FORTINET

XPERTS
SUMMIT 2023

Helping you create a digitally secure future.

Can’t Code? No Problem

Dylan Spille – CSE DevOps

James Huber – Sr Director CSE

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

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"

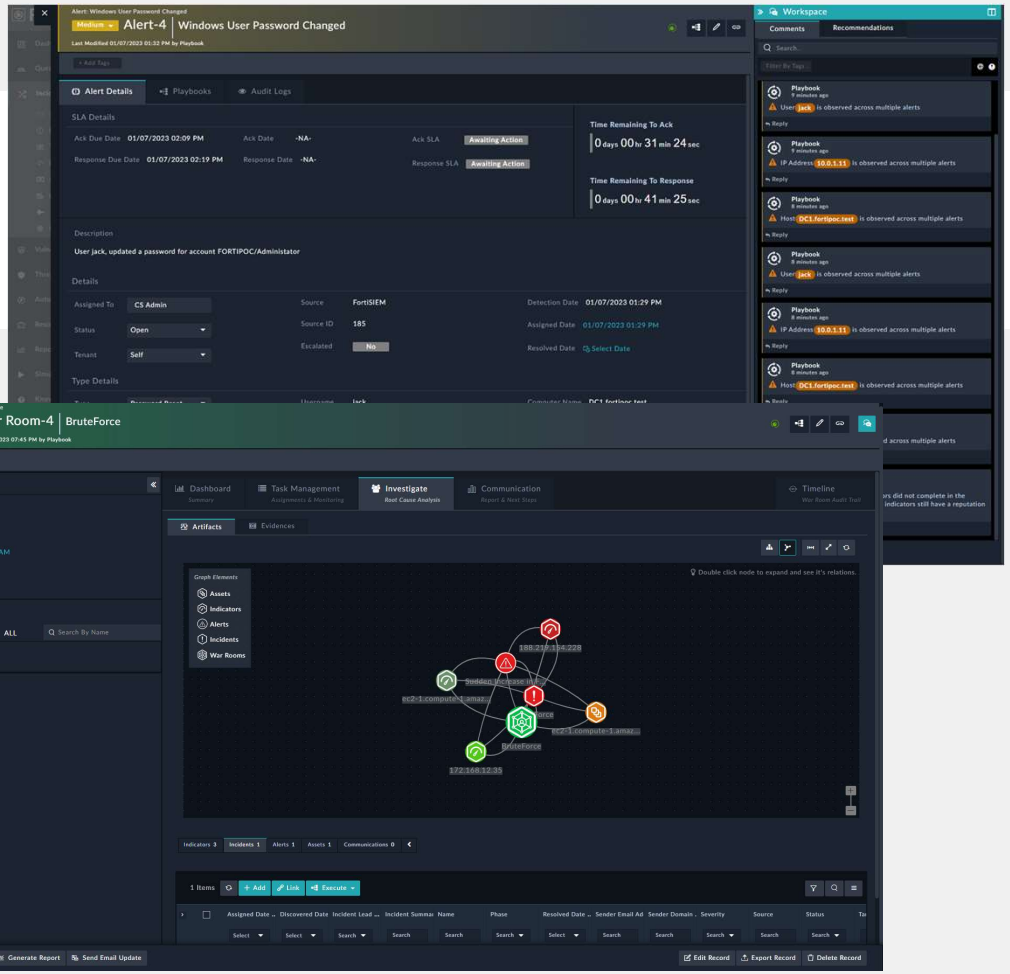
- KuppingerCole Leadership Compass for SOAR, 2023

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

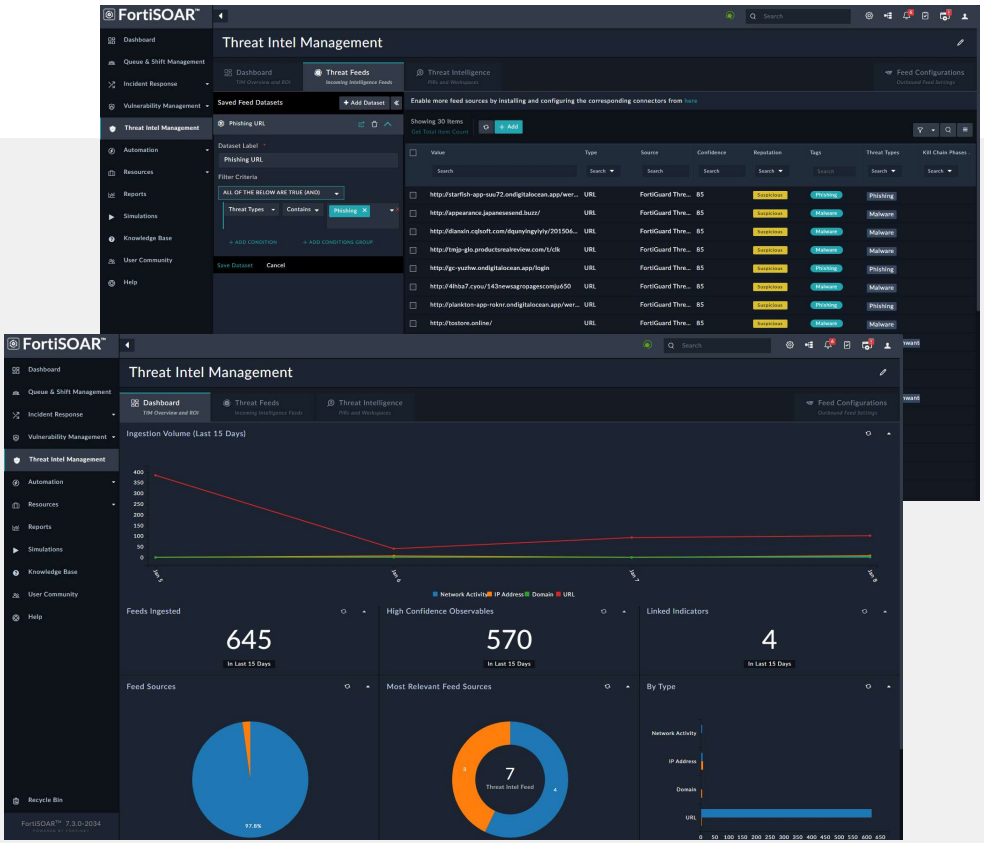
Threat Intelligence Management

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

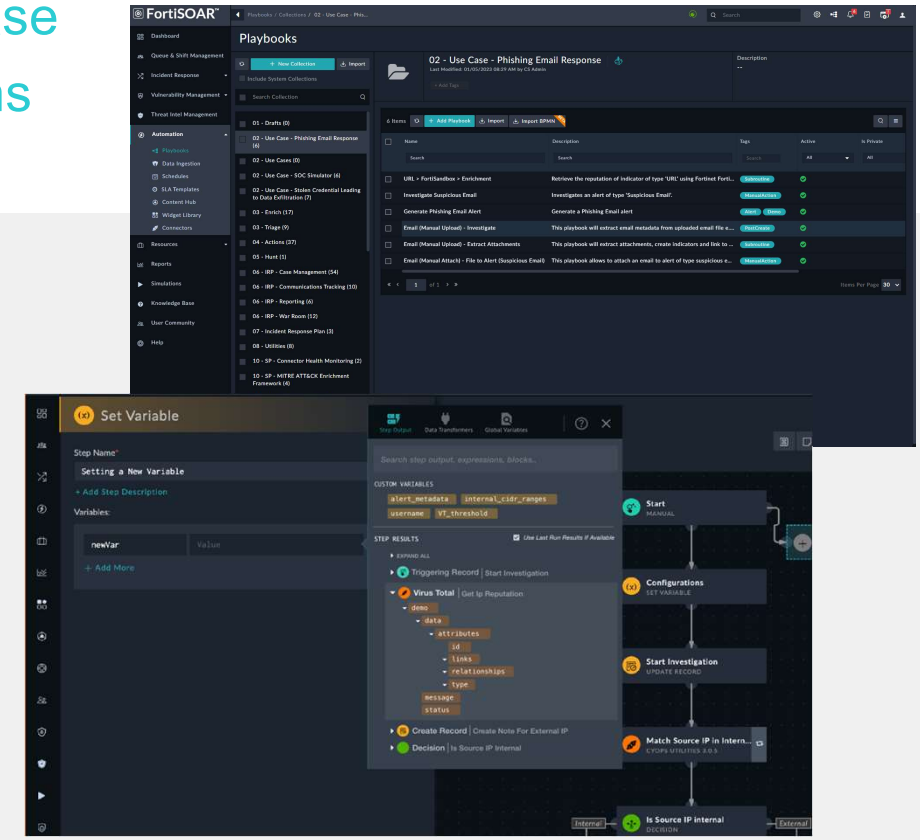


Playbook Creation

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

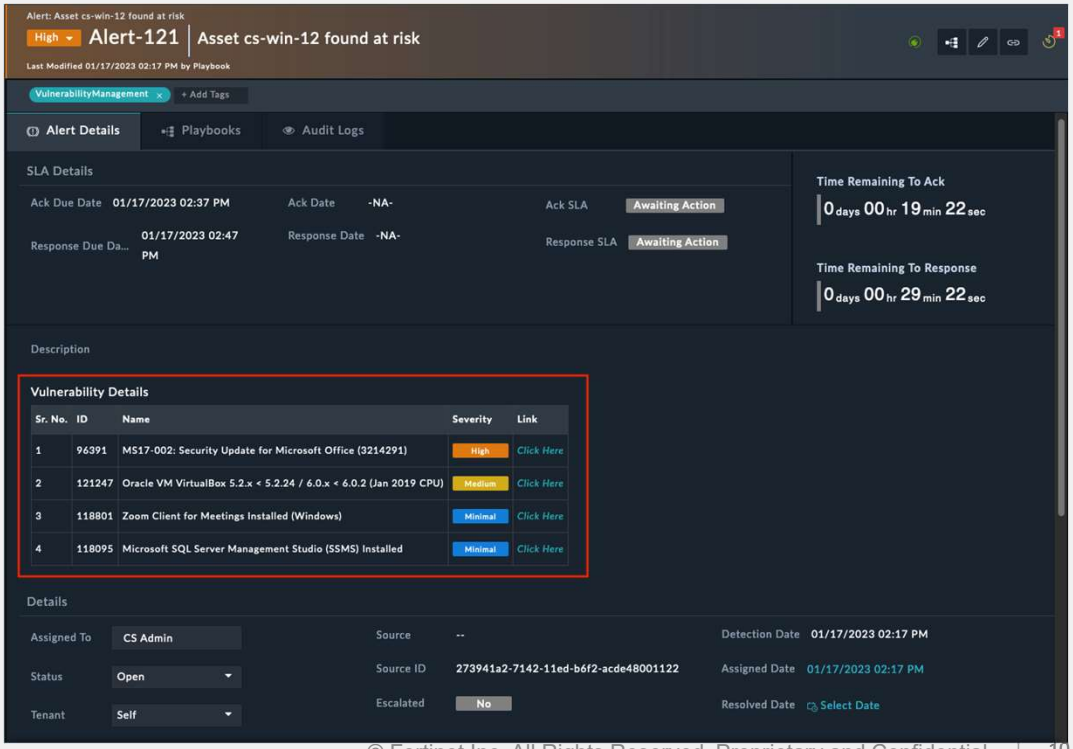
Centralize & automate IT/OT vulnerability management

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



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

NOZOMI NETWORKS · CLAROTY · everbridge · SCADAfence · ARMIS · DRAGOS · Microsoft Sentinel

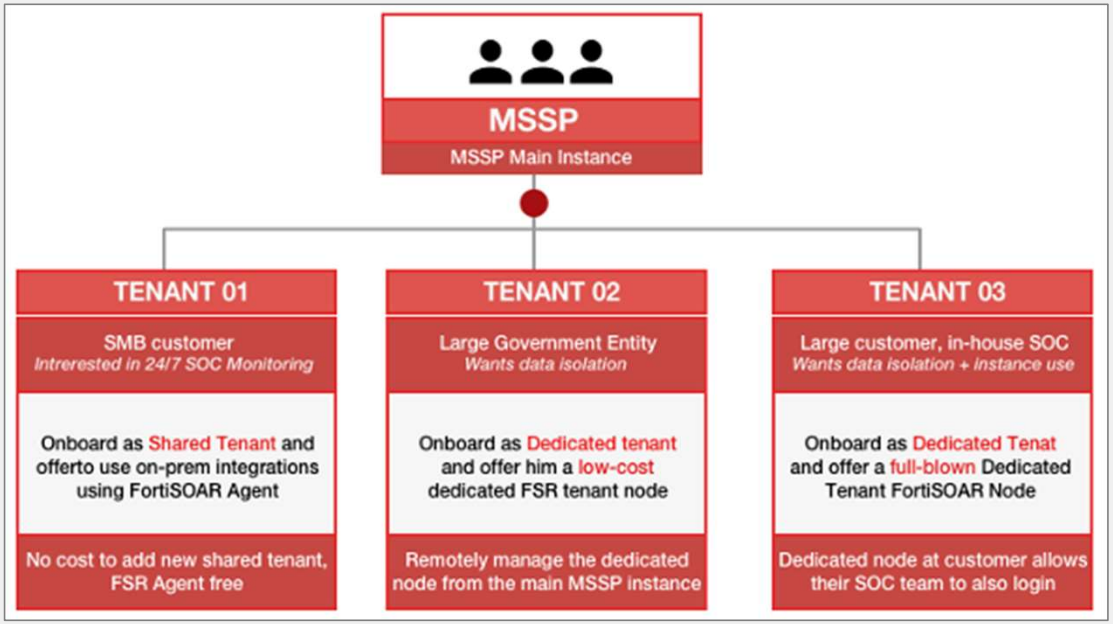
Integrations across multi-vendor IT/OT security products and OT specialty solutions

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

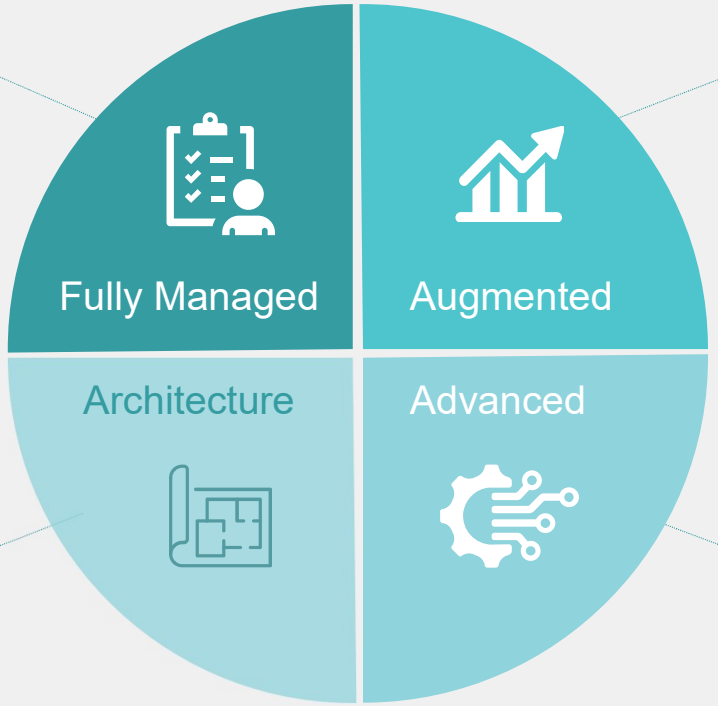
Host tenant on Master SOAR (**no cost increase**)

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**

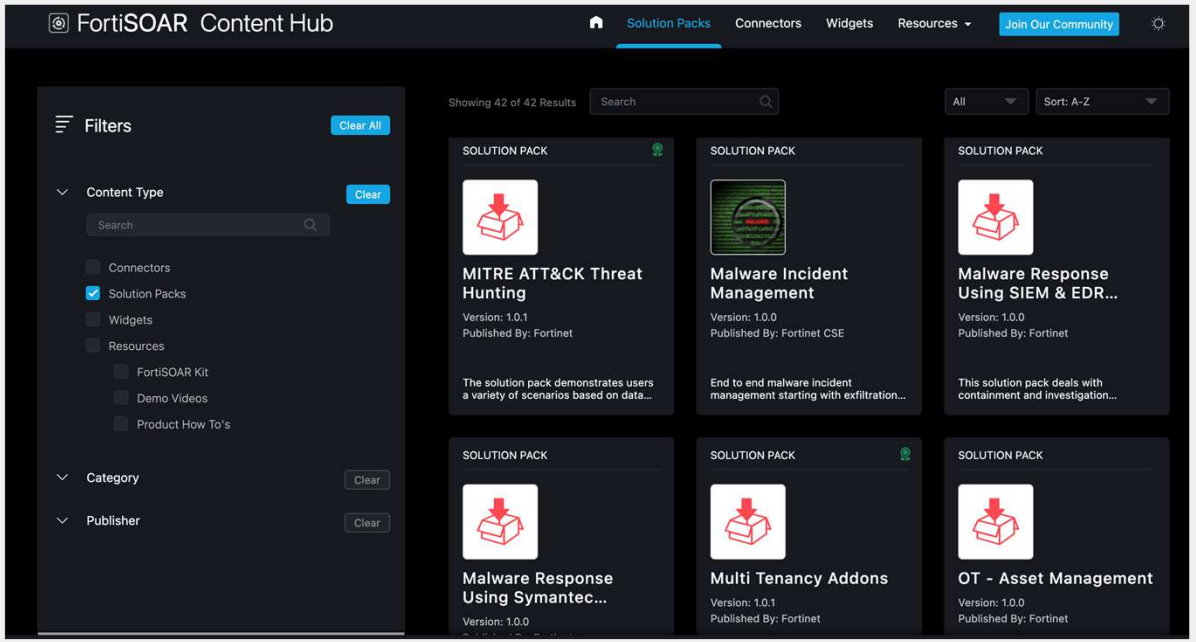
Content Hub and Community

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