Demonstrated ability to interpret security principles/standards and apply them to systems and operations
- Demonstrated ability to perform service and security audits, work with auditors, and take lead of security projects and initiatives
- Demonstrated ability to design and develop scalable and secure multi-tenant security services
- Demonstrated ability to interpret analytics to provide program performance to the director and head of cyber
- Demonstrated ability to interact with clients to obtain feedback, discuss analytics, integration, API development
- Demonstrated ability to provide quality work outputs in any aspect of security
- Demonstrated ability to achieve trusted security advisor status among customers, peers and industry followers

Tier 1

Tier 2

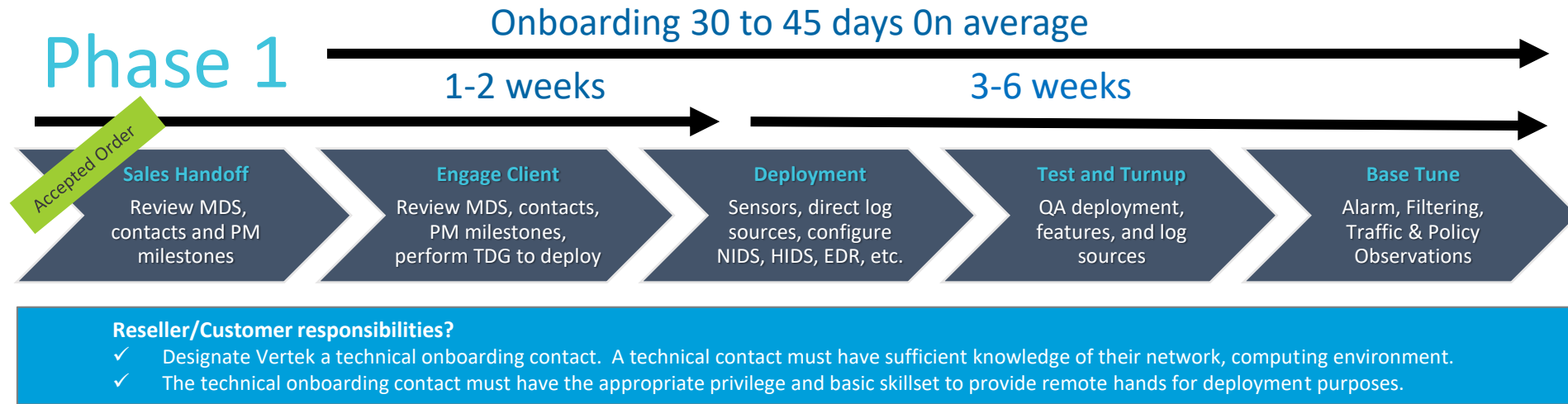
Tier 3

- **Inventory and correctly classify IT assets according to risk** – *so IT can effectively protect, monitor assets*
- **Periodically scan, assess and report on unpatched software, system vulnerabilities** – *so IT can proactively patch and update systems*
- **Continuously identify malicious entities probing the monitored systems and network** – *so IT and the business can know when attacks are occurring, who is attacking and how to block attacks*
- **Continuously monitor network traffic and system events for potential unsecure behaviors** – *so IT and the business knows if systems and data is being accessed by the wrong people*
- **Work with Customer IT to respond to identified malicious events to remediate them** – *so IT has expert cybersecurity engineers and analysts at their side, helping them to defend and protect the company*
- **Provide ongoing service auditing and will report on service effectiveness** – *so IT and Vertek can continue to improve the service and add value to Customer*

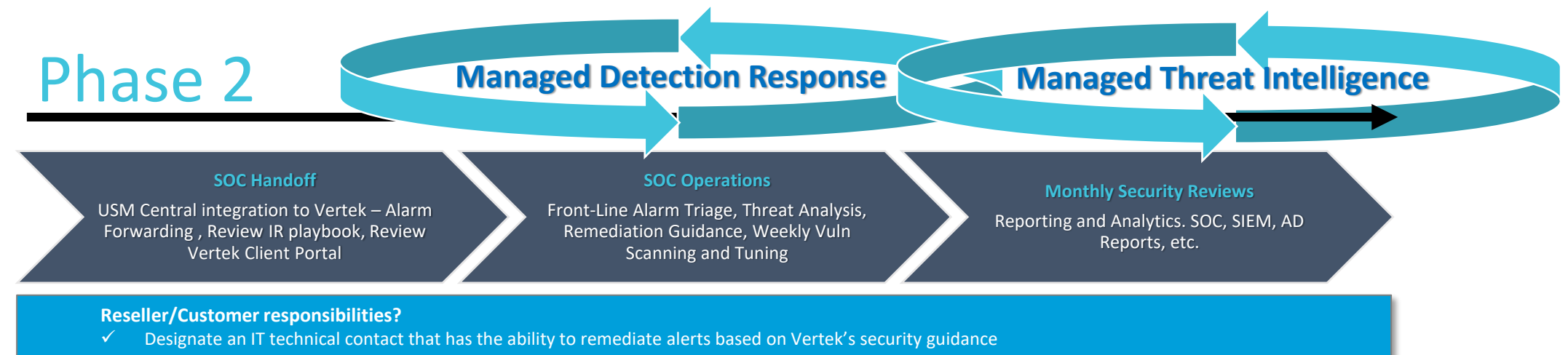
Security Event Priority	Internal Response Time	Client Response Time
Severity 1: High. Anomalous / Suspicious events and activities that indicate an attack in progress. Exploitation and system compromise.	1 hour	2 hours
Severity 2: Medium. Anomalous / Suspicious events and activities that have occurred in succession or resemble an unauthorized attempt to access a system.	2 Support Hours	4 Support Hours
Severity 3: Low. Anomalous / Suspicious events and activities that alone might not constitute a major risk but should be monitored for repeat occurrences.	8 Support Hours	24 Support Hours
Severity 4: Informational. Security events and activities that should be brought to Client's attention that may or may not need to be dealt with to prevent future security events or incidents.	24 Support Hours	Informational only. Included in monthly report

- **24x7 SOC Coverage:** Service-generated alarms sent to Vertek Security Analyst, 365 days a year
- **12x5 SOC Coverage:** Service-generated alarms sent to Vertek Security Analyst, 8am to 8pm EST, Monday thru Friday, and excluding US national holidays
- **9x5 SOC Coverage:** Service-generated alarms sent to Vertek Security Analyst, 8am to 5pm EST, Monday thru Friday, and excluding US national holidays

Implementation



Complete Onboarding & Lifecycle



Service	MDR - Managed Detection & Response Functionality
Description	Detect and respond to threats on premise, in the cloud or in cloud applications
Remote Deployment of Unified Security Management (USM) Solution	<ul style="list-style-type: none"> Physical or virtual appliance deployment Inventory scanning and asset registration Network and endpoint monitoring Baseline vulnerability environment scanning Event correlation, tuning and alarm trimming Basic USM dashboard and MDR report creation
Alarm Monitoring	<ul style="list-style-type: none"> 24x7 Coverage for Severity Level 1 12x5 Coverage for Severity Levels 2 9x5 Coverage for Severity Levels 3-4
SIEM Tuning	<ul style="list-style-type: none"> Continuous
Ticket Creation	<ul style="list-style-type: none"> Included
Threat Analysis	<ul style="list-style-type: none"> 24x7 Coverage for Severity Level 1 12x5 Coverage for Severity Levels 2 9x5 Coverage for Severity Levels 3-4
Remediation Guidance	<ul style="list-style-type: none"> Included
Automated Threat Response	<ul style="list-style-type: none"> Based on USM integration capabilities with Client technology
Client Portal	<ul style="list-style-type: none"> Service notifications Incident response contact and escalation documentation Request alarm or USM support View and respond to tickets Industry feeds and advisories Track USM filtering and suppression 2 portal accounts come standard
Unified Security Management (USM) console access	<p>Read-only Appliance access (clients can access views and search but cannot make system changes that impact other users.). Actions Read-only can take:</p> <ul style="list-style-type: none"> Create dashboard and dashboard views View alarms page and alarm details View events page and event details View asset page and assets details View vulnerabilities page and vulnerabilities details View environment configuration issues and environment users View the saved reports page
Lifecycle Management	<ul style="list-style-type: none"> Platform updates, signature updates, platform maintenance Verification of Data Backup; configuration and job status Health monitoring of Service Software and Appliance
Service Reporting	<ul style="list-style-type: none"> Monthly MDR report emailed to Client contacts (e.g., incident response activities, alarm analytics, change notifications, alarms flagged for review, overall alarm deflection, etc.)
Service Review	<ul style="list-style-type: none"> Quarterly Technical Account Manager guided service review to discuss performance, discuss Client roadmap, obtain service feedback, set high-level goals and objectives

Without visibility into attacks, threats and risks, it's impossible to measure, control and mitigate risk, capture a return on investment, and continuously improve your security or risk program to drive positive business outcomes.

Vertek's Managed Threat Intelligence (MTI) service expands the basic Managed Detection and Response service by providing a greater level of incident response and threat support, and access to dashboards and advanced analytics helping clients to advance their cyber-maturity, realize business value, and proactively reduce risk.

Service	MTI - Managed Threat Intelligence Functionality
Description	MDR + Advanced analytics and Client security operations oversight
Security Action Dashboard	<ul style="list-style-type: none"> • Monthly incident and action dashboard creation • Monthly SIEM, SOC report creation and review • Security concerns, questions and noteworthy items • Monthly report repository
Advanced Analytics Platform	<ul style="list-style-type: none"> • Client SAML authentication provider required • Detect, protect and respond dashboards • Access to 35+ security visualizations and user guides • Ability to customize report visualizations and create dashboards
Service Reporting	<ul style="list-style-type: none"> • Ability to export reports from Vertek's Client Portal or from the Advanced Analytics Platform
Service Review	<ul style="list-style-type: none"> • Monthly Security Analyst guided alarm review, report review, and tuning discussion (e.g., discuss outstanding and important alarms and vulnerabilities, help prioritize and set remediation activities, discuss standard and custom reports and document action items that carry forward month to month.)

Client Portal

Client Support Portal

- Identifies IR Playbooks, SOC Handoff
- Provides Industry Specific RSS feeds
- Request Alarm or SIEM Platform Support



Powered by vertek Spaces People Calendars Create

Pages 6001-Demo
Created by Ron Hruby, last modified by Bruce Haskin on Mar 29, 2018

COMPANY LOGO

Client Dashboard

- Request Alarm or Platform Support
- Currently Open Requests
- Reports and Analytics
- Change Password

system maintenance
no outages or maintenance items to report
Client Identifier: 6001

- Account Management | Kristen Kennedy | kkennedy@vertek.com
- Billing and Finance | Pete McCormick | pmccormick@vertek.com
- Director of SOC Operations | Ron Hruby | rhruby@vertek.com
- General Questions | Security Operations Center | SOC@vertek.com

CLIENT CONTACTS	OTHER CONTACTS
Primary contact in the event of a critical event: <ul style="list-style-type: none"> Name: Title: Information Security Manager Phone: E-Mail: NOTE: Primary Critical Event & Technical Contact 	MSP/Vendor Technical contact: <ul style="list-style-type: none"> Company: Name: Title: Phone: E-Mail:
Secondary Contact: <ul style="list-style-type: none"> Name: Title: Phone: E-Mail: NOTE: Secondary Critical Event & Technical Contact 	Security Alarm/Event CC: <ul style="list-style-type: none"> Company: Name: Title: Phone: E-Mail:
Change Management Contact: <ul style="list-style-type: none"> Name: Title: Phone: E-Mail: NOTE: Special notes or approval process HERE 	Escalation Contact: <ul style="list-style-type: none"> Name: Title: Phone: E-Mail: NOTE: Special notes or approval process HERE

Initial Contact:

BGH:5012	Initial Contact	(DG)BGH Notifications	(PC)John.doe@bgh.com; (SC)Jane.doe@bgh.com	Escalations should occur if no response within 1 hour
----------	-----------------	-----------------------	---	---

Escalations:

BGH:5012	Escalations	(DG)BGH Notifications	(PE)it.manager@bgh.com; (SE)dir.manager@bgh.com	Escalate to secondary by phone if it.manager does not respond within the hour
----------	-------------	-----------------------	--	---

Vertek Accelerate to Value

SIEM: DIY or Managed Threat Intelligence

- How to Cement Your Trusted Advisor Status with Managed Threat Intelligence
- Ask These Critical Questions About Compliance and Managed Threat Intelligence
- What is a SIEM and Why Does My Customer Need One?
- A Vertek Threat Intelligence Analyst Identifies Trik Spam Botnet Leaks 43 Million Email Addresses
- Microsoft Patches IE Zero-Day Dubbed "Double Kill"
- Microsoft Patches 17 year old MS Office Memory Corruption Flaw
- Detection and Prevention of Bad Rabbit Ransomware
- Malware distributed via MS Office DDE "feature" — no macros required!
- Locky ransomware switches up extension with asasin variant

US-CERT Alerts

Alerts warn about vulnerabilities, incidents, and other security issues that pose a significant risk.

- AA19-024A: DNS Infrastructure Hijacking Campaign
- AA18-337A: SamSam Ransomware
- TA18-331A: 3ve - Major Online Ad Fraud Operation
- AA18-284A: Publicly Available Tools Seen in Cyber Incidents Worldwide
- TA18-276B: Advanced Persistent Threat Activity Exploiting Managed Service Providers
- TA18-276A: Using Rigorous Credential Control to Mitigate Trusted Network Exploitation
- TA18-275A: HIDDEN COBRA - FASTCash Campaign
- TA18-201A: Emotet Malware
- TA18-149A: HIDDEN COBRA - Joannap Backdoor Trojan and Brambul Server Message Block Worm
- TA18-145A: Cyber Actors Target Home and Office Routers and Networked Devices Worldwide

Analytics

Monthly Alarm Status Report – Last 30 days

- Alarms by status – Who has the action items on security alarms
- Deflection – Tracks how well the SOC understands the client environment
- Alarm information - Tracks the number of true positives sorted by severity
- Alarm information - Tracks the number of true positives vs. false positives



Client 5010

Two Dimensional Filter Statistics: 5010 - All tickets last month

Status	Alarm Analysis	Change Notification	General Support Request	T:
Open	0	1	0	1
Resolved	13	8	0	21
Support Triage	0	0	1	1
Awaiting Client	0	1	0	1
Total Unique Issues:	13	10	1	24

Grouped by: Issue Type

Pie Chart: 5010 - Alarm Deflection last month

Event Closed By, Total Issues: 13

Two Dimensional Filter Statistics: True positives last month

Severity	Alarm Analysis	T:
Severity 2: Medium	1	1
Severity 4: Informational	9	9
Total Unique Issues:	10	10

Page 1

- Alarm Analytics, Change Notifications, General Support Requests
- Open Alarms, Closed Alarms, and Alarms SOC flagged for Review
- Overall Alarm Deflection (e.g. SOC closed w/o engaging client)
- True Positives, False Positives, Trends, etc.

04/Jan/19 by Derrick Farmer with the [JIRA PDF View Plugin](#)

Grouped by: Issue Type

Filter Results: 5010 - Last Month's Tickets for Review

T	Key	Severity	Summary	Created	Status
Change Notification	SOC-12311		Tune JexBox scans on host	03/Dec/18	Resolved
Change Notification	SOC-12393		Tune JexBox scans on host	05/Dec/18	Resolved
Change Notification	SOC-12337		Tune iexBox scan on	04/Dec/18	Resolved
			Enterprise and Schema Admin changes	07/Dec/18	Open
			USM Release 5.6	10/Dec/18	Resolved
			Temp Tune 5010 - Windows Authentication attack against DST_IP - USERNAME	12/Dec/18	Resolved
Change Notification	SOC-12454		USM Release 5.6	06/Dec/18	Resolved
Change Notification	SOC-13877		Temp Tune 5010 - Windows Authentication attack against DST_IP - USERNAME	20/Dec/18	Awaiting Client
Change Notification	SOC-13911		Modify SQL injection Directive	27/Dec/18	Resolved
Change Notification	SOC-13944		Modify Availability Monitoring directive	31/Dec/18	Resolved
General Support Request	SOC-12473		Checkpoint logs are no longer normalizing, needs investigation	07/Dec/18	Support Triage

Filter Results: 5010 - True positives last month

T	Key	Severity	Summary	Created
Alarm Analysis	SOC-13890	Severity 4: Informational	AV Web attack SQL injection attacks detected against 192.168.161.15 (185.206.225.222:38534 -> 192.168.161.15:8080)	21/Dec/18
Alarm Analysis	SOC-13574	Severity 4: Informational	VTK 5010 AV Network scan_JexBoss hacking tool (119.28.204.237:10015 -> 192.168.100.55:80)	13/Dec/18
Alarm Analysis	SOC-13443	Severity 2: Medium	Vertek Emotet IOC (192.42.93.30:53 -> 192.168.100.21:61491)	11/Dec/18

Page 2

Value & Impact of MDR, MTI

TIME, RESOURCE & RISK REDUCTION

Vertek will...

- Inventory and correctly classify IT assets according to risk – *so IT can effectively protect, monitor assets*
- Periodically scan, assess and report on unpatched software, system vulnerabilities – *so IT can proactively patch and update systems*
- Continuously identify malicious entities probing the monitored systems and network – *so IT and the business can know when attacks are occurring, who is attacking and how to block attacks*
- Continuously monitor network traffic and system events for potential unsecure behaviors – *so IT and the business knows if systems and data is being accessed by the wrong people*
- Work with Customer IT to respond to identified malicious events to remediate them – *so IT has expert cybersecurity engineers and analysts at their side, helping them to defend and protect the company*
- Provide ongoing service auditing and will report on service effectiveness – *so IT and Vertek can continue to improve the service and add value to Customer*

COST & RISK REDUCTION

Vertek's MDR service...

- Reduces the need to hire 1st, 2nd and 3rd shift security analysts – *saving \$100,000 in additional salaries x 3*
- Reduces the need to purchase, maintain, operate security information event & monitoring software – *saving the company an estimated software, maintenance and training costs of \$30,000 per year*

***TOTAL EST YEAR 1 SAVINGS: \$330,000**

*Versus hiring additional analysts, engineers, and running, maintaining the SIEM internally

Supplemental Slides: MDR

 **MDR - Managed Detection & Response**

MTI - Managed Threat Intelligence

MDR + MTI Custom

Solutions designed around AT&T Cybersecurity Unified Security Management (USM) Anywhere Platform

USM Includes Threat Detection Capabilities



Open Threat Exchange® (OTX™) Threat Indicators

100,000 participants in 140 countries, contributing over 19 million threat indicators daily.

OTX Pulse

Pulses provide you with a summary of the threat, a view into the software targeted, and the related indicators of compromise (IOC) that can be used to detect the threats.

IOCs include:

- IP addresses
- Domains
- Hostnames (subdomains)
- Email
- URL
- URI
- File Hashes: MD5, SHA1, SHA256, PEHASH, IMPHASH
- CIDR Rules
- File Paths
- MUTEX name
- CVE number

Pulses make it easy for you to answer questions like:

- Is my environment exposed to this threat?
- Is this relevant to my organization?
- Who is behind this, and what are their motives?
- What are they targeting in my environment?

The screenshot displays a web browser window showing an OTX Pulse page. The main heading is "Multiple covid-19 related malware threats - March 30th". Below the heading, there is a summary of the threat, including references to Twitter posts and tags like "covid-19, malware, android, Anubis, Cerberus, Xerxes, Nanocore, malwrhunterteam". A section titled "Types of Indicators" shows a bar chart with categories: URL (2), FileHash-SHA256 (5), Domain (4), FileHash-SHA1 (5), and FileHash-MD5 (5). Below this is a table of indicators with columns for Type, Indicator, Title, Added, Active, and Related Pulses.

TYPE	INDICATOR	TITLE	ADDED	ACTIVE	RELATED PULSES
FileHash-SHA1	017105e5ab63b3c15866b24a9dca45a9df19bbc		Mar 30, 2020, 4:31:39 PM	●	2
FileHash-MD5	4ddd83359040f9958f777cdf5819b192		Mar 30, 2020, 4:31:39 PM	●	2
FileHash-SHA256	a754c35d09677b0b96d8a0dad5c9c5fdd28abd8c72d8d38a9bd945ca8362e02		Mar 30, 2020, 4:31:39 PM	●	6
FileHash-SHA1	a24d10310a01794c463bb43d0284b983aaac11e	Nanocore, NanoCore	Mar 30, 2020, 4:31:39 PM	●	0
FileHash-MD5	50ca929ae4fd1d38c2e97d17a6bd404e	Nanocore, NanoCore	Mar 30, 2020, 4:31:39 PM	●	0
FileHash-SHA256	96f183bd8300b59d995110d0ae5ac2e79961e21640acd5f434fe630c7da4ec45	Nanocore, NanoCore	Mar 30, 2020, 4:31:39 PM	●	0
domain	rmagent.xyz		Mar 30, 2020, 4:31:39 PM	●	0
FileHash-SHA1	003ea98c3aeeb87df64918704fedc6c6bf1a5c		Mar 30, 2020, 4:31:39 PM	●	0
FileHash-SHA1	8dd03b7b7e130113b4685ccfa80ba790ba5f847		Mar 30, 2020, 4:31:39 PM	●	0
FileHash-MD5	5815a29e5f062840f4bc9620a8b618a		Mar 30, 2020, 4:31:39 PM	●	0

Vertek Enhanced Capabilities Included in MDR

Cybersecurity Resources

Cybersecurity Resources From Vertek

We're always looking to add more resources!

Your input helps us create content that would be valuable to you.

[SUGGEST AN IDEA](#)

THREATS AND IOCS

HAFNIUM: Exchange
Zero Days Actively
Exploited by APT
Group

[READ](#)

CYBERSECURITY, HOW TO,
RESOURCES

MSSP Tips & Tricks:
Security Operations
Management Metrics
and Analytics
Considerations

[WATCH VIDEO](#)

CYBERSECURITY, HOW TO,
RESOURCES

MSSP Tips & Tricks:
Creating an OTX
account

[WATCH VIDEO](#)

CYBERSECURITY, HOW TO,
RESOURCES

MSSP Tips & Tricks:
Integrating OTX With
USM Anywhere

[WATCH VIDEO](#)

CYBERSECURITY, HOW TO,
RESOURCES

MSSP Tips & Tricks:
Creating an OTX Pulse

[WATCH VIDEO](#)

CYBERSECURITY, HOW TO,
RESOURCES

MSSP Tips & Tricks:
Connecting OTX To
The USM API

[WATCH VIDEO](#)

Search

Enter search term...

Resource Type

- Cloud Computing
- Cybersecurity
- Case Study
- How To
- News and Events
- Resources
- Threats and IOCs

Industry

- Finance
- Healthcare
- Manufacturing
- Other
- Utility

Topics

- AlienVault
- Cybersecurity
- Events
- Industry Best Practices
- SIEM
- SOC
- Threat Detection

Media

- Blog
- PDF
- Video

www.vertek.com

We've found 42 results for "vthehelpdesk"

Advanced Threat Detection



PhishTank - Dynamic List of Verified/Online Dropbox Phishing URLs

MODIFIED 17 MINUTES AGO by vthehelpdesk | Public | TLP: ○ White

URL: 753

This is an automated process that is updated hourly by the Vertek MTI Labs Team. We pull all active/online and verified phishing URLs from phishtank API and parse the list for URLs containing "dropbox". These indicators include phishing, dropbox, vsoc, Vertek MTI



PhishTank - Dynamic List of Verified/Online Banking Phishing URLs

MODIFIED 17 MINUTES AGO by vthehelpdesk | Public | TLP: ○ White

URL: 403

This is an automated process that is updated hourly by the Vertek MTI Labs Team. We pull all active/online and verified phishing URLs from phishtank API and parse the file for URLs that are related to banking. These indicators include phishing, banking, financial, bank, phishtank, vsoc, Vertek MTI



PhishTank - Dynamic List of Verified/Online Office365 and other Microsoft Phishing URLs

MODIFIED 17 MINUTES AGO by vthehelpdesk | Public | TLP: ○ White

URL: 353

This is an automated process that is updated hourly by the Vertek MTI Labs Team. We pull all active/online and verified phishing URLs from phishtank API and parse the list for URLs containing Microsoft and Office365. These indicators include phishing, microsoft, office365, phishtank, vsoc, Vertek MTI



PhishTank - Dynamic List of Verified/Online Docusign Phishing URLs

MODIFIED 18 MINUTES AGO by vthehelpdesk | Public | TLP: ○ White

URL: 21

This is an automated process that is updated hourly by the Vertek MTI Labs Team. In light of the docusign breach we are pulling all active/online and verified phishing URLs from phishtank API and parse the list for URLs containing phishing, docusign, vsoc, Vertek MTI



PhishTank - Dynamic List of Verified/Online PayPal Phishing URLs

MODIFIED 18 MINUTES AGO by vthehelpdesk | Public | TLP: ○ White

URL: 892

This is an automated process that is updated hourly by the Vertek MTI Labs Team. We pull all active/online and verified phishing URLs from phishtank API and parse the file for URLs reported as PayPal. These indicators are then phishing, PayPal, phishtank, vsoc, Vertek MTI



PhishTank - Dynamic List of Verified/Online IRS (Internal Revenue Service) Phishing URLs

MODIFIED 18 MINUTES AGO by vthehelpdesk | Public | TLP: ○ White

URL: 34

This is an automated process that is updated hourly by the Vertek MTI Labs Team. We pull all active/online and verified phishing URLs from phishtank API and parse the file for URLs reported as IRS phishing scams. These indicators include phishing, IRS, Internal Revenue Service, phishtank, vsoc, Vertek MTI



PhishTank - Dynamic List of Verified/Online GoogleDocs Phishing URLs

MODIFIED 18 MINUTES AGO by vthehelpdesk | Public | TLP: ○ White

URL: 56

This is an automated process that is updated hourly by the Vertek MTI Labs Team. We pull all active/online and verified phishing URLs from phishtank API and parse the file for URLs containing googledocs. These indicators are then phishing, googledocs, phishtank, vsoc, Vertek MTI



HAFNIUM Targeting Exchange Servers With Zero-Day Exploits

MODIFIED 21 DAYS AGO by vthehelpdesk | Public | TLP: ○ White

CVE: 4 | **FileHash-MD5:** 5 | **FileHash-SHA1:** 3 | **FileHash-SHA256:** 14 | **URL:** 1 | **YARA:** 12 | **Domain:** 1 | **Hostname:** 2

webshell, aspx, webshell, azure, sentinel, hafnium, microsoft, exchange, server, powercat, covenant, procdump, lsass, service, powershell, crn_apt, China, email, Exploit, CVE



SolarWinds Breach - SUNBURST Trojan - IOCs

MODIFIED 106 DAYS AGO by vthehelpdesk | Public | TLP: ○ White

FileHash-MD5: 10 | **FileHash-SHA1:** 10 | **FileHash-SHA256:** 16 | **YARA:** 7 | **Domain:** 15 | **Hostname:** 10

teardrop, cobalt strike, fireeye, supernova, cosmicgale, sunburst, solarwinds web, webshell, orion, unc2452, orion software, solarwinds



Tools Allow Vertek to Detect, Alert and Respond to Threats & Cyber Attacks Across All On Premise, Colocation, Cloud Environments

Cloud Apps

Office 365, G-Suite,
and Okta



Private Cloud

VMware & Hyper-
V

Public Cloud

AWS, Azure, &
hosted VPC

Physical Infrastructure

On-premises servers &
machines

Supporting the Alarm from Cradle to Grave



Vertek Analysis

Validation

Did it happen?

Disposition

What does that mean?

Response

What should my customer do?

Customer can respond via
Email or Portal

SLA Metrics
Available!

www.vertek.com

[Ticket Portal](#) / SOC-8879
DEMO TICKET VTK 5001 Gozi / Ursnif Malware Infection (198.49.65.130:80 -> 10.99.99.111:0)

SLAs
2d 5h ✓ Report Incident SLA within 2d 6h

Edit Comment Assign More Move: Waiting for Client Resolve Admin

Details

Type: Alarm Analysis Status: WAITING ON SOC (View Workflow)

Resolution: Lab Team Tripped

Sent From: alarm_mailer@vertek.com

Client: Alarm Info OTX Info

Client ID: 5002
 Client Device: USM5002
 Architecture: AV Appliance
 Severity: Severity 2: Medium
 Alarm Category: Environmental Awareness
 Rule Strategy: OTX Indicators of Compromise
 Rule Method: PULSE
 Directive Name: OTX Pulse: PULSE
 Alarm Created Date / Time: 2020-10-22 17:12:45

Source IP: 192.35.51.30
 Destination IP: 192.168.80.101
 Source Port: 53
 Destination Port: 49758
 Source Name: None
 Destination Name: toc-ads01
 Event Closed By: CSOC

Dynamic OTX inspection

OTX Pulse ID: 5C3C9451CDB49E3D43C87AD5
 OTX Hash: 8808ef5064dffe421fe42cc1df0d5b3
 OTX IOC Value: ovationcomm[.]com

Non RFC1918 analysis lookups

Internal lookup inspection of trends

Workflow

People

- Derrick Farmer (Assign to me)
- Auto Attendant
- Ron Hruby

Request

Request type: Alarm Analysis
 Customer status: Waiting on SOC
 Channel: JIRA

Dates

Created: 23/Apr/18 11:12 AM
 Updated: 15/Dec/18 9:06 AM

Time Tracking

Estimated: 0m
 Remaining: 0m
 Logged: 27m

Automated Log Work

Your timer: Not started

Attachments

Drop files to attach, or browse.

image-2018-04-23-11-27-54
 23/Apr/18 11:28 AM 377 KB

image-2018-04-23-11-29-52
 23/Apr/18 11:30 AM 302 KB

image-2018-04-23-11-31-08
 23/Apr/18 11:31 AM 377 KB

image-2018-04-23-11-31-14
 23/Apr/18 11:31 AM 277 KB

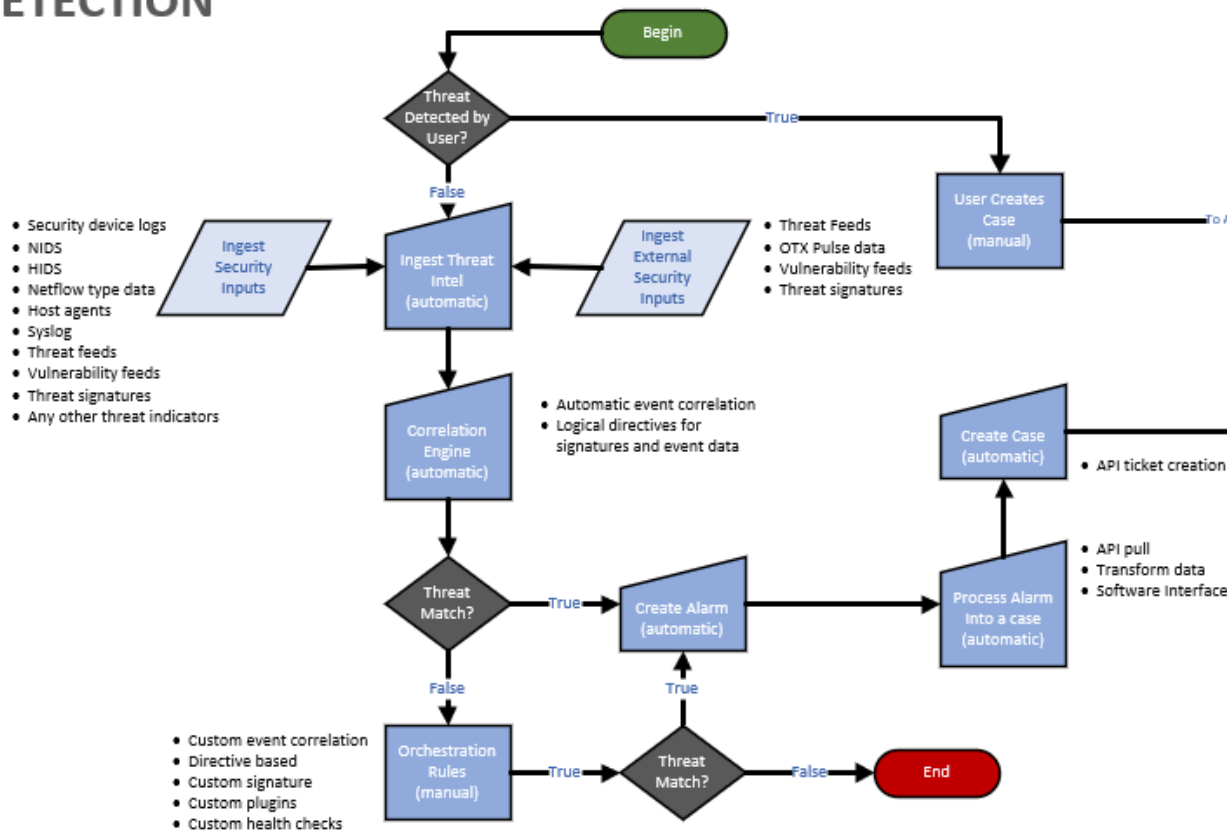
image-2018-04-23-11-35-45
 23/Apr/18 11:35 AM 254 KB

- Advanced Threat Intel
- Threat Analysis
- Remediation Guidance
- SOC Ticket and SLA Response Metrics
- Client IDs (5001) vs. Client Names

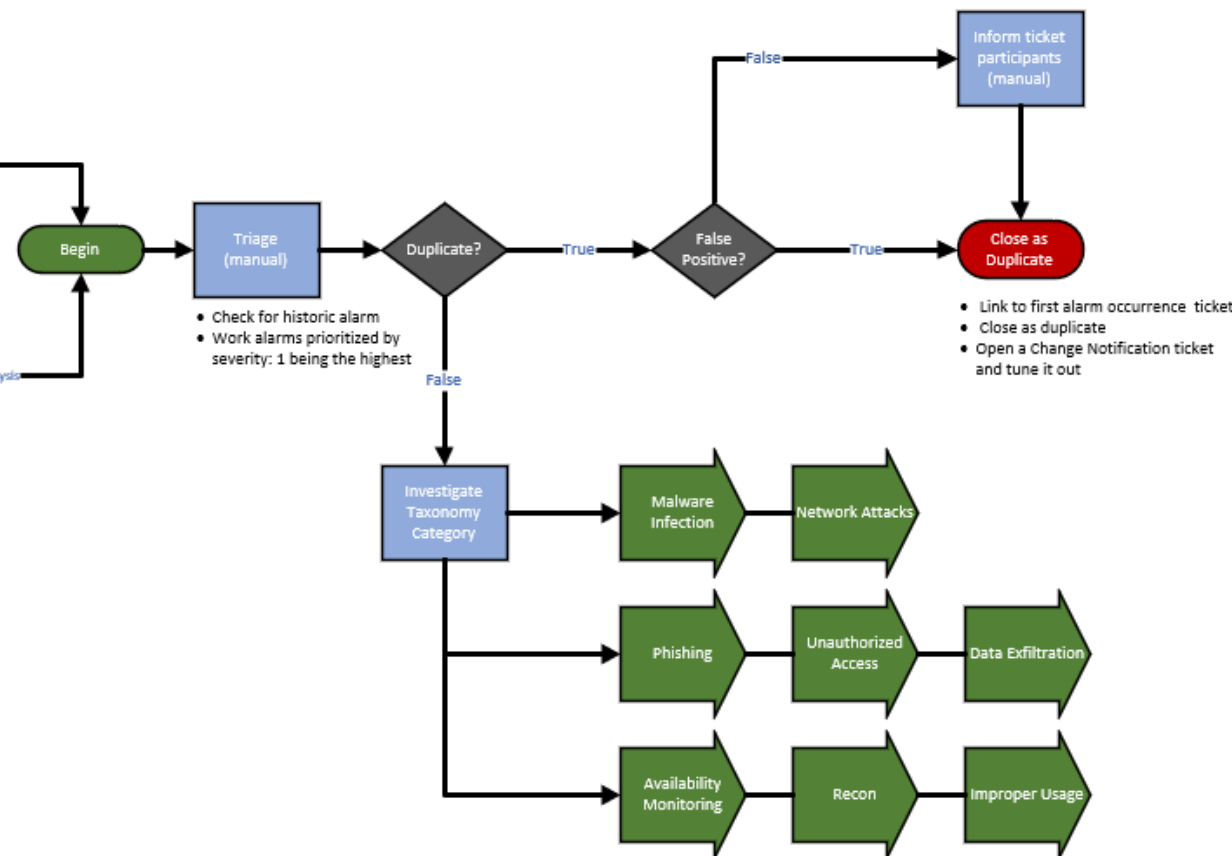
Providing NIST Compliant Processes



DETECTION



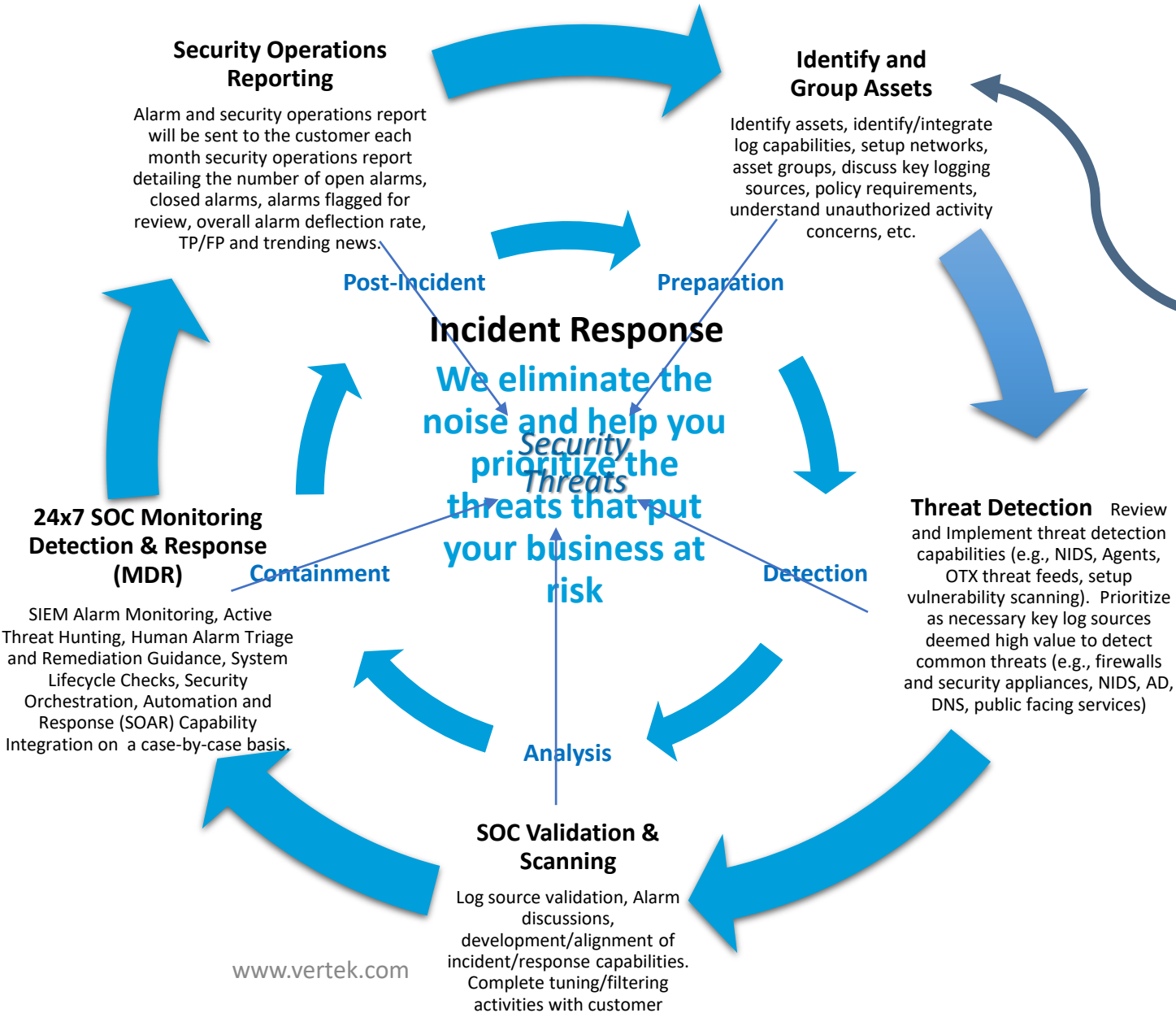
ANALYSIS



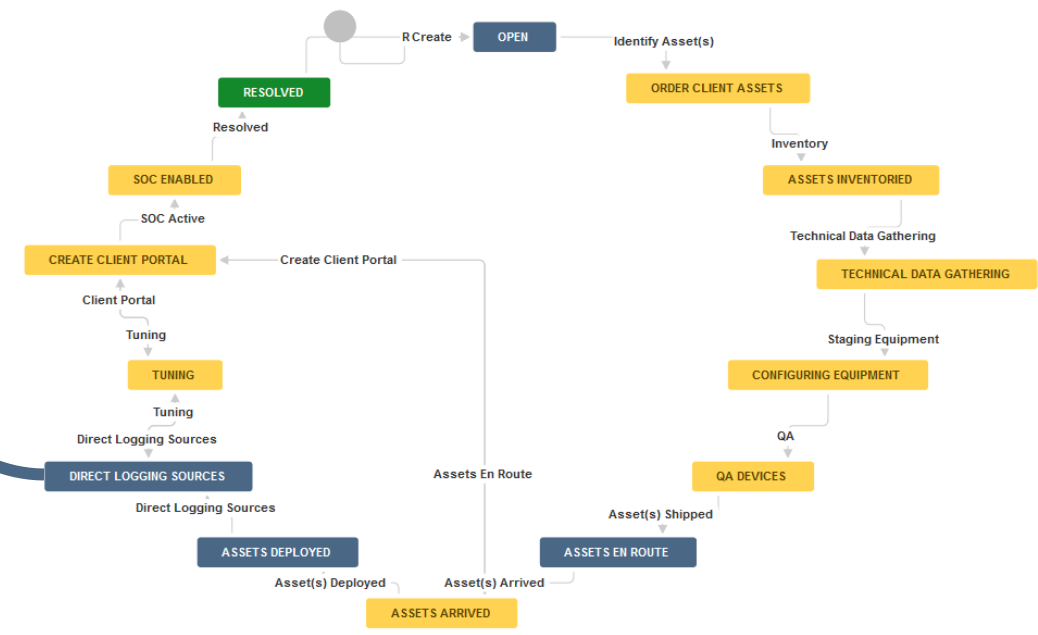
Sample Incident Responses Playbook

Detection – Analysis – Contain/Eradicate – Recover – Post Incident Review

Managed Service Lifecycle



Order Fulfillment Process:



Baseline inventory scanning and asset registration	Included
Baseline vulnerability environment scanning	Included
Baseline event correlation, tuning, and alarm trimming	Included
Basic threat dashboard and report creation	Advanced
SIEM tuning	Continuously
Vulnerability scanning	Weekly
Network IDS and endpoint monitoring	Included
Security Orchestration, Automation and Response (SOAR)	Included
SIEM Alarm monitoring and analysis	Included
Remediation guidance	Included

Supplemental Slides: MDR+MTI



MDR - Managed Detection & Response

MTI - Managed Threat Intelligence

MDR + MTI Custom

Solutions designed around AT&T Cybersecurity Unified Security Management (USM) Anywhere Platform



Managed Threat Intelligence Advanced Compliance & Analytics Package

MTI extends active log retention license (30-day/90-day), provides additional security oversight (monthly action dashboard and human analyst led reviews) and delivers advanced SIEM/SOC analytics geared towards IT compliance officers/auditors and stakeholders



Managed Threat Intelligence

Without visibility into attacks, threats and risks, it's impossible to measure, control and mitigate risk, capture return on investment, and continuously improve your program to drive positive business outcomes.

- **Asset and Risk Documentation, Tracking, Reporting**
- **Remediation & Resolution Tracking, Reporting**
- **Attack, Threat, Risk Trending, Remediation Reporting**
- **Audit Trail & Reporting for Compliance**
- **Advanced Oversight- Monthly Security Reviews Action Tracking Dashboard**

Through analysis, customized reporting, and actionable intelligence, Vertek helps companies advance their cyber-maturity, realize business value, and get to the next level.

Managed Service Lifecycle

Managed Threat Intelligence (MTI) Security Reviews

Review SIEM filtering, tuning activities, detection, protection and response activities, alarms flagged for review, follow up on action items from previous month, set new goals, discuss changes or noteworthy security concerns

Post-Incident

Preparation

Incident Response

We eliminate the noise and help you prioritize the threats that put your business at risk

Containment

Detection

Analysis

SOC Validation & Scanning

Log source validation, Alarm discussions, development/alignment of incident/response capabilities. Complete tuning/filtering activities with customer

Identify and Group Assets

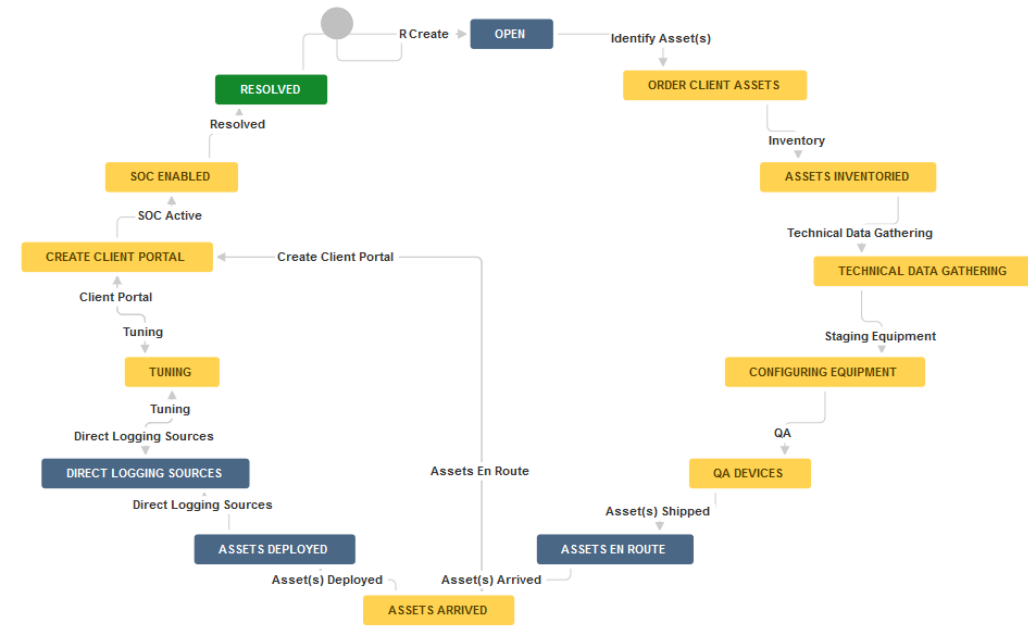
Identify assets, identify/integrate log capabilities, setup networks, asset groups, discuss key logging sources, policy requirements, understand unauthorized activity concerns, etc.

24x7 SOC Monitoring Detection & Response (MDR)

SIEM Alarm Monitoring, Active Threat Hunting, Human Alarm Triage and Remediation Guidance, System Lifecycle Checks, Security Orchestration, Automation and Response (SOAR) Capability Integration on a case-by-case basis.

www.vertek.com

Order Fulfillment Process:



MDR + MTI

Baseline inventory scanning and asset registration	Included
Baseline vulnerability environment scanning	Included
Baseline event correlation, tuning, and alarm trimming	Included
Basic threat dashboard and report creation	Advanced
SIEM tuning	Continuously
Vulnerability scanning	Weekly
Network IDS and endpoint monitoring	Included
Security Orchestration, Automation and Response (SOAR)	Included
SIEM Alarm monitoring and analysis	Included
Remediation guidance	Included
Lifecycle and compliance report management	Included
Service/Security review	Monthly

Managed Reports and Advanced Analytics



Tactical MONTHLY – Immediate Security Alarms Items and Action Tracking

- Inform management of relevant details, risks, current status and progress, tasks to be completed, and expected outcomes and dates – supporting regulatory compliance requirements, audits.

Client Dashboard

- Client Specific IR Playbook and Escalation Matrix
- RSS feeds related industry and Vertek OTX
- Request or Review Alarm or Platform Tickets
- System Maintenance Notifications
- Link to Report and Analytics

MDR

2018-01-24

- A New Report Dashboard is created each month
- Open action items are carried to the next month
- AlienVault and Vertek Reports are posted and reviewed each month

MTI

Client 6010

Alarm Analytics, Change Notifications, General Support Requests

- Open Alarms, Closed Alarms, and Alarms SOC flagged for Review
- Overall Alarm Deflection (e.g. SOC closed w/o engaging client)
- True Positives, False Positives, Trends, etc.

MDR

Client Portal

Monthly Incident & Action Dashboard

Monthly Alarm Status Report – Last 30 days



- A New Report Dashboard is created each month
- Open action items are carried to the next month
- AlienVault and Vertek Reports are posted and reviewed each month

SIEM UPDATES	ACTIONS, NOTES AND ITEMS FLAGGED FOR REVIEW
Alarms	<ul style="list-style-type: none"> • SOC-2011 - OTX Pulse Imagetrack • SOC-1994 - Web Server scanned for ShellShock • SOC-2957 - Spora OTX Pulse
Tuning	<ul style="list-style-type: none"> • Tuned noisy DNS request for Microsoft update services
Tasks	<ul style="list-style-type: none"> • Added HIDS agent for new client server
Maintenance	<ul style="list-style-type: none"> • Release 5.6 is in QA at this time.

REVIEW ITEMS		
<input checked="" type="checkbox"/> SIEM Updates	<input checked="" type="checkbox"/> AD Report	<input checked="" type="checkbox"/> Policy Violations
<input checked="" type="checkbox"/> SIEM Report	<input checked="" type="checkbox"/> Critical/High Vulnerabilities	<input checked="" type="checkbox"/> Monthly Maintenance
<input checked="" type="checkbox"/> SOC Report	<input checked="" type="checkbox"/> Change Management	<input checked="" type="checkbox"/> Service Enhancements

REPORT ATTACHMENTS	SCAN ATTACHMENTS	NON-MTI OPTIONAL
<input checked="" type="checkbox"/> SIEM Report <input checked="" type="checkbox"/> SOC Report <input checked="" type="checkbox"/> AD Report <input checked="" type="checkbox"/> Policy Report	<input type="checkbox"/> Vulnerability Scans <input type="checkbox"/> Q1 -March <input type="checkbox"/> Q2 -June <input type="checkbox"/> Q3 -September <input type="checkbox"/> Q4 -December	<input type="checkbox"/> Data Access Spot Check (U <input type="checkbox"/> Microsoft Patching Report <input type="checkbox"/> Linux Patching Report <input type="checkbox"/> AV/Malware Report <input type="checkbox"/> Monthly Patching / Maint

SECURITY CONCERNS, QUESTIONS AND NOTEWORTHY ITEMS

Notes and Existing Recommendations

- Clients access mail server over http with base64 encoded password
- Leverage group policy to implement a Domain Password Policy including password history, age, length, and complexity: [https://technet.microsoft.com/en-us/library/hh994571\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/hh994571(v=ws.10).aspx)
- Ensure tomcat facing web services are secured and hardened adequately. These links may be of interest: https://www.owasp.org/index.php/Securing_tomcat <https://tomcat.apache.org/tomcat-7.0-doc/security-howto.htm>

Current Critical Vulnerabilities

- DC still has critical remote code execution vulnerability, missing patch MS17-010
- Legacy OS with no support or patching available: (35+ 2003 and XP)

New/Follow-up Items

- Still hosting java application off domain controller on port :400. We strongly advise moving this and not putting your domain controller on the internet

Weekly Vulnerability Scanning Window

Scans start on Friday evening at 7PM and are staggered throughout the weekend. E grouped targets and start times:

- Cisco Devices - Friday 7PM
- Juniper Switches - Friday 8PM
- Brocade Devices - Friday 9PM
- PaloAlto Firewalls - Friday 10PM
- ESX Servers - Saturday 2AM
- Denver Vlan 50 - Saturday 4AM
- Seattle Vlan 50 - Saturday 8AM
- Dallas Colo Vlan 20 - Saturday 12PM
- New Jersey Vlan 50 - Saturday 4PM
- Boise Vlan 50 - Saturday 8PM

ACTION ITEMS
Vertek Tasks <ul style="list-style-type: none"> • Generate report on AV stats
Client Tasks <ul style="list-style-type: none"> • Provide list of new IP addresses • Enable Macro GPO • Enforce Password Policy
Vendor Tasks <ul style="list-style-type: none"> • TBD

SIEM HEALTH STATUS
<ul style="list-style-type: none"> • SIEM DB event retention: 60 days, unlimited events • Netflow retention: 45 days • Rawlog expiration: no • Alarm expiration: no • Avg EPS: 310 Low EPS: 221 High EPS: 591 • Total SIEM events for past 45 days: 266,906,623 events • Estimated events normalized per day: 5,931,258.28 • Events that exceed retention: 0 • Rawlogs received last month: 948,157,631 • Rawlogs space consumed last month: 214G /var/ossim/logs/2017/12/ • Netflow space consumed past 45 days: 86G

- ## MTI: Monthly Incident & Action Dashboard
- Discuss Outstanding and Important Alarms, Vulnerabilities
 - Provide Critical Prioritization and Remediation Guidance
 - Review Tuning and Maintenance Tickets
 - Provides SIEM Total Events and Statistics
 - Discuss Standard and Custom Reports
 - Track Current Deployment Status and Environmental Changes
 - Follow-Up on Network Changes and Critical Vulnerabilities
 - Generate and Track Action Items for Client and Vertek
 - Track Client Signoff on SIEM Filtering and Suppression

Detect Dashboard

Visualizations:

- [Detect: Alarms by Intent](#)
- [Detect: Alarms by architecture](#)
- [Detect: True pos, alarm trend](#)
- [Detect: True pos. alarms by Intent, time of day](#)
- [Detect: True pos. Strategies by time of day](#)
- [Detect: Alarms by plugin per month](#)
- [Detect: Alarms from 08:00-20:00 and weekdays](#)
- [Detect: Alarms 20:01-07:59 and weekends](#)
- [Detect: Top Destination Countries](#)
- [Detect: Top Destination Orgs](#)
- [Detect: Top Source Countries](#)
- [Detect: Top Source Orgs](#)
- [Detect: Top destination ports](#)
- [Detect: OTX categories by month](#)
- [Detect: True positive alarms](#)
- [Detect: False positive alarms](#)

Protect Dashboard

Visualizations:

- [Protect: Active vulnerable systems CVSS >= 9:](#)
- [Protect: Vulnerabilities where risk accepted:](#)
- [Protect: Vulnerabilities where risk mitigated:](#)
- [Protect: All vulnerabilities not remediated:](#)
- [Protect: Days to remediate by host:](#)
- [Protect: Tracking vulnerabilities first seen, by day:](#)
- [Protect: Active Critical Vulnerable Systems:](#)
- [Protect: Vulnerability drill-down:](#)
- [Protect: Change types trends, auto interval:](#)
- [Protect: Changes by type per month:](#)
- [Protect: Change types by action:](#)

Respond Dashboard

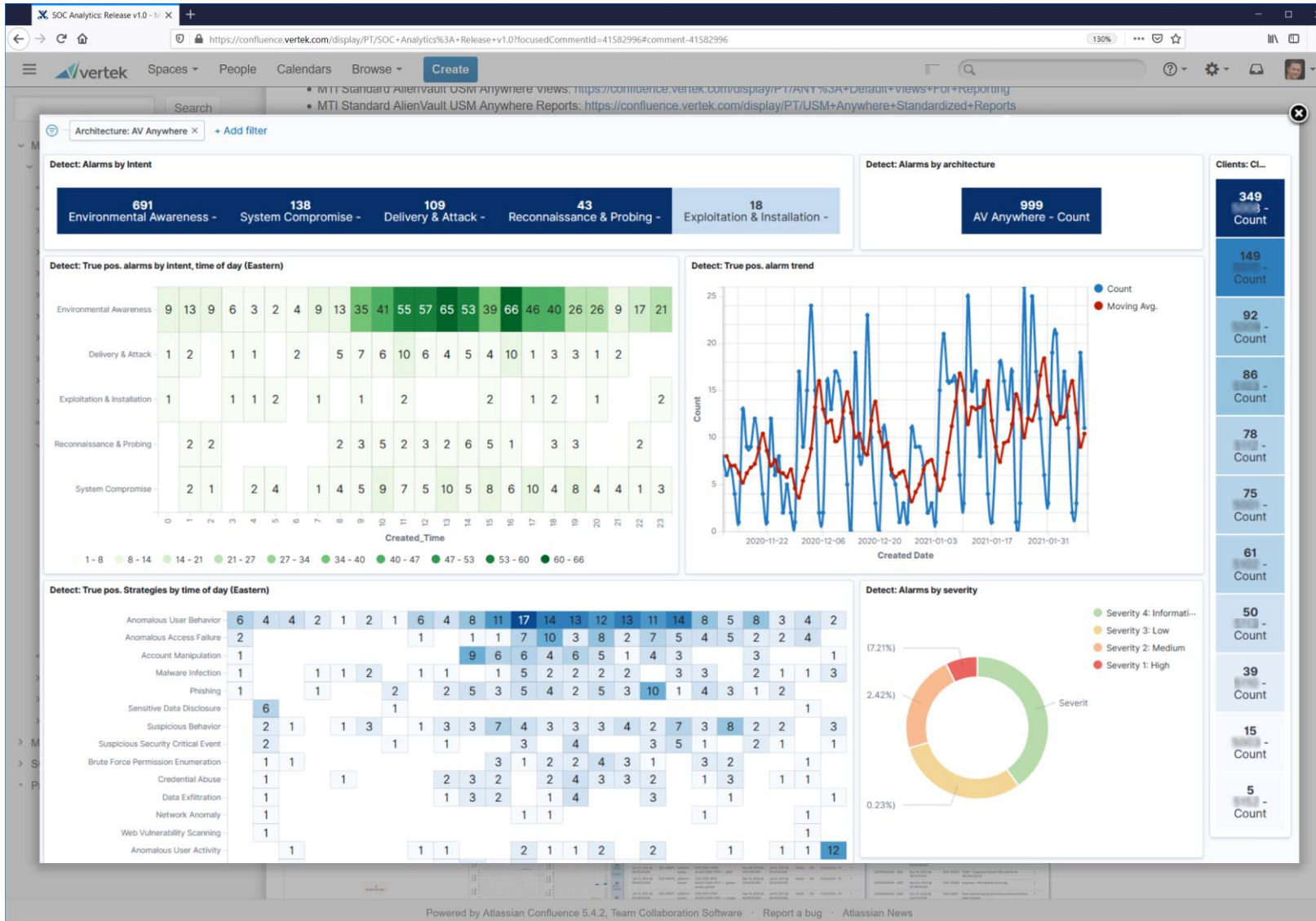
Visualizations:

- [Respond: Sev \(1s - 4s\): Avg. Pickup times:](#)
- [Respond: Deflection Percentage](#)
- [Respond: Avg. days to resolution by severity:](#)
- [Respond: Avg. days to resolution when communicating:](#)
- [Respond: Alarms communicated by month:](#)
- [Respond: Avg. days to resolve alarms, trend:](#)
- [Respond: Communicated alarms by method:](#)
- [Respond: Alarm counts, time spent, days to resolve:](#)
- [Respond: All worked alarms:](#)

Kibana Usage
Tutorial
[CLICK HERE](#)

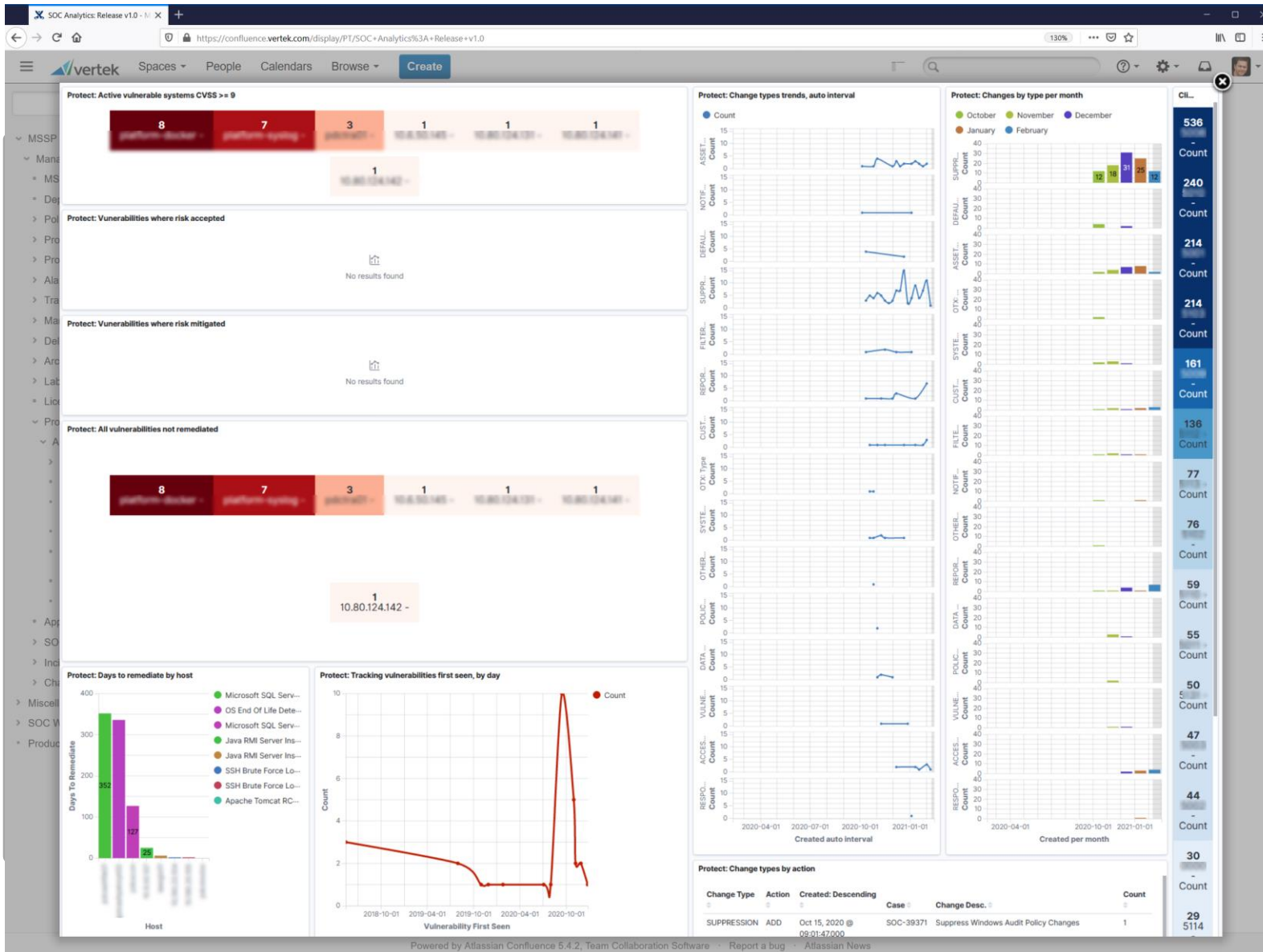
Dashboard User Guides
[CLICK HERE](#)

R1 Detect Dashboard Images



- [Detect: Alarms by Intent](#)
- [Detect: Alarms by architecture](#)
- [Detect: True pos, alarm trend](#)
- [Detect: True pos. alarms by Intent, time of day](#)
- [Detect: True pos.Strategies by time of day](#)
- [Detect: Alarms by plugin per month](#)
- [Detect: Alarms from 08:00-20:00 and weekdays](#)
- [Detect: Alarms 20:01-07:59 and weekends](#)
- [Detect: Top Destination Countries](#)
- [Detect: Top Destination Orgs](#)
- [Detect: Top Source Countries](#)
- [Detect: Top Source Orgs](#)
- [Detect: Top destination ports](#)
- [Detect: OTX categories by month](#)
- [Detect: True positive alarms](#)
- [Detect: False positive alarmsz](#)

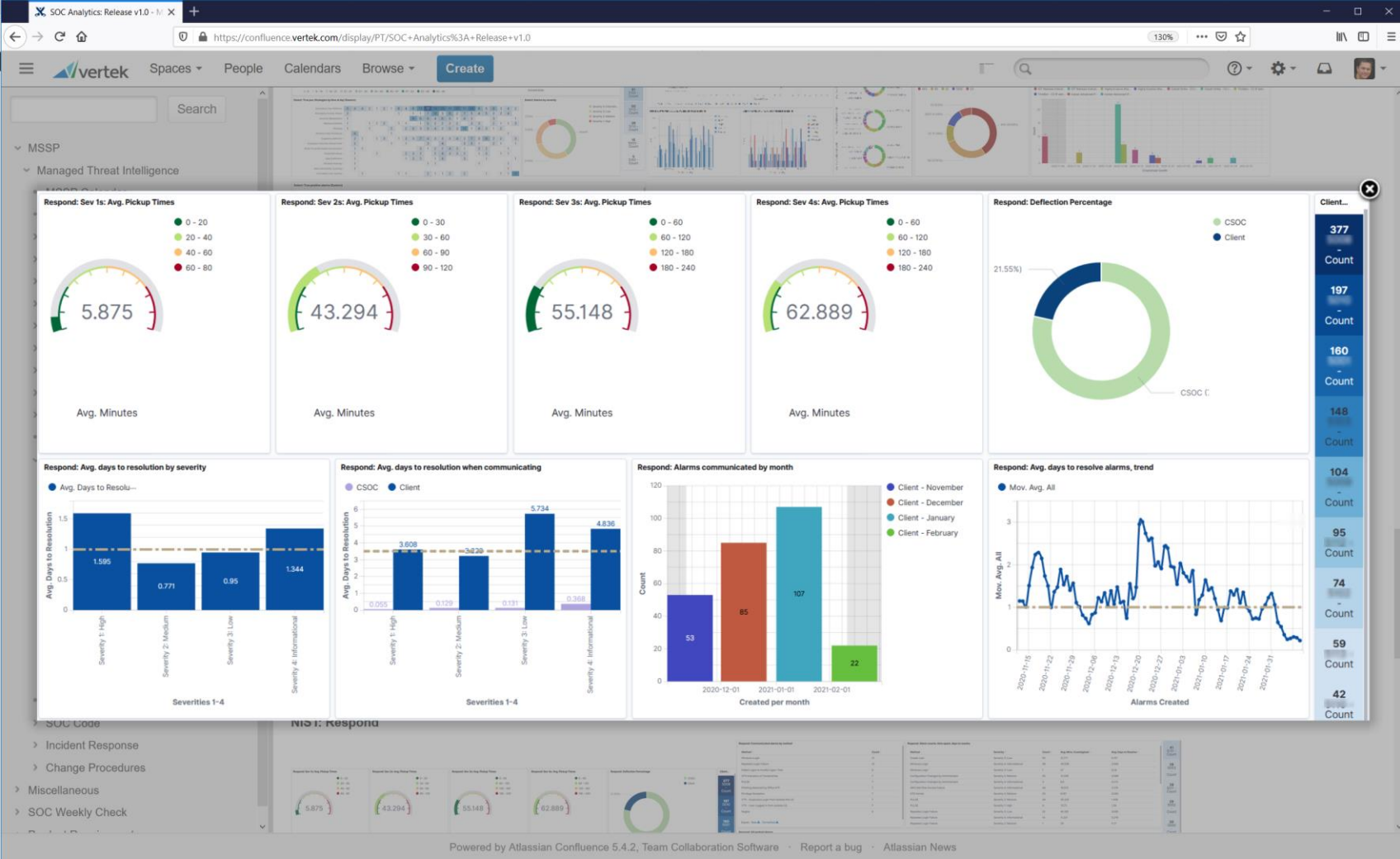
R1 Protect Dashboard Images



- [Protect: Active vulnerable systems CVSS >= 9:](#)
- [Protect: Vulnerabilities where risk accepted:](#)
- [Protect: Vulnerabilities where risk mitigated:](#)
- [Protect: All vulnerabilities not remediated:](#)
- [Protect: Days to remediate by host:](#)
- [Protect: Tracking vulnerabilities first seen, by day:](#)
- [Protect: Active Critical Vulnerable Systems:](#)
- [Protect: Vulnerability drill-down:](#)
- [Protect: Change types trends, auto interval:](#)
- [Protect: Changes by type per month:](#)
- [Protect: Change types by action:](#)

NOTE: Vulnerability data not possible across all SIEM deployments. Visualizations may be blank as a result.

R1 Respond Dashboard Images

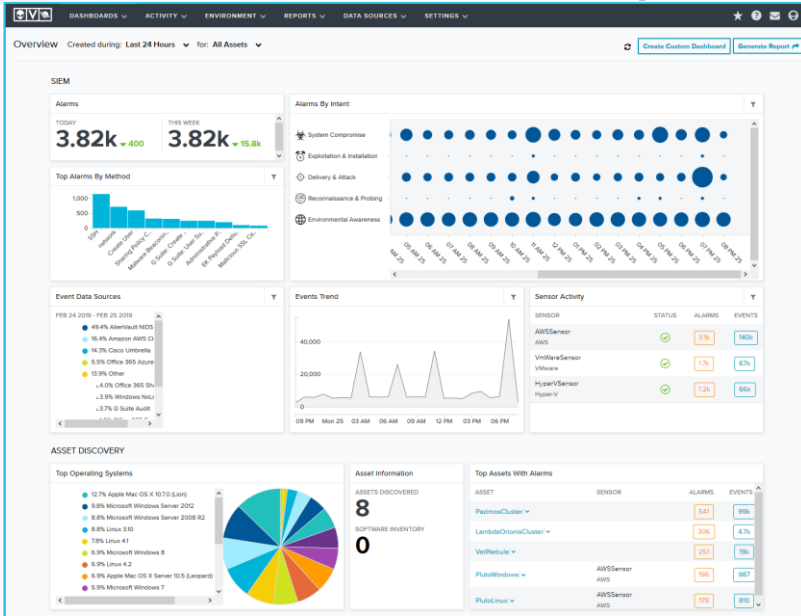


- [Response: Sev \(1s - 4s\): Avg. Pickup times:](#)
- [Response: Deflection Percentage](#)
- [Response: Avg. days to resolution by severity:](#)
- [Response: Avg. days to resolution when communicating:](#)
- [Response: Alarms communicated by month:](#)
- [Response: Avg. days to resolve alarms, trend:](#)
- [Response: Communicated alarms by method:](#)
- [Response: Alarm counts, time spent, days to resolve:](#)
- [Response: All worked alarms:](#)

Managed SIEM Reporting and Dashboards



AlienVault® USM™ Reports



SIEM Health and Real-Time Alarms and Metrics

- Asset Reports
- Alarm Reports
- Threat Reports
- Policy Reports
- Event Reports
- Security Technology Reports
- Vulnerability Reports

USM Dashboard Threat Visibility

Multiple integrated technologies to detect, correlate and present real-time alarms and analytics in a single pane of glass

Vertek MSSP Custom SIEM Report Views

Note: Views must be approved prior to usage during readouts. [Authorization of new views](#) must be approved by an Engineer or above.

View Index

- [Microsoft AD](#)
- [o365 Audit](#)
- [o365 Exchange](#)
- [o365 SharePoint](#)
- [Microsoft ATP](#)
- [Cisco](#)
- [FortiGate](#)
- [Palo Alto](#)
- [Dell SonicWall](#)
- [Skype](#)
- [Umbrella](#)
- [Linux](#)
- [MS Teams](#)
- [Vulnerable Java](#)
- [Team Viewer](#)
- [Google Talk](#)

View name (Share Filters)	Plugin REQ	Views Attributes	Event Columns	Approval Status	Approved By	Approved Date
VTK (AD) Local group changes	ALIENVAULT AGENT - WINDOWS EVENTLOG	Filter Attribs Collapse source 1 Data Source Plugin: AlienVault Agent - Windows EventLog 2 Event Name: A member was added to a security-enabled local group 3 A member was removed from a security-enabled local group 4 A security-enabled local group was changed	Event Columns Collapse source 1 Event Name 2 Time Created 3 Username 4 Security Group Name 5 Relative Distinguished Name	APPROVED	BHASKIN	2020-05-27
VTK (AD) Global group users added/removed	ALIENVAULT AGENT - WINDOWS EVENTLOG	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) Global group created-deleted	ALIENVAULT AGENT - WINDOWS EVENTLOG	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) User Added to Global Sec. Group	ALIENVAULT AGENT - WINDOWS EVENTLOG	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) Universal group users added/removed	ALIENVAULT AGENT - WINDOWS EVENTLOG	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) User Added to Local Sec Group	ALIENVAULT AGENT - WINDOWS EVENTLOG	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) User Removed From Local Sec Group	ALIENVAULT AGENT - WINDOWS EVENTLOG	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) User Removed From Global Sec Group	ALIENVAULT AGENT - WINDOWS EVENTLOG	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) A User Account Deleted	NONE	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) Windows Account Lockouts	NONE	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) Password Reset Invoked	NONE	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27
VTK (AD) Local group changes	WINDOWS NXLOG	Filter Attribs Expand source	Event Columns Expand source	APPROVED	BHASKIN	2020-05-27

MTI SOC Reports and Advanced Analytics

Improving Security Program Maturity



Organizations operating within or serving regulated industries need a cybersecurity program that (among other things):

- Inventories and correctly **classifies assets according to risk**
- **Identifies malicious entities probing systems and network**
- **Continuously monitors network traffic and system events** for potential unsecure behaviors
- **Responds to identified malicious events** to remediate them
- **Has the ability to audit and report effectiveness**

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Security Event Priority	Internal Response Time	Client Response Time
Severity 1: High. Anomalous / Suspicious events and activities that indicate an attack in progress. Exploitation and system compromise.	1 hour	2 hours
Severity 2: Medium. Anomalous / Suspicious events and activities that have occurred in succession or resemble an unauthorized attempt to access a system.	2 Support Hours	4 Support Hours
Severity 3: Low. Anomalous / Suspicious events and activities that alone might not constitute a major risk but should be monitored for repeat occurrences.	8 Support Hours	24 Support Hours
Severity 4: Informational. Security events and activities that should be brought to Client's attention that may or may not need to be dealt with to prevent future security events or incidents.	24 Support Hours	Informational only. Included in monthly report

- **24x7 SOC Coverage:** Service-generated alarms sent to Vertek Security Analyst, 365 days a year
- **12x5 SOC Coverage:** Service-generated alarms sent to Vertek Security Analyst, 8am to 8pm EST, Monday thru Friday, and excluding US national holidays
- **9x5 SOC Coverage:** Service-generated alarms sent to Vertek Security Analyst, 8am to 5pm EST, Monday thru Friday, and excluding US national holidays

Solution Deployment Models & Guidance



Vertek Security Operations Service Tier	Which Option is Right for Us?
<p>Managed Detection and Response (MDR)</p>	<p>Use Case: Our business may not have a formal cyber security program yet- could be on the list or in the early development stages, but we know our stakeholders want to limit risk to the business, protect the employees, our clients and our revenue streams. In order to do this, we know we need to increase our threat detection and response capabilities. We know from research, that it is too costly to develop in-house threat detection capabilities, evaluate/purchase tools, and/or manage dedicated security resources to effectively detect and respond to security threats or cyber attacks. We need to develop incident and response capabilities in days/weeks not months/years. <u>As a priority objective that we can build on</u>, we are looking for a <u>managed security vendor</u> to integrate and manage their own people, process and security tools to help our organization quickly detect and respond to daily/unknown threats on-premise, in the cloud or in our cloud applications we subscribe to.</p> <ul style="list-style-type: none"> • Target: Everyone • Why it works: Simple and cost-effective way to add essential enterprise managed detection and response capabilities • (\$\$) 15-day active logs for MDR purposes is recommended at this level • New program launch in 2021 • Can be upgraded at any point during the contract term or at renewal
<p>MDR + Managed Threat Intelligence (MTI)</p>	<p>Use Case: Our cyber security program or policy requires that we have advanced audit/logging, incident detection/response, vulnerability management, reports/analytics, etc. in place and the ability to demonstrate these capabilities. We need a <u>managed security partner</u> that has experience with clients that have well-established policy and compliance requirements. We are looking for a security partner to work as an extension of our IT and compliance team to help us improve our overall security posture and be a resource for security expertise and threat trends. We have the time to attend monthly security review meetings and we can make use of proprietary security dashboards, and advanced metrics/trending used to continuously measure and improve security operations.</p> <ul style="list-style-type: none"> • Target: Cyber Mature / Compliance Driven Customers • Why it works: Simple and cost-effective way to meet many compliance and security due-diligence requirements with a single service. Vertek's MTI program is guaranteed to provide value. • (\$\$) 30-day active logs for MTI purposes are required for reporting (*minimum tier once MTI is added) • (\$\$\$) 90-day may be required based on compliance requirements • Managed Threat Intelligence (MTI) service offering launched in 2015
<p>MDR + MTI Custom (RFI/RFP)</p>	<p>Use Case: My business is looking for a <u>managed security partner</u> that has the capabilities to <u>develop custom security solutions</u>, meet or comply with specific business or compliance requirements, or work with multiple vendors/partners. We need a solution partner that has a deep channel partner network, that can make key connections/introductions and bring solutions together from multiple partners and providers.</p> <ul style="list-style-type: none"> • (\$\$\$\$) Custom scope and pricing to completed • National channel management program launched in 2015



Ron Hruby | Vice President of Cybersecurity

(M) 802.598.9313

rhruby@vertek.com

Mark Dallmeier | Head of Channels

(M) 602.410.7793

mdallmeier@vertek.com

Sean McGovern | Channels Sales Manager

(M) 480.544.0830

smcgovern@vertek.com

Kristen Kennedy | Technical Account Manager

(M) 802.777.0513

kkennedy@vertek.com

www.Vertek.com/managed-cybersecurity/