

ConnectWise SIEM™ What's New?

Roopak Patel



IT NATION™ **SECURE**

Agenda

- Announcements review
- Key capabilities and benefits
- Call to action
 - Keynote
 - Sessions
 - Main booth—multiple stations

Top SIEM Deliverables

- Themes and continuous innovations
- Specific announcements (SaaS, Retention, ECS Rules)
- Detailed list
 - New dashboards (EDR & IDS)
 - Azure rulesets
 - SaaS v2 (separate training)
 - SOC value report
 - SIEM 3.0 themes
 - True retention
 - ECS
 - Sharp MFP offer
- Next steps



New EDR + IDS Dashboards

- Shows value of combining high fidelity alert information
- Targeted to assist with investigations as initial use case
- Stepping-stone for our broader XDR framework

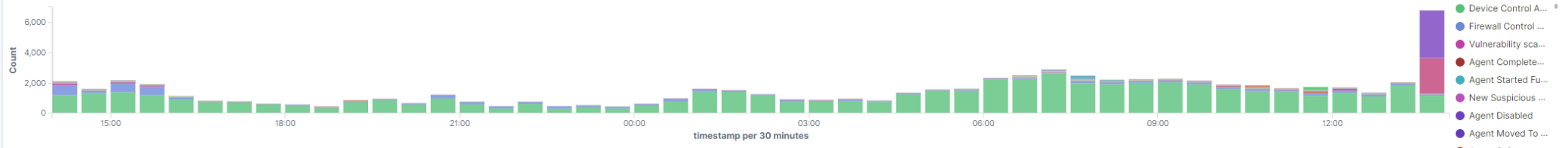


EDR & SIEM Summary



SIEM + IDS + MDR
Security Dashboard

Sentinel One Alerts



Sentinel One New Threats

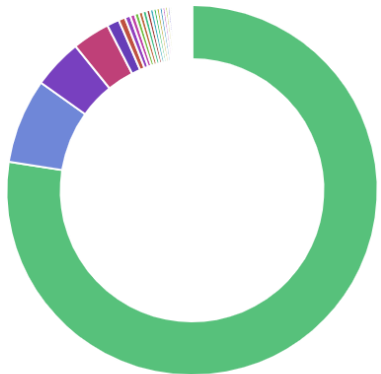


- Malware
- Application Control
- PUA
- Rootkit
- Generic.Heuristic

S1 New Threats

Threat	IP	File Path	Hash	Process Arguments	Count
Malware	192.168.147.240		-install-2.4.4-1601.exe	N/A	1
Malware	10.11.12.191	p_util_sh.py	f6eaa99a9f56213bf59e193598e02a253852983f	"/usr/bin/python3 /opt/tall/_local_setup_util_sh.py sh"	3
Malware	10.11.12.191	h.py	f6eaa99a9f56213bf59e193598e02a253852983f	"/usr/bin/python3 /opt/tall/_local_setup_util_sh.py sh"	3
Malware	192.168.140.89	h.py	f6eaa99a9f56213bf59e193598e02a253852983f	"/usr/bin/python3 /opt/tall/_local_setup_util_sh.py sh"	2
Malware	192.168.140.89	la4bbe8d8772968f000b8dc8335ac760/merged/var/lib/dpkg/info/libpam-	99971876c953dae147ad34752f44ab6abd3e1284	"/bin/sh /var/lib/dpkg/info/libpam-systemd:amd64.prerm upgrade 249.11-0ubuntu3.9"	1
Malware	192.168.140.89	3cae361ef419816b8861c87e3302dbb/merged/var/lib/dpkg/info/libc6:amd64.postrm	7383eefa9630f02987705c577f63319ce2bcf5ca	"/bin/sh /var/lib/dpkg/info/libc6:amd64.postrm upgrade 2.27-3ubuntu1.6"	1
Malware	192.168.140.89	_sh.py	f6eaa99a9f56213bf59e193598e02a253852983f	"/usr/bin/python3 /opt/tall/_local_setup_util_sh.py sh"	1
Malware	172.16.4.47		013812680-3567710555-188991\$R6A8E3K.Ink	a68769ce65d27d65d39f23ae0b7247063db36136	1

Sentinel One Activity



- Device Control A...
- Firewall Control ...
- User Reconnect...
- Agent Reconnect...
- Agent Moved To ...
- Agent Software ...
- Agent updated
- Vulnerability sca...
- Agent subscribed
- Agent Decommis...
- Threat Incident S...
- Agent Complete...
- Agent Started Fu...
- Tag Manager - U...
- Scan Initiated
- User Requested ...
- New Suspicious ...
- Threat Mitigation...

IDS Alerts

Indicator	Source IP	Destination IP	Count
[ConnectWise CRU] Plaintext Login for IMAP 143	174.196.134.14	192.168.113	1
[ConnectWise CRU] Plaintext Login for IMAP 143	195.219.98.44	192.168.11.72	1
ET POLICY Anonymous LDAPv3 Bind Request Outbound	10.20.1.247	98.158.162.101	278
ET POLICY Anonymous LDAPv3 Bind Request Outbound	10.241.0.97	151.193.104.131	6
ET POLICY Anonymous LDAPv3 Bind Request Outbound	10.241.0.97	151.193.108.131	2
ET POLICY Anonymous LDAPv3 Bind Request Outbound	192.168.165.16	214.23.240.177	1
ET POLICY DNS Query to .onion proxy domain (.pet)	192.168.0.100	8.8.8.8	181
ET POLICY DNS Query to .onion proxy domain (.pet)	192.168.0.100	8.8.4.4	102
ET MALWARE Windows qwinsta Microsoft Windows DOS prompt command exit OUTBOUND	192.168.100.49	103.36.248.79	280
ET MALWARE Windows route Microsoft Windows DOS prompt command exit OUTBOUND	192.168.100.49	103.36.248.79	280

Export: [Raw](#) [Formatted](#)

EDR & IDS Threat Details



SIEM + IDS + MDR
Security Dashboard

Sentinel One New Threats



S1 New Threats

Threat	IP	File Path
Malware	10.10.1.137	
Malware	10.10.1.137	
Malware	10.10.1.137	
Malware	10.10.1.137	
Malware	10.10.1.137	
Malware	10.10.1.137	

File Path	Hash	Process Arguments	Count
Vinfrarecorder_964.exe	841c8eec4c2fe2240b85d23c8f37581e9253126e	N/A	2
ids(CouponPrinterCPS (1).exe	ae197ca540c814e1f9a311be6db37af534efd0ad	N/A	2
...j\fonts\ZipV1c.exe	2b90dc9a28d9cc94c0f064d39ce7a01a92b73ce	N/A	1
...ori\Adobe Acrobat 7.0 Professional - Keygen by PARADOX 2004.exe	ee2dd7a7db919336df9d2cce6a0d529939455889	N/A	1
Converter Full\Crack\CrackCopyMeToInstallDirAndRun.exe	743073d2a6fdaba0f2e0bd175470619132ea84f	N/A	1
ids(CouponPrinterCPS (2).exe	ae197ca540c814e1f9a311be6db37af534efd0ad	N/A	1

Sentinel One New Threats Details

Time	agentDetails.lastIpToMgmt	agentDetails.computerName	threatDetails.classification	threatDetails.filePath	primaryDescription	threatDetails.fileContentHash	data.escapedMaliciousProcessArguments
> Apr 24, 2023 @ 13:38:38.495	10.10.1.137		Malware		\Quarantine(C:\Program Files)\MyPC Backup\MyPC Backup.exe.vir	182d4dcb2c2f31e7d971ac4456f4a1be22fa6a1	-
> Apr 24, 2023 @ 02:23:20.089	10.10.1.137		Malware		Total Video Converter Full\Crack\CrackCopyMeToInstallDirAndRun.exe	743073d2a6fdaba0f2e0bd175470619132ea84f	-

IDS Alerts

Indicator	Source IP	Destination IP	Count
ET MALWARE Antibody Software Installed (PUA)	10.10.1.137	104.156.52.74	1

Export: [Raw](#) [Formatted](#)

Windows Least Common Process Command Line

Least Common Process Command Line	Count
/N /P --UseSystemFonts /Q:15	1
-i -cDir ASMedia_USB_Controller -o 5KBB7_temp.xml	1
-i -cDir ASMedia_USB_Controller -o CRNYQ_temp.xml	1
-i -cDir ASMedia_USB_Controller -o DZMOX_temp.xml	1
-i -cDir ASMedia_USB_Controller -o IC3J7_temp.xml	1
-i -cDir ASMedia_USB_Controller -o UC184_temp.xml	1
-i -cDir RLtek_Ethernate -o 5KBB7_temp.xml	1
-i -cDir RLtek_Ethernate -o CRNYQ_temp.xml	1
-i -cDir RLtek_Ethernate -o DZMOX_temp.xml	1
-i -cDir RLtek_Ethernate -o IC3J7_temp.xml	1

Easily View Azure Alert and Activity Sources

Top Users

Azure Top UserID

Export

UserId.keyword: De...	Count
app@sharepoint	38,626
Unknown	11,598
NOT-FOUND	6,106
System	4,161
	3,757
	2,915
	2,667
	2,187
	2,031

< 1 2 3 4 5 ... 500 >

Top Workload

Azure Top Workload

Export

Workload.keywor...	Count
OneDrive	93,256
SharePoint	73,825
Exchange	71,302
AzureActiveDirectory	26,000
CRM	17,037
MicrosoftTeams	16,989
Endpoint	10,354
SecurityCompliance...	6,399
CompliancePosture...	4,161

< 1 2 3 >

Top Operations

Azure Top Operations

Export

Operation: Descending	Count
FilePreviewed	24,537
FileAccessed	21,503
MailItemsAccessed	19,584
CrmDefaultActivity	17,037

Export

geoiip.country_...	Count
United States	237,916
Canada	11,464
India	4,428
United Kingdom	3,739
Ireland	2,462
France	1,906
China	1,898

5 ... 24 >

SaaS Security Essentials

Problem

- Few security products provide low cost, “essentials only” monitoring solutions
- Most solutions are “full SIEM”—hard to configure, expensive, and require SOC management
- Need “essential” SaaS monitoring to ensure critical incidents are investigated and mitigated

ConnectWise Solution

- Features “self-service” SaaS security monitoring
- Leverages expertise of security professionals
- Offers advanced threat detection and pre-curated alerting rules from the CRU
- Reduces staffing or infrastructure investments
- Includes mitigation and investigation recommendations via knowledge base

SaaS v2: Access SaaS Security Essentials in Asio™

The screenshot shows a web browser window displaying the 'Security Overview Module' of the Community Healthcare Network. The browser's address bar shows the URL: `control.qa.itsupport247.net/QADashB/QuickAccess/NewDesktops/overview?SSECTION=junoPortal&STAB=597&SLINK=53616c7465...`. The page features a dark sidebar on the left with a navigation menu. The main content area is white and contains several informational cards.

Community Healthcare Network

Chat Support Resources

Service Delivery

Devices

Automation

OS Patching

Alert Management

Reporting

Communicator

Security

- Overview
- Profiles
- Activation
- Vulnerability Mgmt
- Assessment
- Reports
- SaaS Security

Learn More >

Learn More >

ConnectWise SOC Services

Provide 24/7 threat monitoring and response backed by ConnectWise SOC experts.

ConnectWise Cybersecurity Operation Center is working as an extension of your team, with our certified security analysts, cutting-edge threat intelligence, and our latest solutions to manage all your security monitoring, 24/7.

Learn More >

ConnectWise Incident Response

24/7 security experts on tap to address critical security incidents for you and your clients.

Cybersecurity attacks are overwhelming and stressful, especially if you are short on bandwidth and cybersecurity expertise. You can have peace of mind with our team of security experts who are here to help you and your clients through critical security incidents with 24/7 support.

Learn More >

CW SaaS Security Essentials

SaaS Application Security Monitoring

Produces notifications to help your organization identify potential threats or vulnerabilities within your cloud-based SaaS applications. It provides recommendations on how to remediate these issues and offers visibility into user access, activity, and data usage to detect anomalous behavior. The service is designed to identify and address security issues, reducing the risk of a security incident.

Learn More >

SaaS v2: Activate SaaS Clients in Asio

The screenshot shows the ConnectWise SaaS Security dashboard. A modal dialog box titled "Activate Site" is centered on the screen, asking for confirmation to activate the site "Arti ATX". The background dashboard includes a sidebar menu, a breadcrumb trail "Security / SaaS Security", and a table of configured applications.

Activate Site

Confirm the site activation!
Are you sure to activate site **Arti ATX**?

Company Name	Critical	High	Medium	Low	Score	Status	Active Rules
Arti ATX	-	-	-	-	-	Activate Site	-
Foxprompt	-	-	-	-	-	Activate Site	-
Dynamic	-	-	-	-	-	Activate Site	-

SaaS v2: Add New Alerting Integrations in Asio

The screenshot displays the ConnectWise SaaS Security interface. A modal window titled "Install Applications" is open, showing the configuration for Microsoft Office 365. The dialog includes a list of SaaS vendors, an "Authorize" button, and a configuration toggle for "Enable log collection".

CONNECTWISE

Security / SaaS Security

SaaS Security

Total Applications

Install Applications

SaaS Security: Install Applications
Follow the instructions provided by the SaaS Security to set up and configure the applications to receive alerts.

Select SaaS vendor(s)...

- Microsoft Office 365 Not Installed
- Google Workspace Not Installed
- Duo Not Installed
- Okta Not Installed

It may take up to 24 hours for Microsoft to configure the tenant after authorization, during which testing and ingesting may fail. For more about our integration with Office 365 and how to get set up, check out the [Office 365 ConnectWise help page](#). Office 365 audit logs must be enabled to use this feature.

Authorize

Authorized-tenant: b9jski92ed02-ham38vb920-nks729gf02

Configuration Enable log collection

Close **Submit**

No Available Data
Looks like there is no data to show you right now.

Status	Active Rules
● Site Activated	-
Activate Site	-
Activate Site	-

Rows per page: **✓ Site activation request successfully submitted.**

SaaS v2

Individual Alerts Detail View

Alert: Login Alert (detected on April 1, 2023 10:15 AM)

Login Alert CRITICAL

Detected on April 1, 2023 10:15 AM • Microsoft Office 365

Description:
This security alert is to inform you that we have detected suspicious activity on your Google Workspace account. This could indicate an unauthorized attempt to access your data or email.

Alert Details	
Title	Value
User ID	user@domain.com
IP Address	341.82.12.342
Date and time	December 16, 2022 - 6:03 am EDT
Location	Brazil (-1.269339, -60.428029)
Activity Type	Login Failure
Device or Application used	Mac
Source IP address	342.82.12.213
Destination IP address	222.82.12.103
File path used	C:\Windows
Result (of the activity)	Failure

Review Status

Investigation

Close Submit

Security Alerts Client Overview

CONNECTWISE

Security / SaaS Security

SaaS Security

Total Applications Configured: 45

- Microsoft 365 - 15
- Duo - 10
- Okta - 10
- Google - 10

Open Alerts

- 175 Critical
- 56 Medium
- 34 Info

Company Name	Critical	Medium	Info	Applications configured	Status	Active Rules
Arti ATX 1 New	55	78	17	Microsoft Office 365, Duo, Okta	Site Activated	2
Foxprompt	34	45	87	Microsoft Office 365, Duo, Okta, Google	Site Activated	2
Dynamic	63	34	12	Microsoft Office 365, Duo, Okta, Google	Site Activated	2
ZenSec	23	54	97	Duo, Okta, Google	Site Activated	2
WebInfo	85	97	64	Microsoft Office 365, Okta, Google	Site Activated	2
CAS Sec	98	86	57	Okta, Google	Site Activated	2
WebInfo	85	97	64	Microsoft Office 365, Duo	Site Activated	2
WebInfo	85	97	64	Microsoft 365, Duo, Okta, Google	Site Activated	2

Rows per page: 25 | 1 - 10 of 10

Active Security Alerts Client View

CONNECTWISE

SaaS Security / Arti ATX

Company: Arti ATX

Alerts Applications Configured Rules

False Positive

Alerts per Application: 45

- Microsoft 365 - 15
- Duo - 10
- Okta - 10
- Google - 10

Open Alerts

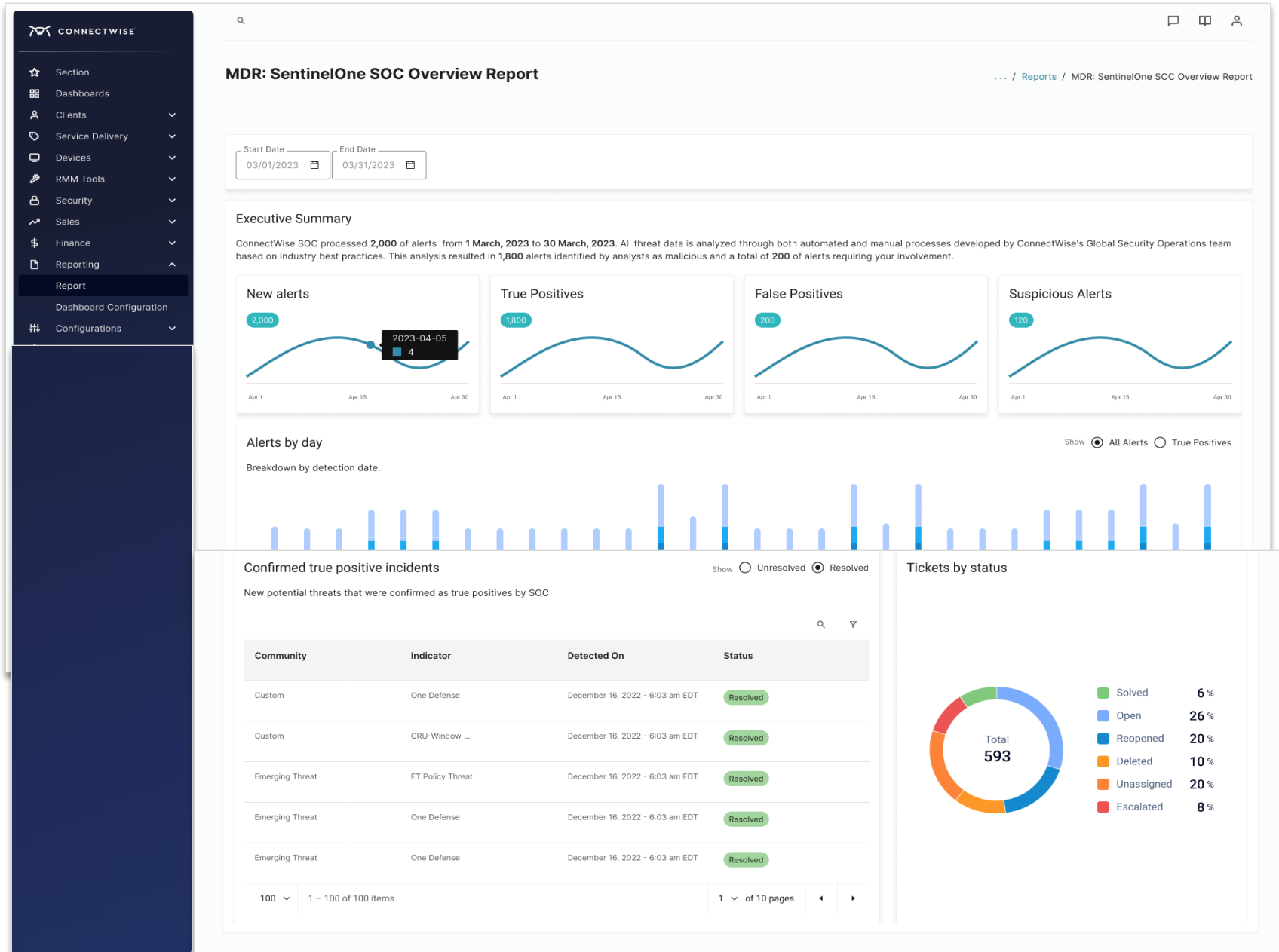
- 175 Critical
- 56 Medium
- 34 Info

Alert	Description	Application	Severity	Detected On	Review Status	Action
<input checked="" type="checkbox"/>	Login Alert	Login Alert details XYZ	Microsoft Office 365	CRITICAL	December 16, 2022 - 6:03 am EDT	Pending Send Alert
<input checked="" type="checkbox"/>	Unusual Traveling	Lorem Ipsum	Okta	MEDIUM	December 16, 2022 - 6:03 am EDT	Investigation Send Alert
<input checked="" type="checkbox"/>	Failed Login Attempt	Lorem Ipsum	Microsoft Office 365	INFO	December 16, 2022 - 6:03 am EDT	Escalated Send Alert
<input checked="" type="checkbox"/>	Unusual Login	Lorem Ipsum	Google	INFO	December 16, 2022 - 6:03 am EDT	Closed Send Alert
<input checked="" type="checkbox"/>	XYZ Alert	Lorem Ipsum	Microsoft Office 365	MEDIUM	December 16, 2022 - 6:03 am EDT	Closed Send Alert

Rows per page: 25 | 1 - 10 of 10

ConnectWise SOC Services™ Value

- Displays alerts breakdown for the past month—new, true, and false positives and suspicious alerts
- Details investigated alerts with ticket handling and status at month's end



Sharp MFP Monitoring Offer Details

What is it?	What is the commercial offer?	What are the scenarios?	How do end users benefit?
<ul style="list-style-type: none">• Network-enabled MFPs monitored using ConnectWise SIEM.• Tracks activity and reviews device logs to identify security risks.• Requires installation of a dedicated LogShipper.	<ul style="list-style-type: none">• Standalone SKU with special price per IP: \$4/device with 30-day retention (default).• Existing partners: Targeted for orgs that have not purchased ConnectWise SIEM SKUs.• New partners: Entry point for becoming ConnectWise partner.• Orgs can upgrade to regular SIEM SKUs for broader monitoring (including Sharp).• SOC monitoring included for designated Sharp MFPs in stand-alone SKU.	<ul style="list-style-type: none">• Net-new partner: Does not have SIEM—can get Sharp-only SIEM.• SHARP-SKU assigned to the org. Org not usage-billed but on contracted number of printers at \$4/device.• Existing partner: Can add Sharp devices and pay under existing usage guidelines (user or IP).• An org can have either SKU, not both.• Partners started on SHARP-SKU can upgrade to full SIEM and become a regular SIEM user. SKU replaced with upgraded SKU(s).	<ul style="list-style-type: none">• Expanded usage of simple, easy-to-deploy monitoring at scale.• Immediate value and coverage for unprotected devices.• Starting point of a broader security conversation for many partners.

SIEM 3.0 Rollout Plan

The 5 things

- 1 True retention
- 2 ECS rollout practical rollout
- 3 Content set based on ECS
- 4 Download capability for cold storage
- 5 SaaS v2, Phase 2

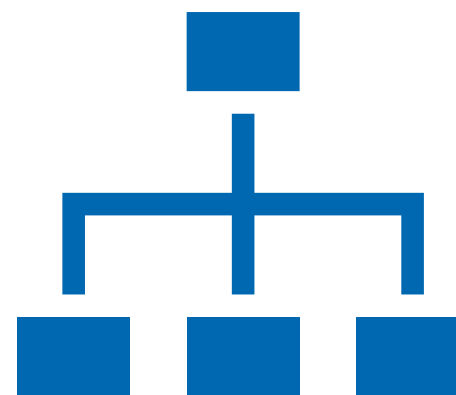
True Retention

- Partners pay for certain level of retention periods and expect to be able to search across that time frame
- True retention will allow partners to search the retention period that they've paid for (with certain performance constraints)
- Search period to cover—30 days (default) to 12 months (upgrade)



ECS Common Schema

- Normalized data is easier to leverage
- Advanced correlation, simpler search capability, and vendor agnostic
- Categorization groups set of events by categories for type of behavior being monitored
- Easier and more efficient correlation (used in rules creation) and better understanding of alerts



ECS Data Normalization

Events	Cisco	Checkpoint	Palo Alto
RAW	May 16 2023 10:24:53: %ASA-4-106023: Deny tcp src outside:203.0.113.45/54893 dst inside:192.168.0.100/80 by access-group "outside_access_in" [0x0,0x0]	2023-05-16T10:24:53+00:00 firewall1 CEF:0 CheckPoint VPN-1 & FireWall-1 R80.40 Accept 190 src=203.0.113.45 dst=192.168.0.100 spt=54893 dpt=80 proto=tcp rule=outside_access_in	2023-05-16T10:24:53+00:00 firewall1 CEF:0 CheckPoint VPN-1 & FireWall-1 R80.40 Accept 190 src=203.0.113.45 dst=192.168.0.100 spt=54893 dpt=80 proto=tcp rule=outside_access_in
Normalized	"timestamp": "2023-05-16T10:24:53", "severity": "Informational", "source_ip": "203.0.113.45", "source_port": 54893, "destination_ip": "192.168.0.100", "destination_port": 80, "protocol": "tcp", "action": "Deny", "access_group": "outside_access_in", "event_id": "ASA-4-106023"	"timestamp": "2023-05-16T10:24:53", "device_vendor": "CheckPoint", "device_product": "VPN-1 & FireWall-1", "device_version": "R80.40", "action": "Accept", "event_id": "190", "source_ip": "203.0.113.45", "destination_ip": "192.168.0.100", "source_port": 54893, "destination_port": 80, "protocol": "tcp", "rule_name": "outside_access_in"	"timestamp": "2023-05-16T10:24:53", "device_vendor": "CheckPoint", "device_product": "VPN-1 & FireWall-1", "device_version": "R80.40", "action": "Accept", "event_id": "190", "source_ip": "203.0.113.45", "destination_ip": "192.168.0.100", "source_port": 54893, "destination_port": 80, "protocol": "tcp", "rule_name": "outside_access_in"

ECS Event Categorization

The natural grouping of events based on the behavior or activity being reported

Category:

Authentication Failures

- Incorrect Password
- Expired User Account
- Account Lockout
- Failed Multi-Factor Authentication (MFA)
- Suspicious Login Pattern
- Account Disabled



Category:

Brute Force Attack

- Multiple Failed Login Attempts
- Account Lockout
- Rapid Login Attempts
- Password Guessing
- Credential Stuffing
- Brute Force on Service



Category:

Malicious Detections

- Exploit Attempt
- Malware Detection
- Command and Control (C2) Communication
- Data Exfiltration
- Insider Threat: Description
- Account Compromise



Complex rule created with minimal effort



Practical usage

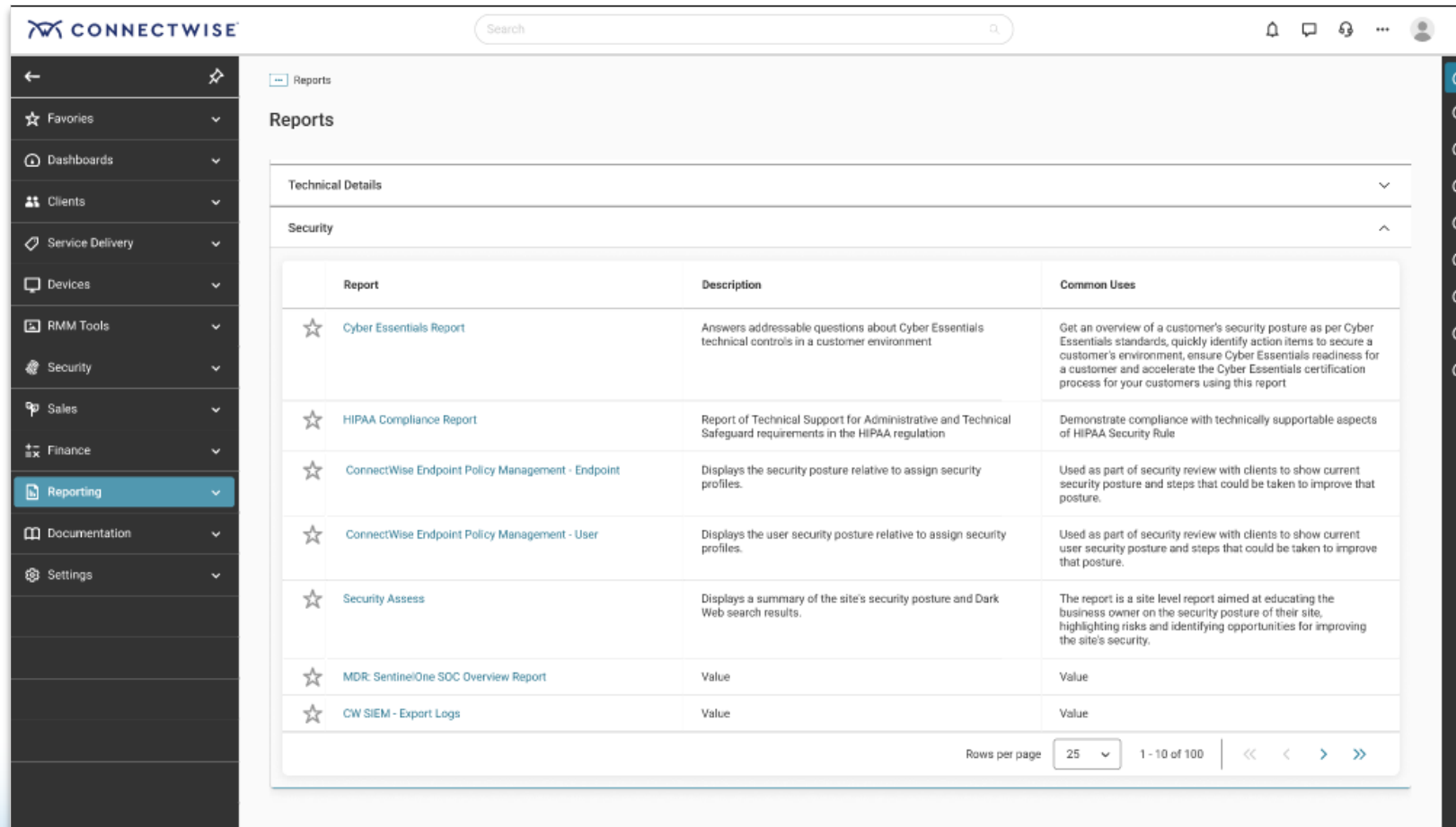
Instead of searching for individual events in lists, set up a rule to search for the event category.



Benefits

Easier rule setup • Granular detection without noise • Category groups enable complex detection

Retention and Download from Asio



The screenshot displays the ConnectWise interface, specifically the Reports section. The left sidebar contains navigation options such as Favorites, Dashboards, Clients, Service Delivery, Devices, RMM Tools, Security, Sales, Finance, Reporting (highlighted), Documentation, and Settings. The main content area is titled 'Reports' and features a table with columns for Report, Description, and Common Uses. The table lists several reports, including Cyber Essentials Report, HIPAA Compliance Report, and ConnectWise Endpoint Policy Management reports. At the bottom right of the table, there is a pagination control showing 'Rows per page' set to 25 and '1 - 10 of 100'.

Report	Description	Common Uses
★ Cyber Essentials Report	Answers addressable questions about Cyber Essentials technical controls in a customer environment	Get an overview of a customer's security posture as per Cyber Essentials standards, quickly identify action items to secure a customer's environment, ensure Cyber Essentials readiness for a customer and accelerate the Cyber Essentials certification process for your customers using this report
★ HIPAA Compliance Report	Report of Technical Support for Administrative and Technical Safeguard requirements in the HIPAA regulation	Demonstrate compliance with technically supportable aspects of HIPAA Security Rule
★ ConnectWise Endpoint Policy Management - Endpoint	Displays the security posture relative to assign security profiles.	Used as part of security review with clients to show current security posture and steps that could be taken to improve that posture.
★ ConnectWise Endpoint Policy Management - User	Displays the user security posture relative to assign security profiles.	Used as part of security review with clients to show current user security posture and steps that could be taken to improve that posture.
★ Security Assess	Displays a summary of the site's security posture and Dark Web search results.	The report is a site level report aimed at educating the business owner on the security posture of their site, highlighting risks and identifying opportunities for improving the site's security.
★ MDR- SentinelOne SOC Overview Report	Value	Value
★ CW SIEM - Export Logs	Value	Value

Call to Action

ConnectWise Keynote

- June 5, 5:00pm
- Patrick Beggs, Jason Magee, Raffael Marty, Peter Melby

General Sessions

- SIEM v3.0—Today & Future Roadmap, June 6, 10:30am
- SaaS Security—You Can't Ignore That Your Data Lives in the Cloud, So What Are We Going to Do? June 6, 4:15pm
- The Hidden Powers of Combining Network and Endpoint Detection, June 7, 1:30pm
- Simply SIEM, June 7, 2:35pm

Focus Groups

June 5

- SaaS Security and Security Essentials Products, 4:00pm

June 6

- Understanding XDR and How It Affects You, 2:00pm

June 7

- Hero Type Reports (Value driven reports) in ConnectWise SIEM, 10:30am

BACKUP

ECS In Action: Checkpoint Mapped

```
`<6> Apr 1 15:47:21 firewall1 authd[3235]: id=12345 login successful for user john.doe`
```



```
{  
  "timestamp": "2023-05-01T15:47:21.000Z",  
  "firewall": "firewall1",  
  "service": "authd",  
  "event_id": 12345,  
  "event_type": "login_successful",  
  "user": "john.doe"  
}
```

Example of normalized data for a log entry in Checkpoint FW showing a user's successful authentication.

```
`<4> Apr 1 15:49:08 firewall1 kernel: [fw4_2];DROP packet received (in=eth1.1003 out=eth2.1001)`
```



```
{  
  "timestamp": "2023-05-01T15:49:08.000Z",  
  "firewall": "firewall1",  
  "interface_in": "eth1.1003",  
  "interface_out": "eth2.1001",  
  "event_type": "packet_dropped"  
}
```

Example of normalized data for a log entry in Checkpoint FW following a blocked connection attempt.

ECS In Action: Cisco ASA Mapped

```
`%ASA-6-113005: AAA user authentication Successful : user = john.doe`
```



```
{  
  "timestamp": "2023-05-01T00:00:00.000Z", // Assuming that the timestamp  
  "firewall": "ASA",  
  "event_id": null, // Event ID is not provided in this log entry  
  "event_type": "vpn_auth_successful",  
  "user": "john.doe"  
}
```

Example of normalized data for a log entry in Cisco ASA showing a successful VPN connection.

```
`%ASA-4-106023: Deny tcp src inside:192.168.1.2/52435 dst outside:8.8.8.8/80  
by access-group "outside_access_in" [0x0, 0x0]`
```



```
{  
  "timestamp": "2023-05-01T00:00:00.000Z", // Assuming that the timestamp  
  "firewall": "ASA",  
  "event_id": null, // Event ID is not provided in this log entry  
  "event_type": "packet_dropped",  
  "protocol": "tcp",  
  "src_ip": "192.168.1.2",  
  "src_port": 52435,  
  "dst_ip": "8.8.8.8",  
  "dst_port": 80,  
  "rule_name": "outside_access_in"  
}
```

Example of normalized data for a log entry in Cisco ASA showing a dropped packet due to an ACL.

ECS In Action: Palo Alto Mapped

```
`May 1 10:23:45 firewall1 1,2023/05/01 10:23:45,007100001,USER-  
ID,INFO,AuthdUser(1),User authentication successful, johndoe@acme.com`
```



```
{  
  "timestamp": "2023-05-01T10:23:45.000Z",  
  "firewall": "firewall1",  
  "event_id": 1,  
  "event_type": "user_auth_successful",  
  "user": "johndoe@acme.com"  
}
```

Example of normalized data for a log entry in Palo Alto showing a user's successful authentication.

```
`May 1 11:23:45 firewall1 1,2023/05/01 11:23:45,007200001,THREAT,INFO,Threat-  
ID 12345, Attack detected and blocked, src 192.168.1.2, dst 8.8.8.8`
```



```
{  
  "timestamp": "2023-05-01T11:23:45.000Z",  
  "firewall": "firewall1",  
  "event_id": "007200001",  
  "event_type": "threat_detected_and_blocked",  
  "threat_id": 12345,  
  "src_ip": "192.168.1.2",  
  "dst_ip": "8.8.8.8"  
}
```

Example of normalized data for a log entry in Palo Alto showing a threat detected and blocked.