

FORTINET®

Can't Code? No Problem

Dylan Spille – CSE DevOps

James Huber – Sr Director CSE

XPERTS
SUMMIT 2023

Helping you
create a digitally
secure future.

Security Operations Challenges

Keeping pace with attack volume and sophistication



- **Evasive attacks:** Sophisticated multi-stage campaigns evade prevention security require detailed alert investigations
- **Alert volume:** Alerts and manual tasks can inundate staff, delaying or even hindering critical investigation & response
- **Siloed security tools:** Investigations span multiple tools with no central point of control. SIEM may lack depth and automation.
- **Limited budgets:** Adding headcount is difficult, costly and not a viable long-term solution.

Unacceptable risk

SOC teams have difficulty to keep pace with I&R and proactive measures. The risk of serious breach is high.



FortiSOAR



**Centralize, standardize & automate
IT/OT security operations**

Connect anything – automate everything

500+ integrations, 800+ playbooks, robust use-case solutions for SOC/NOC/OT

Security incident response

Automated triage, enrichment, investigation, case mgmt, collaboration, and response actions

Threat Intelligence management

Powered by FortiGuard Labs and any public source

Asset and vulnerability mgmt

IT/OT risk-based tracking and remediation playbooks

No/low-code playbook creation

Patented development modes for any user and workflow

- Overall Leader in KuppingerCole 2023 SOAR Leadership Compass



XPERTS 2023

FortiSOAR Customer Profiles

Over 300 enterprise, public sector and service provider customers worldwide



Financial Services

Top 5 institutions in 10 countries



Energy

8 top producers/distributors
#1 O&G producer worldwide



Healthcare

Largest US Healthcare insurer
Largest US Healthcare provider



Telecom

Over 10 major providers
5 of top 20 worldwide providers



Government

Over 20 institutions in 15 countries



Managed Security Services

Over 15 major MSSPs worldwide
4 of top 20 worldwide providers



Technology & Software

Top Telecom provider
Top CAD/CAM provider



Manufacturing

Top 5 automaker
Top 5 electronics maker





Core Features

Automation across your entire ecosystem

500+ integrations & Solution Packs with multi-vendor products



"The champion product when it comes to automation and having the ability to maximize existing tools"



XPERTS 2023

- KuppingerCole Leadership Compass for SOAR, 2023

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

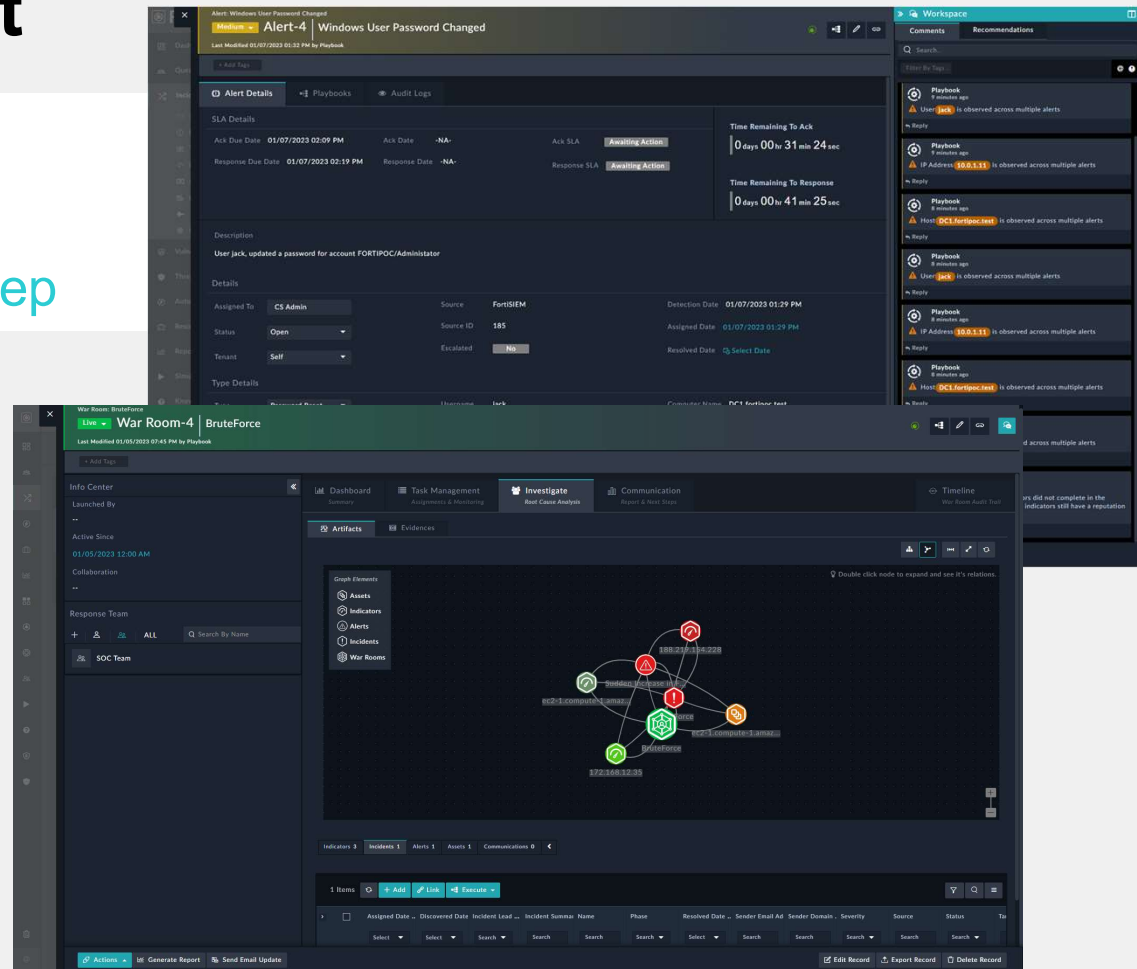
Incident Management

Automatically process alerts

Investigate & respond to incidents

Leverage AI & automation at every step

- Robust **case management** experience
- ML-driven **playbook recommendations**
- **MITRE ATT&CK** mappings
- **War Room**: collaboration, task mgmt, forensics-level logging
- **Workforce/Ops management** - tasks, work queues, shifts; SLA tracking
- **Role-based access** and capabilities



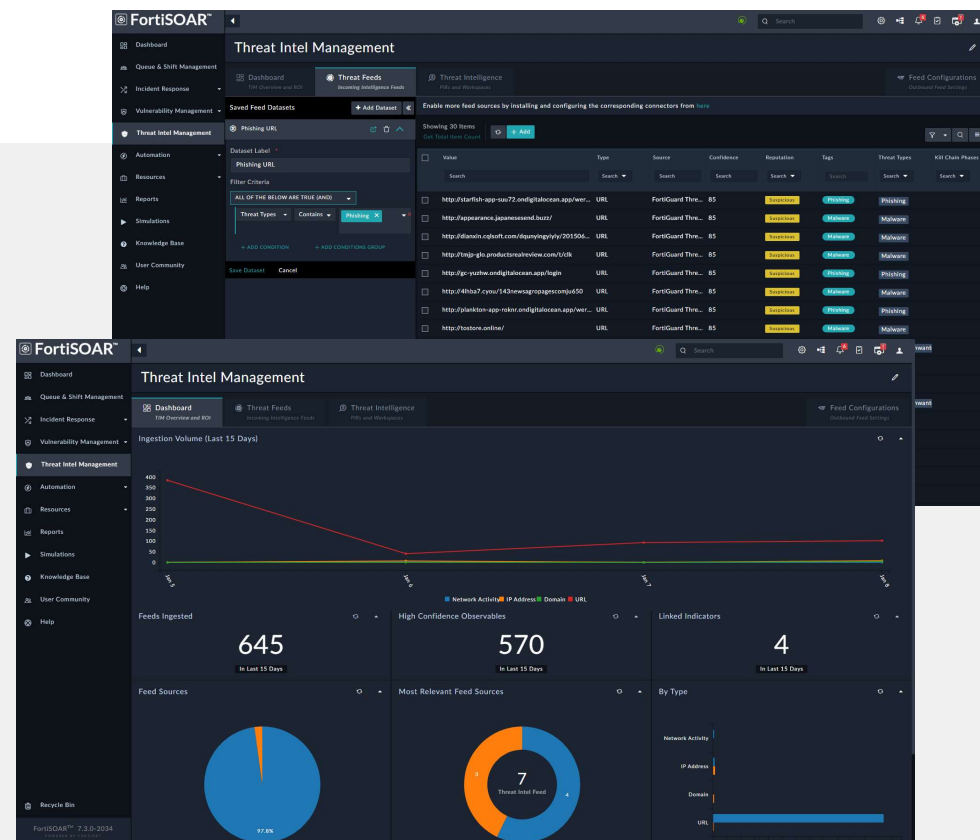
Threat Intelligence Management

Fully manage and curate threat intel from Fortinet and any source

Automatically enrich threat investigations

Research and respond to intel requests

- Built-in **FortiGuard** intel feeds
- Supports virtually **any feed source**
- **TIM engine** aggregates, normalizes, curates, and and risk-scores all feeds
- **IOC export** via STIX and TAXII
- **TIM workspace** facilitates threat research, collaboration and sharing
- **Intel request ticketing** and assignment

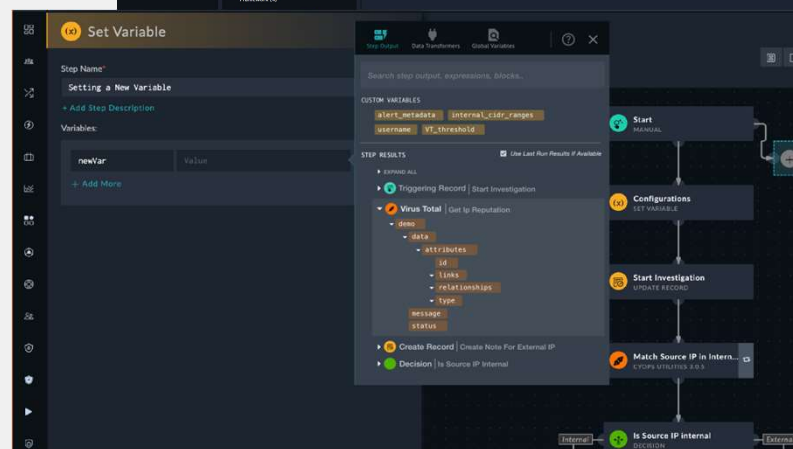
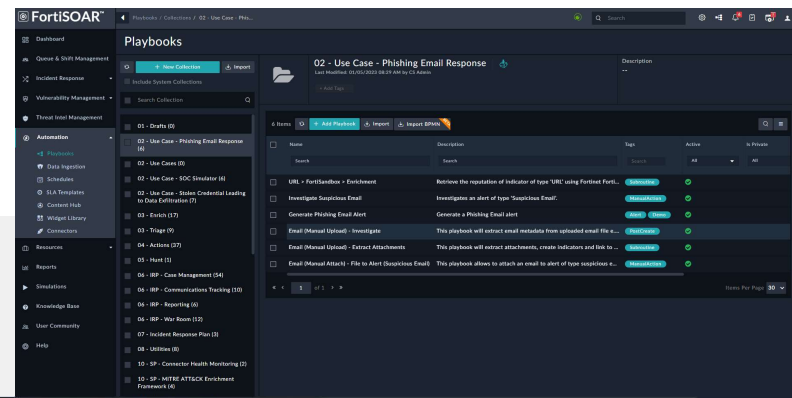


XPERTS 2023

Playbook Creation

Create playbooks and new connectors with ease
Leverage no/low code GUI & recommendations
Simulate and test before deploying

- **Patented designer** provides drag/drop, native language, and python options
- **Pre-built playbooks & action library** speed design
- **Recommendation engine** for stepwise guidance
- **Reference Blocks** give contextual aid, samples
- **Full CI/CD process** support with source control
- **Simulation tools** ensure successful deployment



Vulnerability Management

Centralize & automate IT/OT vulnerability management

Enrich & speed threat investigation with integrated vuln. intelligence

- 2-way scanner integration playbooks
- Risk-based asset vulnerability views
- Standardized alerting & task mgmt
- Patch / mitigation playbooks
- Enriched threat investigation intel

Dashboard displays include:

- Total critical vulnerabilities
- Assets with critical vulnerabilities
- Trends by severity, top 10 vulnerable assets
- Scan history

The screenshot shows the 'Alert-121' details page in the Fortinet Vulnerability Management interface. The alert is titled 'Asset cs-win-12 found at risk' and is classified as 'High'. It was last modified on 01/17/2023 at 02:17 PM by a playbook. The interface includes tabs for 'Alert Details', 'Playbooks', and 'Audit Logs'. Under 'Alert Details', there are sections for 'SLA Details' and 'Description'. The 'SLA Details' section shows 'Ack Due Date' as 01/17/2023 02:37 PM, 'Ack Date' as -NA-, 'Ack SLA' as 'Awaiting Action', 'Response Due Date' as 01/17/2023 02:47 PM, 'Response Date' as -NA-, and 'Response SLA' as 'Awaiting Action'. On the right, there are two timers: 'Time Remaining To Ack' at 0 days 00 hr 19 min 22 sec and 'Time Remaining To Response' at 0 days 00 hr 29 min 22 sec. The 'Description' section contains a 'Vulnerability Details' table with 4 rows. The first row is highlighted with a red box. Below the table is a 'Details' section with fields for 'Assigned To' (CS Admin), 'Status' (Open), 'Tenant' (Self), 'Source' (--), 'Source ID' (273941a2-7142-11ed-b6f2-acde48001122), 'Escalated' (No), 'Detection Date' (01/17/2023 02:17 PM), 'Assigned Date' (01/17/2023 02:17 PM), and 'Resolved Date' (Select Date).

Sr. No.	ID	Name	Severity	Link
1	96391	MS17-002: Security Update for Microsoft Office (3214291)	High	Click Here
2	121247	Oracle VM VirtualBox 5.2.x < 5.2.24 / 6.0.x < 6.0.2 (Jan 2019 CPU)	Medium	Click Here
3	118801	Zoom Client for Meetings Installed (Windows)	Minimal	Click Here
4	118095	Microsoft SQL Server Management Studio (SSMS) Installed	Minimal	Click Here



XPERTS 2023

Asset Visibility & Risk Management

View and track IT/OT asset inventory and complete asset security status
Enrich and prioritize threat investigation activities

- Asset criticality and risk-based alert & vulnerability views
- Flexible view alignments including OT Purdue model
- Asset mgmt system 2-way integrations

Dashboard displays include:

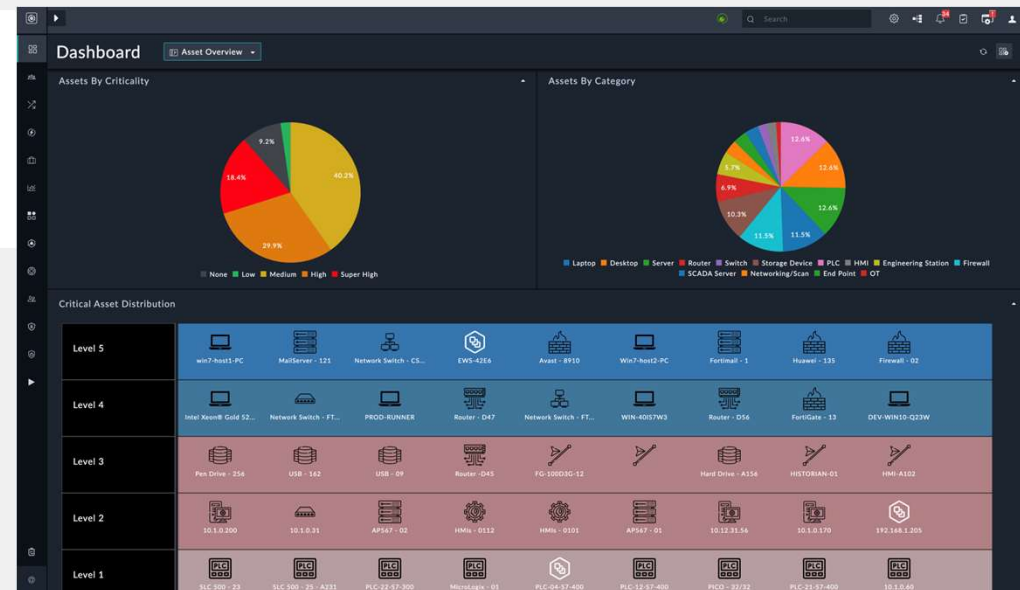
- Asset criticality, alert & vulnerability status
- Alerts by asset, by zone, by asset class
- MITRE IT/OT ATT&CK views



FortiSOAR for OT

Monitor OT assets and risk levels
Respond immediately to OT alerts
Protect OT assets from outside attack

- Integrated OT security & ecosystem products
- OT threat intel feeds and management
- Unified IT/OT workflows with MITRE ATT&CK ICS mapping
- Complete asset & risk views w/Purdue Model
- OT-specific remediation playbooks



Microsoft Sentinel

Integrations across multi-vendor IT/OT security products and OT specialty solutions

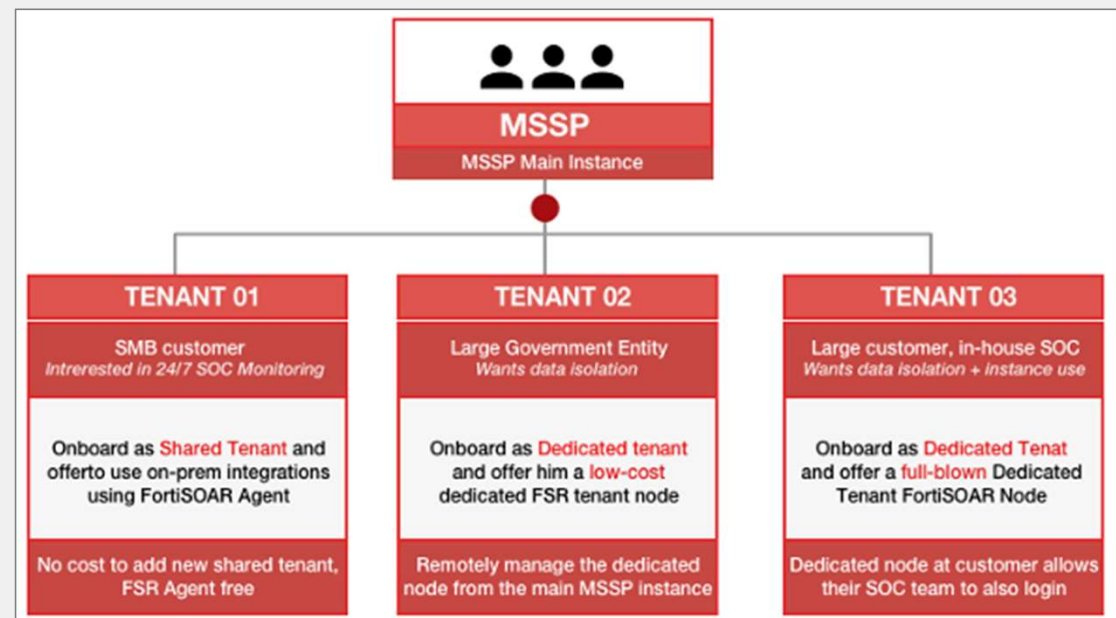
The background is a solid blue color. On the left side, there is a faint, light blue geometric pattern consisting of a square with rounded corners and a line that curves around it. In the bottom left corner, there is a grid of small, light blue dots. On the right side, there are several large, overlapping triangles in various shades of blue and teal, creating a dynamic, abstract design.

What's in it for me?

MSSP Design Features

Support any customer environment with flexible deployment & management features

- Supports hierarchical single and multi-tenant modes
- On-prem agent & full instance options
- Playbook masters auto-translate to tenant specifications
- Tenant-specific alerting, dashboards
- Proven scalability; High Availability configuration support
- Secure exchange layer eliminates VPN



Choose a central or distributed SOC architecture Leverage FortiCloud managed hosting services
Or deploy as SW in your data center or cloud

MSSP Use Cases

Shared, Hybrid and Dedicated Tenant Flavours

No SIEM, No SOAR

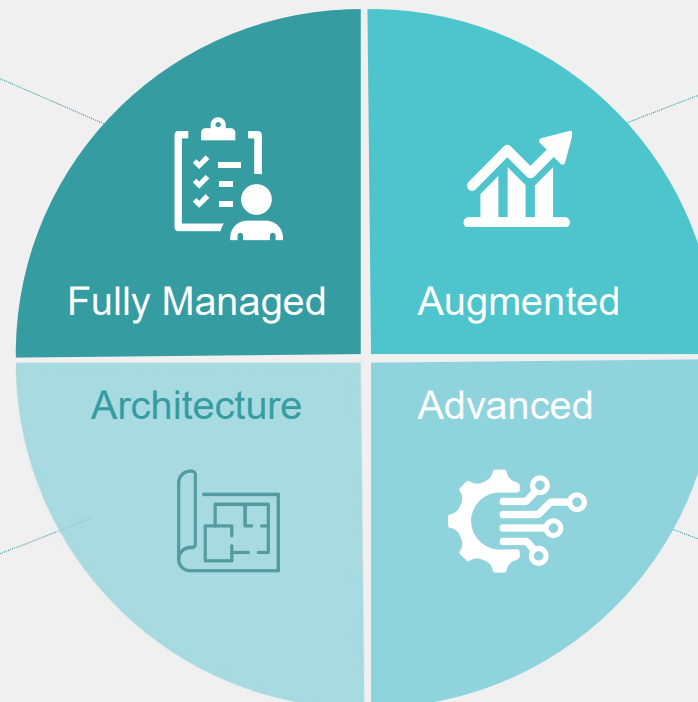
Offer Your Portfolio – Detection to Response
Custom Response and SLA for each Tenant
Host tenant on Master SOAR (**no cost increase**)

Has SIEM, Needs SOAR

Offer your **Response Services** and expand to Fully Managed Services Portfolio
Optionally Deploy FortiSOAR (on Premise) – Chargeable
Augment in Response Remotely using Master SOAR

Salient Features

Remotely Manage (without VPN)
Highly Configurable and Extensible
Highly Integrated (~500 Connectors)
Highly Scalable
MSSP Friendly Licensing



Has SIEM, Has SOAR

Offer your **Incident Response Services** and expand to Augmentation
Augment **3rd Party SOAR** through Manager SOAR – Monitoring as well as Response
Leverage **Integrated Crisis Management**



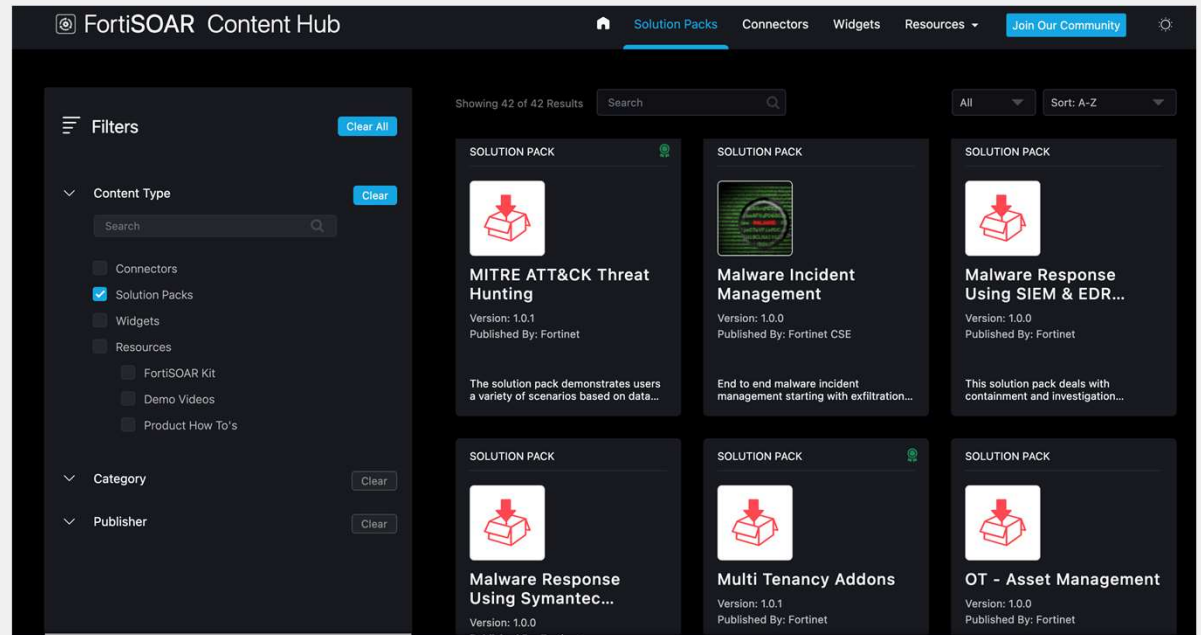
Content Hub and Community

Access ready-made content, demos and how-to videos

Interact with peers and Fortinet experts

- 500+ connectors
- 800+ playbooks
- 30+ solution packs
- Video tutorials and demos
- Community insights
- In-product and web access

fortisoar.contenthub.fortinet.com





FORTINET®

