APRIL 2023

AVEVA's Strategies to Keep Our Products & Customers Secure

For External Use

Alicia Rantos – AVEVA Cyber Security Governance Program Manager CS

Bryan Owen – AVEVA Head of Product Security R&D

AVEVA

Agenda

- Agenda & Introductions
- Current Threat Landscape
- AVEVA Product Cybersecurity Practices
- Customer Success Cybersecurity Best Practices & Resources
- Industry Best Practice Recommendations
- Questions
- Resources and References

Speaker Introduction

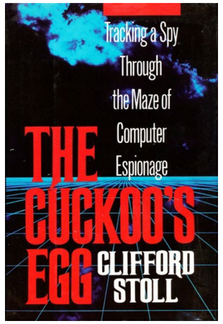
Alicia Rantos

- Cyber Security Governance Program Manager, Customer Success (Global).
- Part of Customer Success since 1999 formerly supporting key products and programs.
- B.Sc. in Computer Information Systems and an MBA.
- Trained by the Department of Homeland Security's Control Systems Security Program and SANS in 2014.
- GIAC Global Industrial Cyber Security Professional (GICSP) certified 2015.

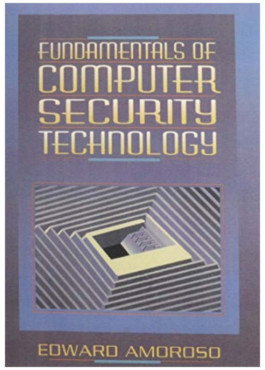
Speaker Introduction

Bryan Owen

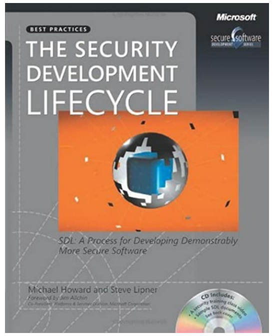
1989



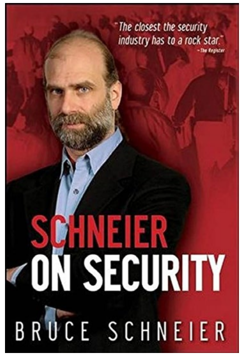
1994



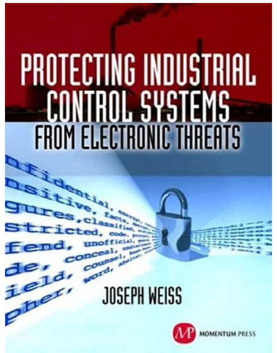
2006


BEST PRACTICES
Microsoft
secure software
THE SECURITY DEVELOPMENT LIFECYCLE
SDL: A Process for Developing Demonstrably More Secure Software
Michael Howard and Steve Lipner

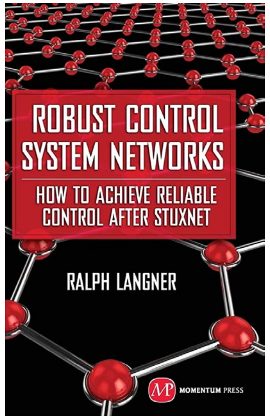
2008



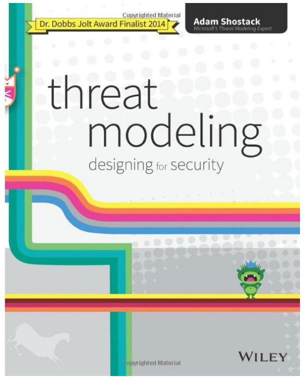
2010


PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS
JOSEPH WEISS
MOMENTUM PRESS

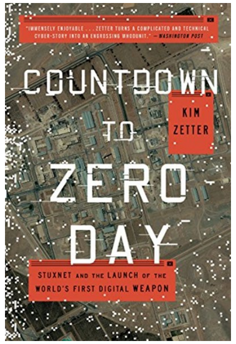
2011


ROBUST CONTROL SYSTEM NETWORKS
HOW TO ACHIEVE RELIABLE CONTROL AFTER STUXNET
RALPH LANGNER
MOMENTUM PRESS

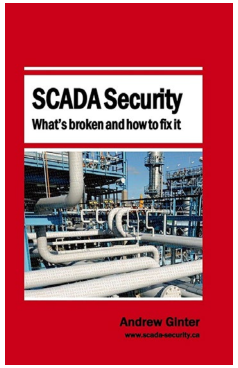
2014



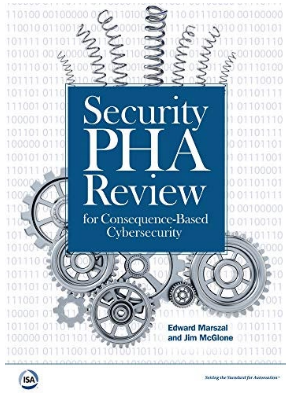
2015



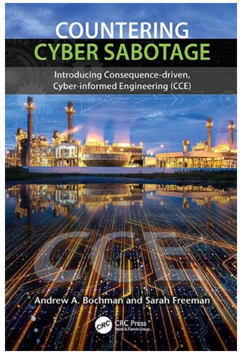
2016

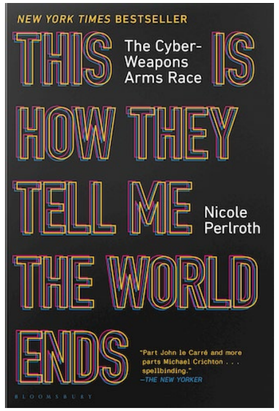


2019

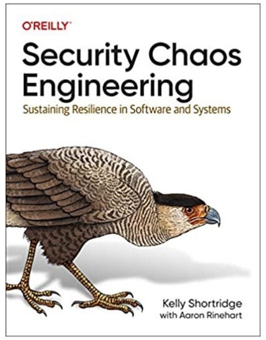

Security PHA Review
for Consequence-Based Cybersecurity
Edward Marszal and Jim McGlone
ISA

2021


COUNTERING CYBER SABOTAGE
Introducing Consequence-driven, Cyber-informed Engineering (CCE)
Andrew A. Bochman and Sarah Freeman
CRC Press


NEW YORK TIMES BESTSELLER
THIS IS HOW THEY TELL ME THE WORLD ENDS
The Cyber-Weapons Arms Race
Nicole Perlroth
BLOOMSBURY

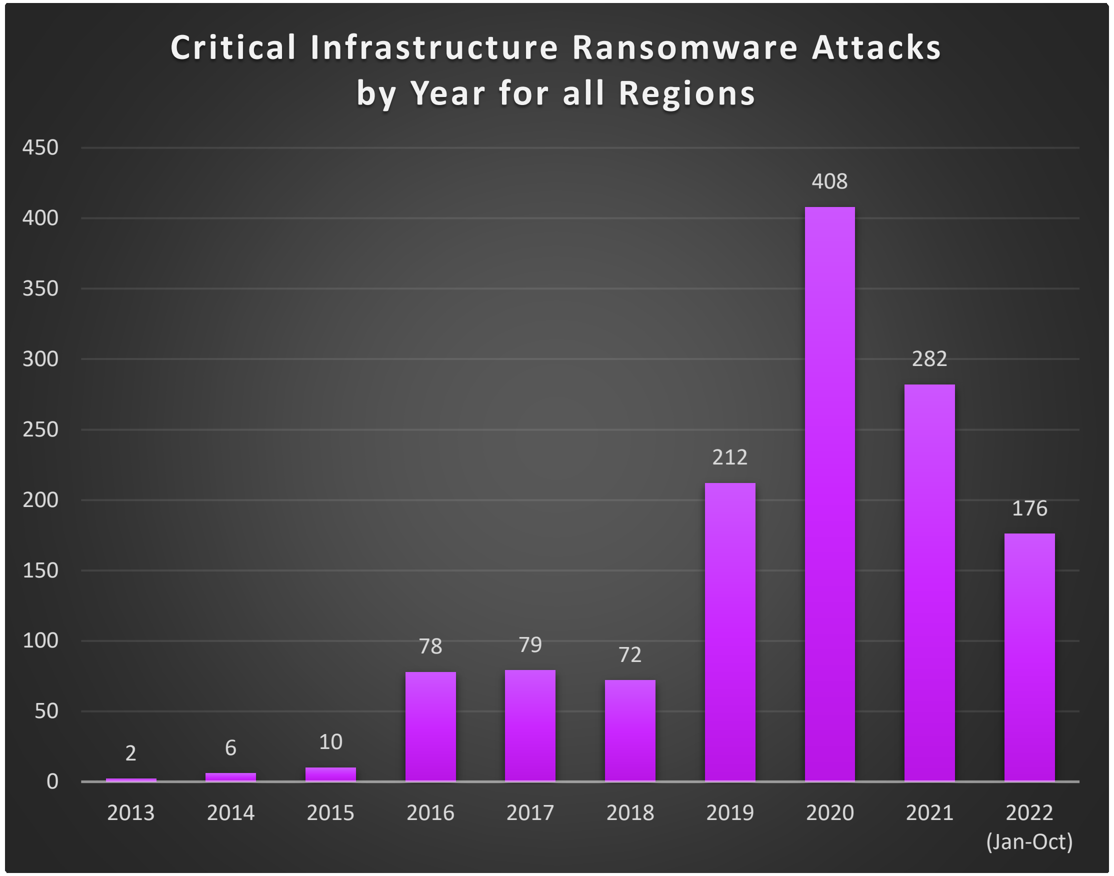
2023


O'REILLY
Security Chaos Engineering
Sustaining Resilience in Software and Systems
Kelly Shortridge
with Aaron Rinehart

Current Threat Landscape

Critical Infrastructure Ransomware Attacks (CIRA) Dataset

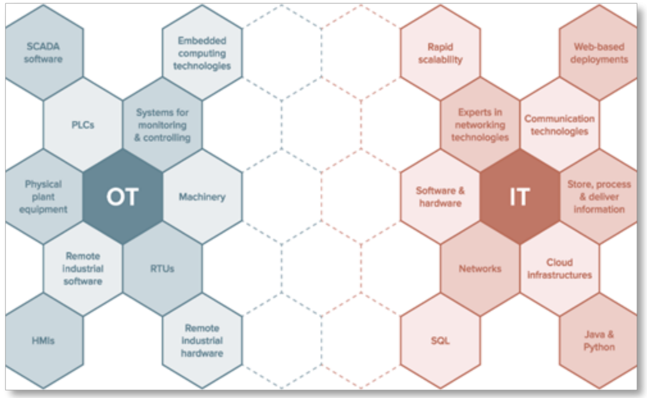
Successful attacks are a new normal for several CI sectors. Government, Healthcare, and Education are the most reported while attacks in Chemical and Water are the least reported.



2022 (Jan-Oct)	2013 thru Oct 2022	Primary Sector
33	295	Government Facilities
25	223	Healthcare
24	197	Education
17	101	Critical Manufacturing
12	98	Information Technology
12	73	Transportation Systems
9	64	Commercial Facilities
10	59	Communications
8	52	Financial
1	49	Emergency Services
12	44	Energy
7	38	Food and Agriculture
0	13	Chemical
3	12	Water and Wastewater
3	7	Defense Industrial
0	1	Nuclear

Source: TEMPLE University *Rege, A. (2022). "Critical Infrastructure Ransomware Attacks (CIRA) Dataset". Version 12.4. Temple University. Online at https://sites.temple.edu/care/cira/. Funded by National Science Foundation CAREER Award #1453040. ORCID: 0000-0002-6396-1066*

Could Ransomware Jump the Gap?


SCADA software
Embedded computing technologies
PLCs
Systems for monitoring & controlling
Physical plant equipment
OT
Machinery
Remote industrial software
RTUs
HMIs
Remote industrial hardware
Rapid scalability
Web-based deployments
Experts in networking technologies
Communication technologies
Software & hardware
IT
Store, process & deliver information
Networks
Cloud infrastructures
SQL
Java & Python

IT / OT CYBERSECURITY GAP

DIGITAL TRANSFORMATION

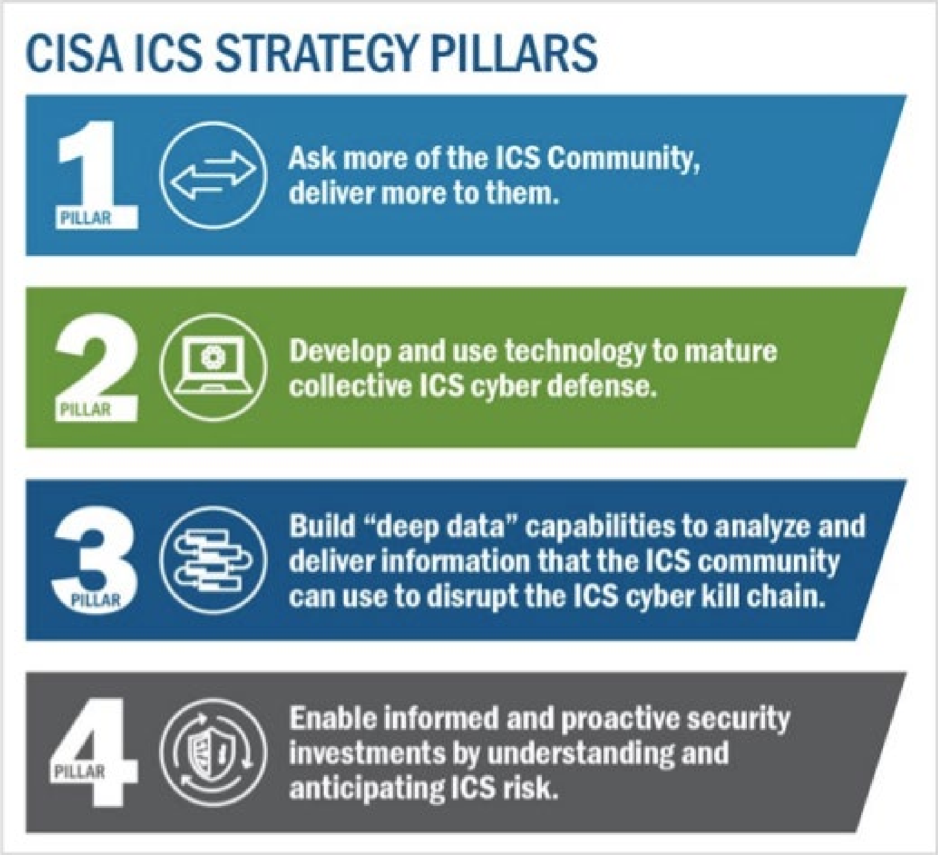
ENTERPRISE ACCESS TO ICS DATA

CISA: Securing Industrial Control Systems

A Unified Initiative

CISA's ICS Vision

- Empower the ICS community to defend itself
- Inform ICS investments and proactive risk management of NCFs
- Unify capabilities and resources of the Federal Government
- Move to proactive ICS security; and
- Drive positive, sustainable, and measurable change to the ICS risk environment.



CISA ICS STRATEGY PILLARS

1 PILLAR — Ask more of the ICS Community, deliver more to them.

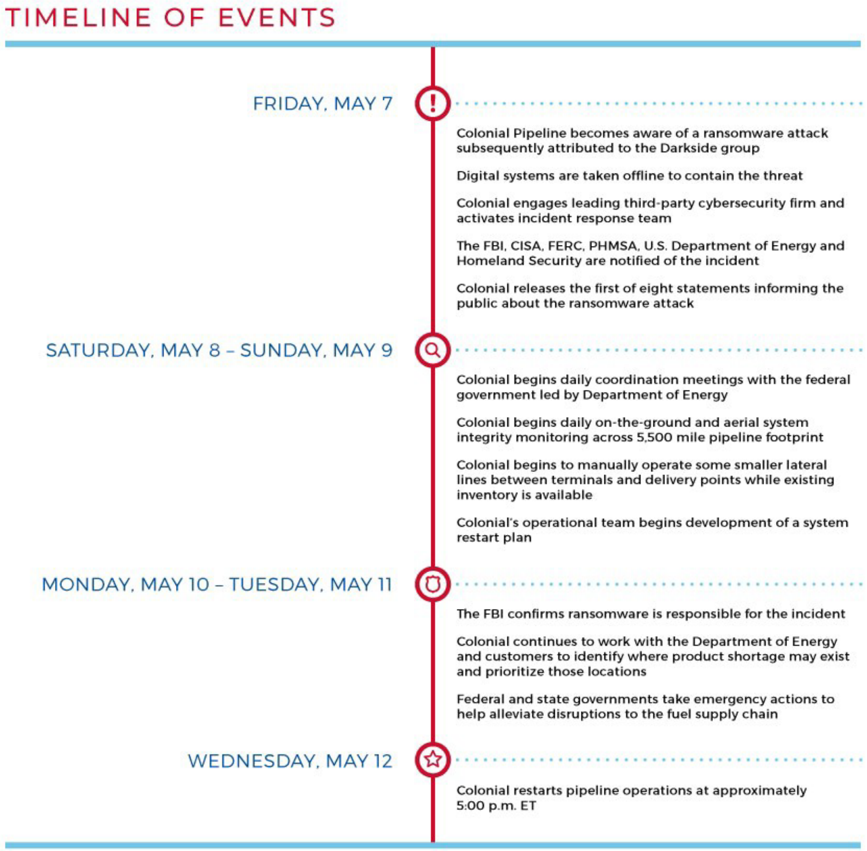
2 PILLAR — Develop and use technology to mature collective ICS cyber defense.

3 PILLAR — Build "deep data" capabilities to analyze and deliver information that the ICS community can use to disrupt the ICS cyber kill chain.

4 PILLAR — Enable informed and proactive security investments by understanding and anticipating ICS risk.

Colonial Pipeline Attack timeline

Massive fuel outages in Eastern USA. $4.4 million in ransom paid.



TIMELINE OF EVENTS

FRIDAY, MAY 7

Colonial Pipeline becomes aware of a ransomware attack subsequently attributed to the Darkside group

Digital systems are taken offline to contain the threat

Colonial engages leading third-party cybersecurity firm and activates incident response team

The FBI, CISA, FERC, PHMSA, U.S. Department of Energy and Homeland Security are notified of the incident

Colonial releases the first of eight statements informing the public about the ransomware attack

SATURDAY, MAY 8 – SUNDAY, MAY 9

Colonial begins daily coordination meetings with the federal government led by Department of Energy

Colonial begins daily on-the-ground and aerial system integrity monitoring across 5,500 mile pipeline footprint

Colonial begins to manually operate some smaller lateral lines between terminals and delivery points while existing inventory is available

Colonial's operational team begins development of a system restart plan

MONDAY, MAY 10 – TUESDAY, MAY 11

The FBI confirms ransomware is responsible for the incident

Colonial continues to work with the Department of Energy and customers to identify where product shortage may exist and prioritize those locations

Federal and state governments take emergency actions to help alleviate disruptions to the fuel supply chain

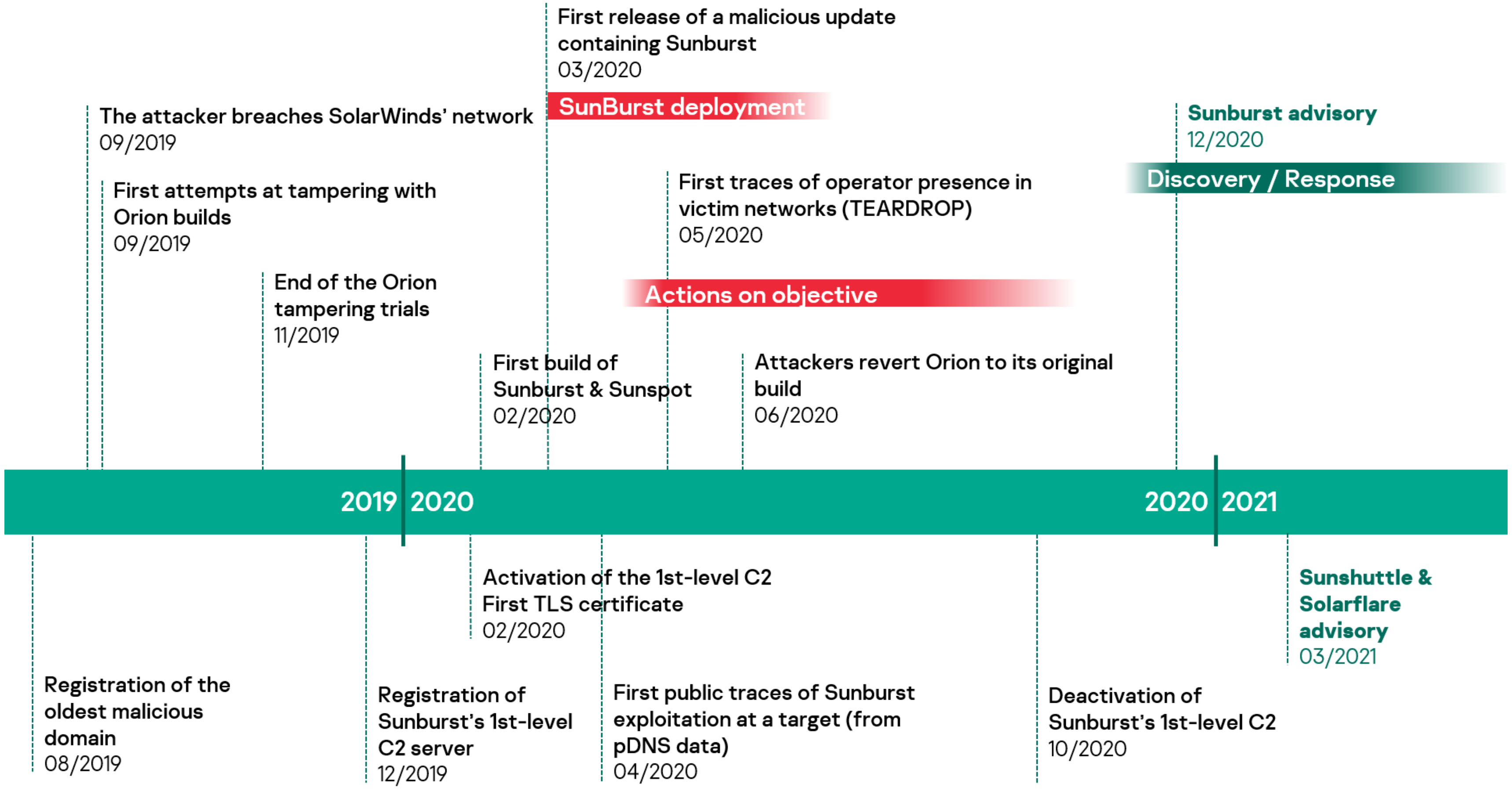
WEDNESDAY, MAY 12

Colonial restarts pipeline operations at approximately 5:00 p.m. ET

- Hackers used old existing credentials to access network via VPN
- The credentials were probably obtained from a previous information leak that had been sold on the dark web
- MFA could have helped
- Deletion of old accounts could have helped

SolarWinds attack timeline

Major operation lasting more than a year



Registration of the oldest malicious domain
08/2019

The attacker breaches SolarWinds' network
09/2019

First attempts at tampering with Orion builds
09/2019

End of the Orion tampering trials
11/2019

Registration of Sunburst's 1st-level C2 server
12/2019

First build of Sunburst & Sunspot
02/2020

Activation of the 1st-level C2
First TLS certificate
02/2020

SunBurst deployment

First release of a malicious update containing Sunburst
03/2020

First public traces of Sunburst exploitation at a target (from pDNS data)
04/2020

Actions on objective

First traces of operator presence in victim networks (TEARDROP)
05/2020

Attackers revert Orion to its original build
06/2020

Deactivation of Sunburst's 1st-level C2
10/2020

Discovery / Response

Sunburst advisory
12/2020

Sunshuttle & Solarflare advisory
03/2021

AVEVA Product Cybersecurity Practices

AVEVA's Commitment

Support of AVEVA and customers' mission to operate safe and reliable systems.

Philosophy

- Do no harm
- Keep the bad guys out
- Limit potential damage
- Hunt for evil

Priorities

- Secure by design
- Pervasive access control
- Just enough privilege
- Resist sabotage

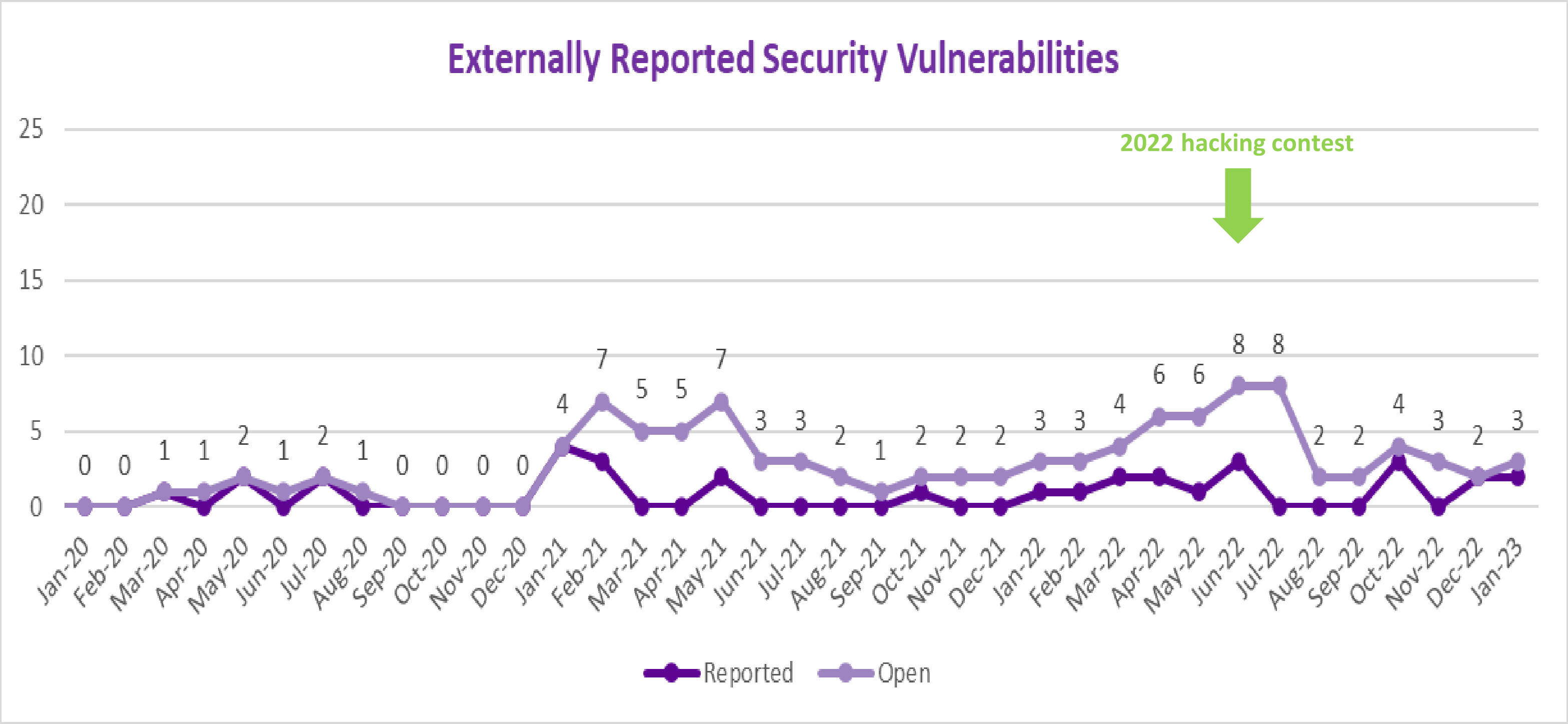
Executive Commitment

Risk management key performance indicators

- Reportable incidents
- Potential major non-conformance
- Cloud security interventions
- Software security interventions
- External discovered issues

External Discovered Issues

AVEVA coordinates with customers, security researchers and authorities on response to security concerns. Updates and/or mitigation guidance are provided in alignment with recognized standards.



Externally Reported Security Vulnerabilities

2022 hacking contest

INTERNATIONAL STANDARD

ISO/IEC 30111

Second edition
2019-10

Information technology — Security techniques — Vulnerability handling processes

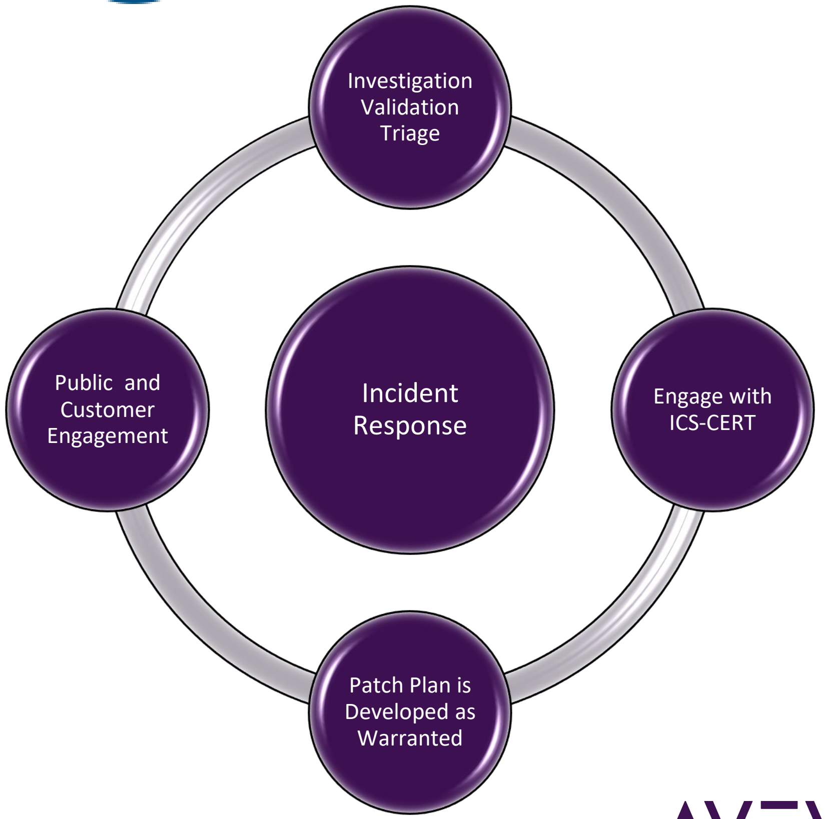
Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité

Incident Response/Vulnerability Management

Incident Response Working Procedure Overview

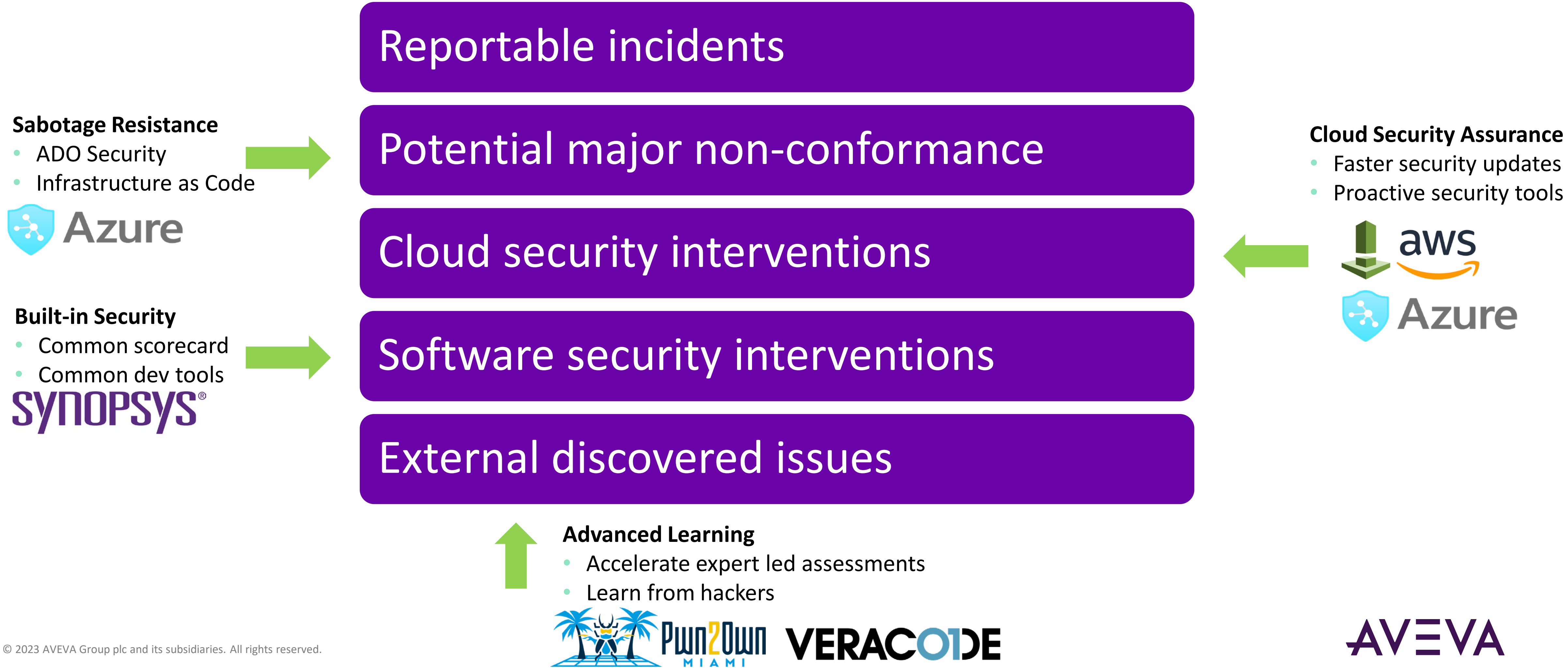
- Investigation, Validation, and Triage of issue
- Severity ranking use Common Vulnerability Scoring System and related information (CISA Known Exploited Vulnerability Catalog, Exploit Prediction Scoring System, etc)
- Coordination with AVEVA Product Teams and ICS-CERT (CISA)
- Remediation/mitigation plan approval including development of a software security update as appropriate
- Security Bulletins, Distributor and Customer alerts, and public announcements as warranted

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY


Investigation Validation Triage
Engage with ICS-CERT
Patch Plan is Developed as Warranted
Public and Customer Engagement
Incident Response

Executive Commitment – Targeted Investments

Accelerate risk reduction commensurate with the changing landscape for cyber threats



Reportable incidents

Potential major non-conformance

Cloud security interventions

Software security interventions

External discovered issues

Sabotage Resistance

- ADO Security
- Infrastructure as Code

Built-in Security

- Common scorecard
- Common dev tools

Cloud Security Assurance

- Faster security updates
- Proactive security tools

Advanced Learning

- Accelerate expert led assessments
- Learn from hackers

AVEVA

Modern Software Development Process and Tool Chains

Secure development lifecycle and operational security assurance practices are integrated within AVEVA R&D processes.

Ensuring Security Knowledge

- Security Training is mandatory and provided to:
  - Dev Engineers, Test Engineers, Architects, Dev/QA Managers
- Team Members have annual security training goals aligned with product technologies
- Any new teams and/or team members are trained in Security
- AVEVA uses Microsoft, Team Professor, and Plural Sight trainings

Flow of built-in, high-quality software

Sprint Minus 1

Definition of Ready

- Story is well defined and ready for execution
- Product management own functional stories
- Architects own advanced design stories
- QA Leads / Dev Mgr own non-functional stories
- Assumptions, how to demo, dependencies

2 Week Sprint

Development via Built-in Quality

Developers create new code via following:

- Coding standards
- Unit Testing
- Static Code Analysis
- Code design
- Code Coverage
- Collaboration Tools
- Continuous Integration

Exploratory & Automated Test

Test team within scrum team additionally:

- Expands automated test coverage
- Based on story definition (Definition of Ready)
- Appropriate regression testing based on SME input
- PSR* & Security testing

Definition of Done

- No story counts unless quality criteria met
- All team members own this
- Each release train has a Definition of Done document based on their product / domain
- End result: Shippable quality code at end of sprint

Sprint Plus 1

System Test

- End to end functionality across the system
- Automated wherever possible
- System level PSR testing
- System level security testing

Release

Release Criteria

- Strictly enforced
- Target is always zero known defects
- Quality overrides schedule
- When exceptions occur, they are well documented in release notes and are few

Cloud DevOps Dashboard – 24/7 Monitoring and Alerts

Alarm

- Metric alarms
- Log search alarms

Log

- Windows Event Logs
- Managed service logs
  - RDS

Health

- Resource health
- Service health

Scaling

- Auto scaling groups

Resource

- Deployments
- CloudFormation events and errors

Security

- Configuration Drift
- Patch Status
- Suspicious Activity

🟥 Red alerts

Urgent alerts indicating likely production outage or severe impact to key production functionality.

🟨 Yellow alerts

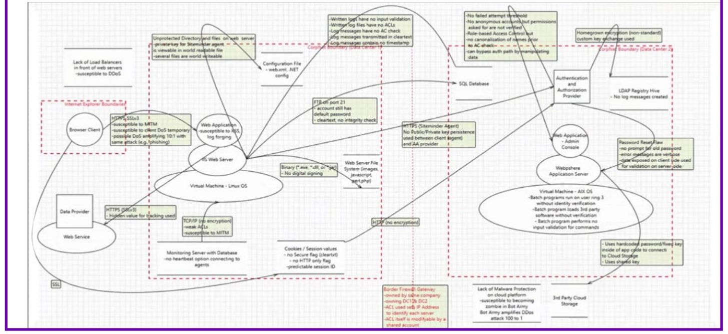
Non-urgent alerts indicating longer term issue or trend, non-urgent error that may be transient, known issue requiring intervention.

□ White alerts

Informational events used for context, such as scaling events or changes to resources.

Secure design threat models:

1) Know what we are building; 2) Identify what can go wrong; 3) Decide what to do about it; 4) Verify we did a good job.



Lack of Load Balancers in front of web servers -susceptible to DDoS
Unprotected Directory and files on web server -private key for Siteminder agent is viewable in world readable file -several files are world writeable
Configuration File - web.xml, .NET config
-Written logs have no input validation -Written log files have no ACLs -Log messages have no AC check -Log messages transmitted in cleartext -Log messages contain no timestamp
Corpnet Boundary (Data Center 1)
-No failed attempt threshold -No anonymous accounts but permissions asked for are not verified -Role-based Access Control but -no canonicalization of names prior to AC check -can bypass auth path by manipulating data
Homegrown encryption (non-standard) custom key exchange used
Corpnet Boundary (Data Center 2)
SQL Database
Authentication and Authorization Provider
LDAP Registry Hive - No log messages created
Internet Explorer Boundaries
Browser Client
HTTPS, SSLv3 -susceptible to MITM -susceptible to client DoS temporary -possible DoS amplifying 10:1 with same attack (e.g. phishing)
Web Application -susceptible to XSS, log forging
FTP on port 21 - account still has default password - cleartext, no integrity check
HTTPS (Siteminder Agent) No Public/Private key persistence used between client (agent) and AA provider
Web Application - Admin Console
Password Reset Flow -no prompt for old password -error messages are verbose -data exposed on client side used for validation on server side
IIS Web Server
Binary (*.exe, *.dll, or *.jar) - No digital signing
Web Server File System (images, javascript, perl,php)
Websphere Application Server
Virtual Machine - Linux OS
Virtual Machine - AIX OS -Batch programs run on user ring 3 without identity verification -Batch program loads 3rd party software without verification - Batch program performs no input validation for commands
Data Provider
Web Service
HTTPS (SSLv3) - Hidden value for tracking used
TCP/IP (no encryption) -weak ACLs -susceptible to MITM
HTTP (no encryption)
Monitoring Server with Database -no heartbeat option connecting to agents
Cookies / Session values - no Secure flag (cleartxt) - no HTTP only flag -predictable session ID
- Uses hardcoded password/fixed key inside of app code to connect to Cloud Storage - Uses shared key
SSL
Border Firewall Gateway -owned by same company owning DC1 & DC2 -ACL used sets IP Address to identify each server -ACL itself is modifyable by a shared account
Lack of Malware Protection on cloud platform -susceptible to becoming zombie in Bot Army Bot Army amplifies DDos attack 100 to 1
3rd Party Cloud Storage

Security Tools

Development

- Checkmarx -> Polaris
- Mend -> Blackduck
- Visual Studio Code Analysis
- Rosyln Analyzers
- BinSkim
- DevSkim
- Microsoft Threat Modeling

Testing

- Attack Surface Analyzer
- NESSUS
- beSTORM
- Burpsuite
- Detectify
- Qualys
- Microsoft OneFuzz

Formal Security Review

Cloud Readiness

Cloud Deployment

AWS GuardDuty, Inspector

Azure Defender for Cloud

- Bitsight
- Detectify

- Qualys
- ReportURI

- IOActive
- Outpost24

- Veracode
- Synopsys

Practices conform or exceed industry standards & compliance: ISA/IEC 62443, NIST 800-218, ISO 27001, SOC2

AVEVA

Current continuous improvement initiatives and activities

*Several workstreams will involve significant joint effort with corporate IT and BU partners

Built-in Security

- Measuring best practices
- Leading security tools
- Chaos engineering

Sabotage Resistance

- Controlled access to code
- DevOps methodology
- Zero trust architecture

Advanced Learning

- Certified ethical hacker
- Penetration testing
- Adversary simulation

Assessed and Verified

- Organization certifications
- Standard benchmarks
- Supply chain risk management

Cloud Security Assurance

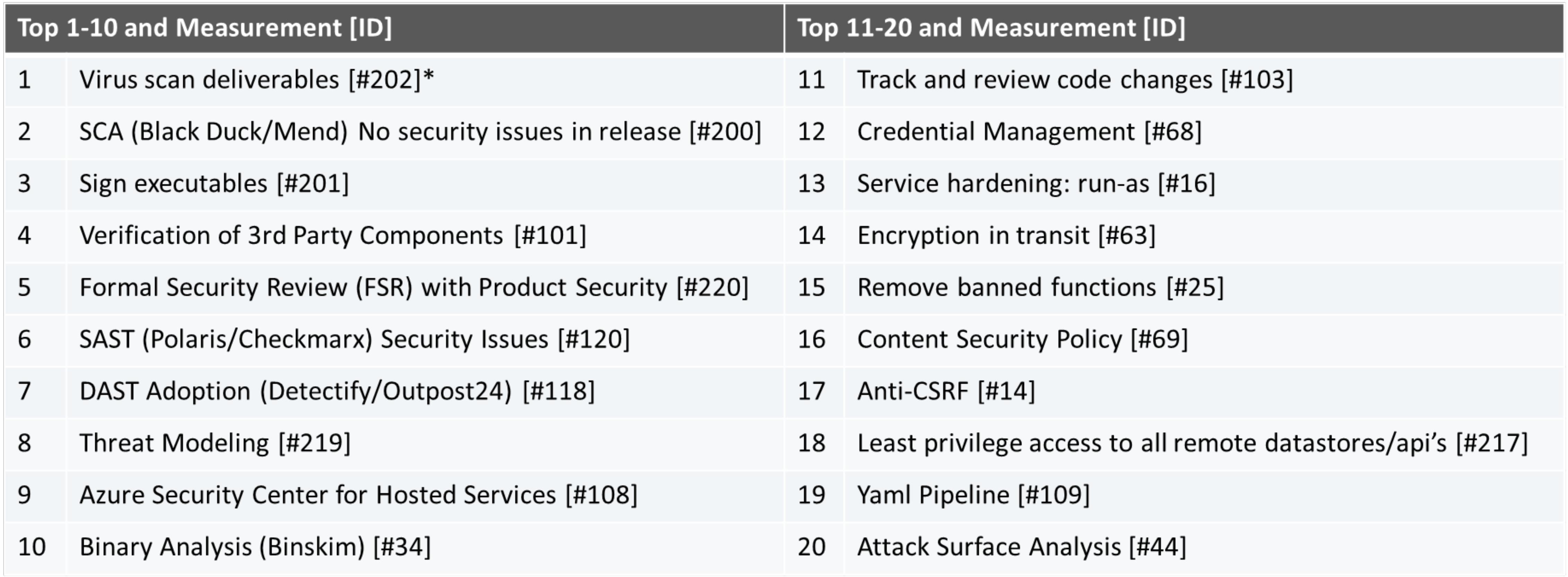
- Configuration management
- Endpoint protection
- Security operations center

Product Security Partners

- Modern frameworks
- Security research
- Public/Private collaboration

Product Security Scorecard

We relentlessly strive to measure and prioritize security best practices.



Top 1-10 and Measurement [ID]		Top 11-20 and Measurement [ID]	
1	Virus scan deliverables [#202]*	11	Track and review code changes [#103]
2	SCA (Black Duck/Mend) No security issues in release [#200]	12	Credential Management [#68]
3	Sign executables [#201]	13	Service hardening: run-as [#16]
4	Verification of 3rd Party Components [#101]	14	Encryption in transit [#63]
5	Formal Security Review (FSR) with Product Security [#220]	15	Remove banned functions [#25]
6	SAST (Polaris/Checkmarx) Security Issues [#120]	16	Content Security Policy [#69]
7	DAST Adoption (Detectify/Outpost24) [#118]	17	Anti-CSRF [#14]
8	Threat Modeling [#219]	18	Least privilege access to all remote datastores/api's [#217]
9	Azure Security Center for Hosted Services [#108]	19	Yaml Pipeline [#109]
10	Binary Analysis (Binskim) [#34]	20	Attack Surface Analysis [#44]

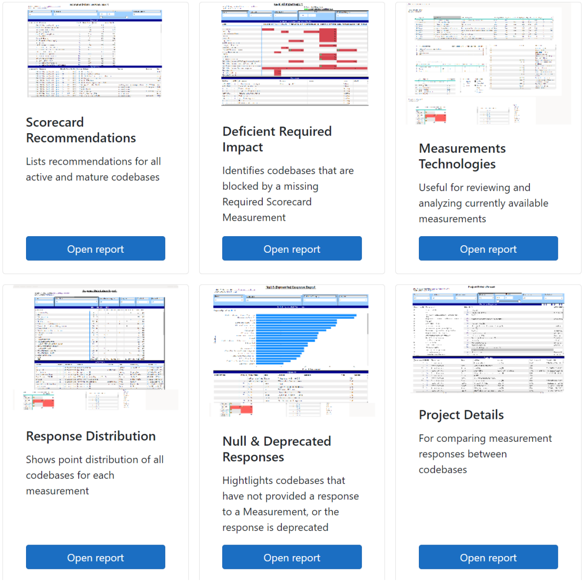
*100's of measurements/practices are in our toolbox

AVEVA

Scorecard Illustration

Use objective data to inform planning and advance best practice implementation

Scorecard PowerBI report selection



Scorecard Recommendations

Lists recommendations for all active and mature codebases

Open report

Deficient Required Impact

Identifies codebases that are blocked by a missing Required Scorecard Measurement

Open report

Measurements Technologies

Useful for reviewing and analyzing currently available measurements

Open report

Response Distribution

Shows point distribution of all codebases for each measurement

Open report

Null & Deprecated Responses

Hightlights codebases that have not provided a response to a Measurement, or the response is deprecated

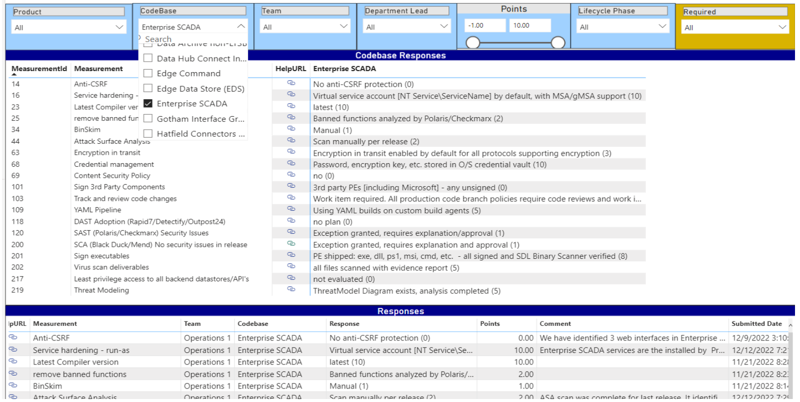
Open report

Project Details

For comparing measurement responses between codebases

Open report

"Project Details" report sample for Enterprise SCADA



Product: All
CodeBase: Enterprise SCADA
Search
□ Data Archive non-LTSB
□ Data Hub Connect In...
□ Edge Command
□ Edge Data Store (EDS)
☑ Enterprise SCADA
□ Gotham Interface Gr...
□ Hatfield Connectors ...
Team: All
Department Lead: All
Points: -1.00 10.00
Lifecycle Phase: All
Required: All

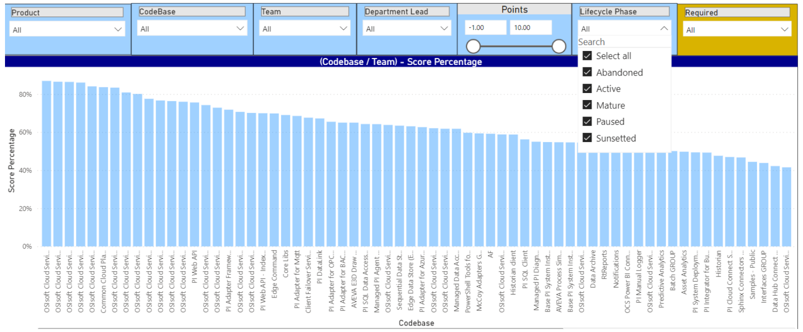
Codebase Responses

MeasurementId	Measurement	HelpURL	Enterprise SCADA
14	Anti-CSRF	🔗	No anti-CSRF protection (0)
16	Service hardening -	🔗	Virtual service account [NT Service\ServiceName] by default, with MSA/gMSA support (10)
23	Latest Compiler ver	🔗	latest (10)
25	remove banned fun	🔗	Banned functions analyzed by Polaris/Checkmarx (2)
34	BinSkim	🔗	Manual (1)
44	Attack Surface Analysis	🔗	Scan manually per release (2)
63	Encryption in transit	🔗	Encryption in transit enabled by default for all protocols supporting encryption (3)
68	Credential management	🔗	Password, encryption key, etc. stored in O/S credential vault (10)
69	Content Security Policy	🔗	no (0)
101	Sign 3rd Party Components	🔗	3rd party PEs [including Microsoft] - any unsigned (0)
103	Track and review code changes	🔗	Work item required. All production code branch policies require code reviews and work i...
109	YAML Pipeline	🔗	Using YAML builds on custom build agents (5)
118	DAST Adoption (Rapid7/Detectify/Outpost24)	🔗	no plan (0)
120	SAST (Polaris/Checkmarx) Security Issues	🔗	Exception granted, requires explanation/approval (1)
200	SCA (Black Duck/Mend) No security issues in release	🔗	Exception granted, requires explanation and approval (1)
201	Sign executables	🔗	PE shipped: exe, dll, ps1, msi, cmd, etc. - all signed and SDL Binary Scanner verified (8)
202	Virus scan deliverables	🔗	all files scanned with evidence report (5)
217	Least privilege access to all backend datastores/API's	🔗	not evaluated (0)
219	Threat Modeling	🔗	ThreatModel Diagram exists, analysis completed (5)

Responses

pURL	Measurement	Team	Codebase	Response	Points	Comment	Submitted Date
🔗	Anti-CSRF	Operations 1	Enterprise SCADA	No anti-CSRF protection (0)	0.00	We have identified 3 web interfaces in Enterprise ...	12/9/2022 3:10:
🔗	Service hardening - run-as	Operations 1	Enterprise SCADA	Virtual service account [NT Service\Se...	10.00	Enterprise SCADA services are the installed by Pr...	12/12/2022 7:2
🔗	Latest Compiler version	Operations 1	Enterprise SCADA	latest (10)	10.00		11/21/2022 8:2
🔗	remove banned functions	Operations 1	Enterprise SCADA	Banned functions analyzed by Polaris/...	2.00		11/21/2022 8:2
🔗	BinSkim	Operations 1	Enterprise SCADA	Manual (1)	1.00		11/21/2022 8:1
🔗	Attack Surface Analysis	Operations 1	Enterprise SCADA	Scan manually per release (2)	2.00	ASA scan was complete for last release. It identifi	12/12/2022 7:2

"Scorecard Summary" report sample for all codebases



Product: All
CodeBase: All
Team: All
Department Lead: All
Points: -1.00 10.00
Lifecycle Phase: All
Search
☑ Select all
☑ Abandoned
☑ Active
☑ Mature
☑ Paused
☑ Sunsetted
Required: All

© 2023 AVEVA Group plc and its subsidiaries. All rights reserved.

Scorecard Tailored Baselines

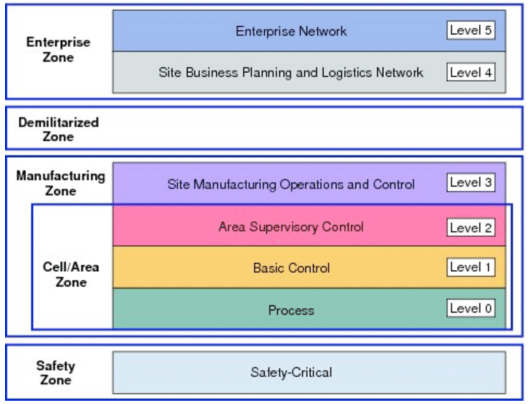
Scorecard leverages internal tools and procedures with proven support for compliance audit.

Cloud Service Baseline

- Measurements specific to rapid deployment of security updates
- Multi-tenant measurements
- Cadence vs release focused measurements
- Threat simulation including
  - Chaos engineering methods
  - External penetration testing
  - Detection and response drills
- SOC2 specific compliance evidence

Process Control Baseline

- Measurements applicable to ISA/IEC 62443 product capability level 2
- Prescriptive threat modeling measurements
- ISA Secure specific compliance evidence



Enterprise Zone

Enterprise Network Level 5

Site Business Planning and Logistics Network Level 4

Demilitarized Zone

Manufacturing Zone

Site Manufacturing Operations and Control Level 3

Cell/Area Zone

Area Supervisory Control Level 2

Basic Control Level 1

Process Level 0

Safety Zone

Safety-Critical

National Security Baseline

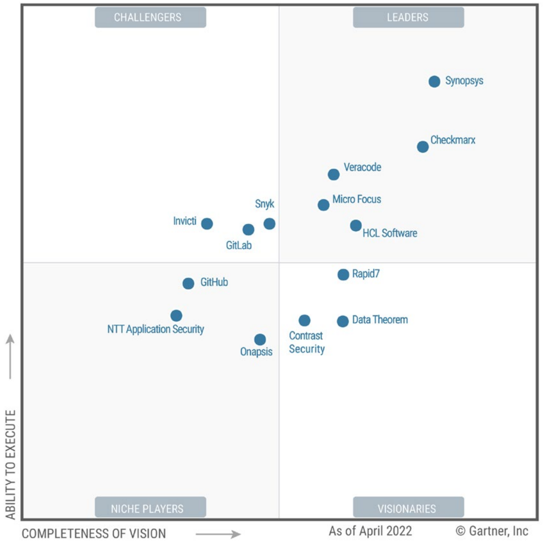
- Measurements specific to regulatory directives
- NIST 800-53 R5 conformance for development environment
- MS ADO security best practices
- Infrastructure as code measurements
- Prescriptive software supply chain security risk management

Advancing Baseline Capability

Important initiatives leveraging industry experts are highlighed below.

SYNOPSYS®

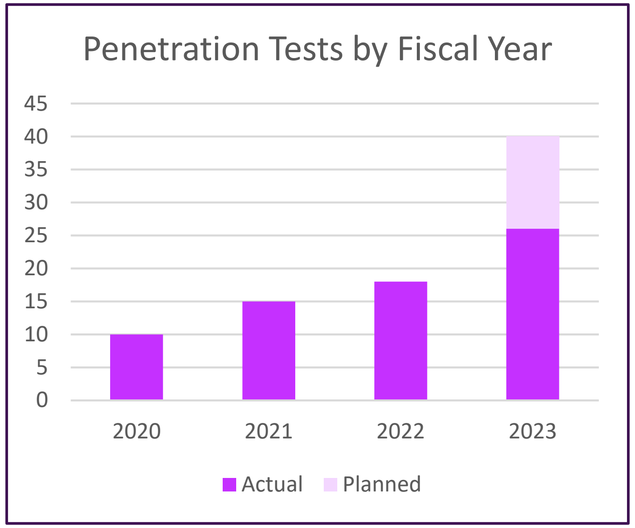
- Advance secure code and manage 3P component risk
- Best of breed software security suite tools
- **Status: Migration in progress**



Source: Gartner (April 2022)

VERACODE

- Accelerate penetration testing and learn from experts
- Trusted security verification consultation
- **Status: In production**



digicert®

- Unify and modernize secure code signing infrastructure
- Trusted root for cryptographic service
- **Status: Preparation and planning**

> "We have 6,000-plus developers on six continents. Trying to secure all the keys that they need (for code signing) would be a nightmare. With SSM, the keys remain in the cloud, and access is provided to sign with them, but not to get the actual keys themselves. That is a huge win for us."
>
> David Nalley, Vice President, Infrastructure, The Apache Software Foundation

AVEVA

Advancing Cloud Capability

Operational assurance built into cloud services includes comprehensive security monitoring and alerting. We are targeting detection rules and alert workflows for faster remediation.

Inside->Out (Configuration and Activity Alerting)

- Vulnerability and network exposure inspection
- On change and continuous security monitoring

aws

AWS Inspector

Azure

Defender for Cloud

Outside->In (Attack Surface Management)

- OWASP compliant web application security testing
- Continuous penetration testing service

detectify

Domain verification

Outpost24

Continuous PenTest

BITSIGHT

Security rating service & supply chain risk management

- Corporate security

Summary of Certifications and Q3 External Audit Highlights

Audit frequencies include biannual, annual and every 3 years

ISO 9001 Quality Certification

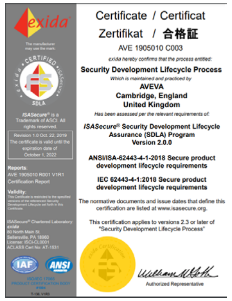
- Quality Management certificate
- Improves product, process and service quality
- Increases customer satisfaction
- **Audit: Oct 2022**

ISO 27001 Security Certification

- Information Security Management
- Risk-based approach to information asset management
- Continuous risk assessments
- **Audit: Oct 2022**

SOC 2 Type 2 Audit

- Security assessment of cloud services
- AICPA Trust Criteria
- Business imperative for AVEVA Cloud
- **Audit: Nov/Dec 2022**



exida

The manufacturer may use the mark:

ISASecure® is a Trademark of ASCI. All rights reserved.

Revision 1.0 Oct. 22, 2019
The certificate is valid until the expiration date of October 1, 2022

Reports:
AVE 1905010 R001 V1R1
Certification Report

Validity:
This Certificate is restricted to the specified versions of the referenced Security Development Lifecycle set forth in this Certificate.

ISASecure® Chartered Laboratory:
exida
80 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

T-136, V1R3

Certificate / Certificat
Zertifikat / 合格証

AVE 1905010 C003

exida hereby confirms that the process entitled:

Security Development Lifecycle Process

Which is maintained and practiced by

AVEVA
Cambridge, England
United Kingdom

Has been assessed per the relevant requirements of:

***ISASecure*® Security Development Lifecycle Assurance (SDLA) Program Version 2.0.0**

ANSI/ISA-62443-4-1-2018 Secure product development lifecycle requirements

IEC 62443-4-1:2018 Secure product development lifecycle requirements

The normative documents and issue dates that define this certification are listed at www.isasecure.org.

This certification applies to versions 2.3 or later of "Security Development Lifecycle Process"

Authorized Representative

ISASecure SDLA

- IEC 62443-4-1 standard
- Security Development Lifecycle Assurance
- Secure by design; secure coding and verification
- **Audit: Sept/Oct 2022**

ANNSI Certification

- France only - country certification
- Product specific: AVEVA System Platform
- French security agency requirement
- Business imperative; sales requirement

ISO 14001

- Environmental Management Systems
- Environmental impact continuous improvement
- Business imperative for ESG
- **Audit: Nov/Dec 2022**

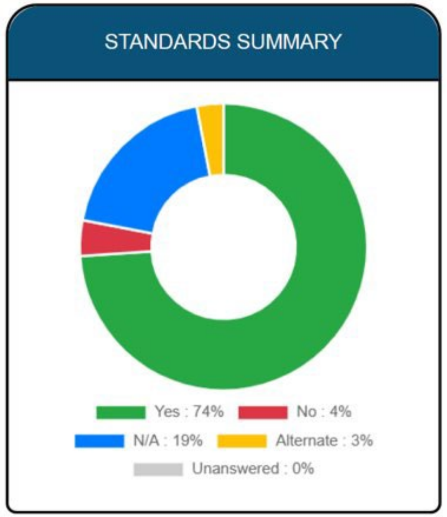
AVEVA

Product Security Special Assessments

Benchmarking and advancing defender knowledge is essential to counter rapidly evolving threats.

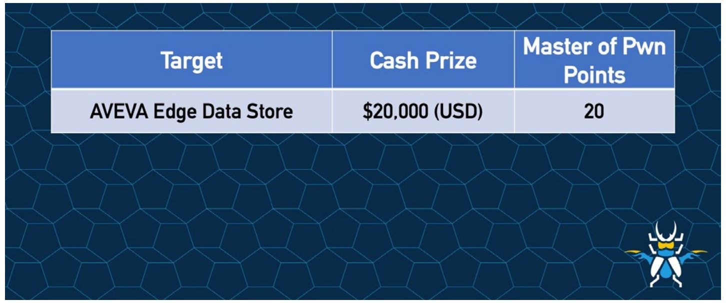
National Security Zone

- US CISA security evaluation tool
- NIST 800-53 Rev 5 Score: >95%



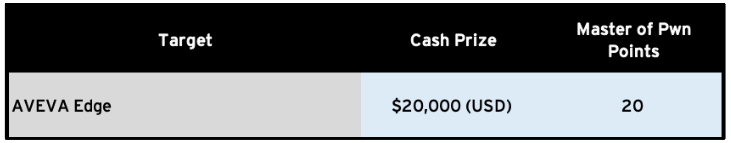
ZDI sponsored bug bounty contest

- AVEVA Edge Data Store
- $20K Award for Remote Code Execution



Target	Cash Prize	Master of Pwn Points
AVEVA Edge Data Store	$20,000 (USD)	20

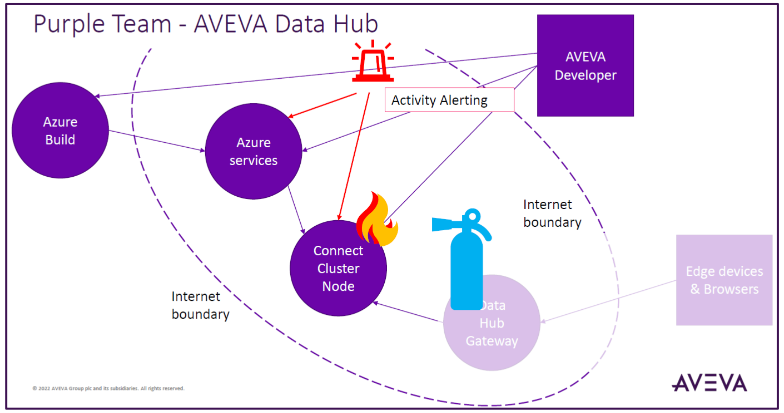
2022 results: Edge HMI 4 exploits ($80K)



Target	Cash Prize	Master of Pwn Points
AVEVA Edge	$20,000 (USD)	20

AVEVA Data Hub

- Purple team engagement
- Highlighted in AWC security presentation



Light 'fires' behind the lines, verify detection, and practice putting the fire out.

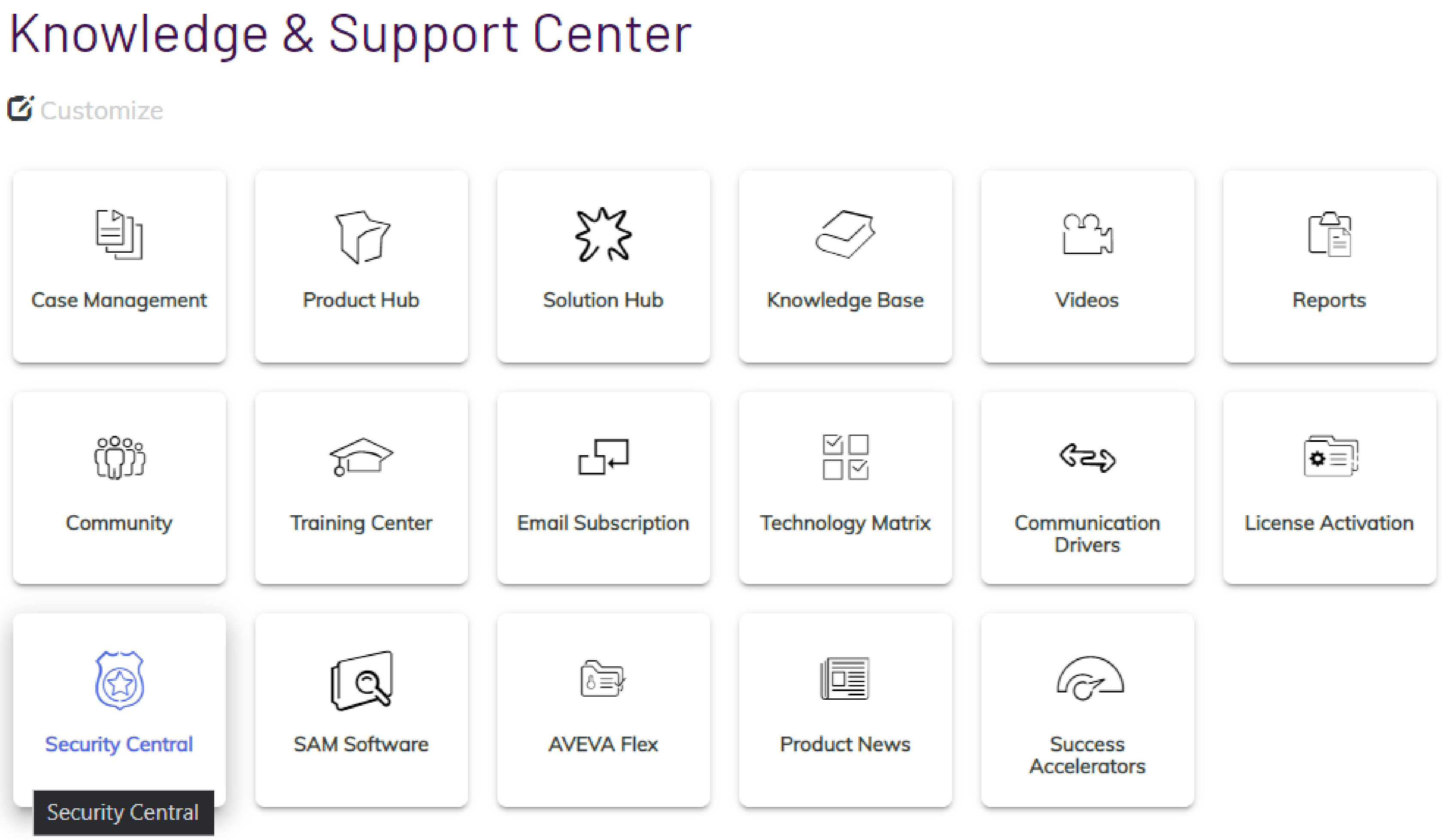
Customer Success Cybersecurity Best Practices

Customer Success Cybersecurity Program

- Customer cyber security issues/incidents, questions, requests.
- Collaborates with organizational resources:
  - R&D / QA product security teams to resolve issues, test, document and present.
  - Marketing, Management and various teams to accomplish cyber security goals.
  - Schneider Electric, Cylance and other Cyber Security consulting groups on consulting projects, training.
  - CF Team on Success Accelerator service offering details and resources.
- Customer Success Website's Security Central and related questions
- Customer Success PI Business website's security pages and articles.

Knowledge & Support Center: **Security Central**

SoftwareSupportSP.Aveva.com/#/SecurityCentral



Security Central Resources

- **Product Cyber Security Updates**
  - Official product vulnerability issue/resolution bulletins
  - Products/lines added as needed
- **Microsoft Security Update Reports**
  - Update/KB testing results posted
- **Policies & Guidelines**
  - Support statement, related updates and statements
- **Certifications & Compliance**
  - Security Certifications, Compliance, Attestations.

Product Cyber Security Updates: Highlight Recent Posts

- Mar 14, 2023 - AVEVA-2023-001
  - AVEVA™ InTouch Access Anywhere and AVEVA™ Plant SCADA Access Anywhere: Multiple Vulnerabilities
- Aug 18, 2022 - AVEVA-2022-005
  - Multiple vulnerabilities in AVEVA Edge (formerly known as InduSoft Web Studio)
- May 9, 2022 - AVEVA-2022-001
  - AVEVA™ InTouch Access Anywhere and AVEVA™ Plant SCADA Access Anywhere – Escape from streamed app into OS context
- Feb 14, 2022 - AVEVA-2021-007
  - System Platform – Cleartext Credentials in Memory and Diagnostic Memory Dumps

Microsoft Security Updates Reporting

- Partnership with Microsoft
- Updates / KBs are tested and posted monthly by last Friday of the month
- Results posted on **Security Central** cross-referenced with **Technology Matrix**

- Related Tech Alerts
  - TA000032813 System Platform and related product issues with KN5004442 – DCOM Hardening
  - TA000034767 Microsoft Updates / KBs for .NET Framework impact System Platform and related AVEA product installations.

Cloud Security Trust Center

Ensuring your digital security

- AVEVA Cloud Security Trust Center at https://sw.aveva.com/trust
- Sub-sites for System Status, Security and Legal
- We also have available by request from Product Management:
  - CSA CAIQ completed for our Cloud products [Consensus Assessment Initiative Questionnaire]
  - Cloud Security White Paper
- And available by request:
  - SOC 2 Type 2 Report (available on request with NDA)
  - CyberGRX report (available on request with NDA)

DHS TSA Security Directive Pipeline 2021-02C (SD02C) [2022]

- Summary of Directive
  - Primarily effects Enterprise Pipeline Management Systems(OASyS), Wonderware, Citect
  - Routinely changing product passwords
  - Secure access of infrastructure, move backup media off-line/site
  - Recovery exercises from malware/ransomware
  - Limit access to customer operations environments
  - Implement multi-factor authentication, Allow-listing/whitelisting
- Typical issues
  - Issues involving Microsoft Updates – challenges bringing systems up-to-date
  - Updating passwords
  - Pointing customer to self-serve info on how-to…

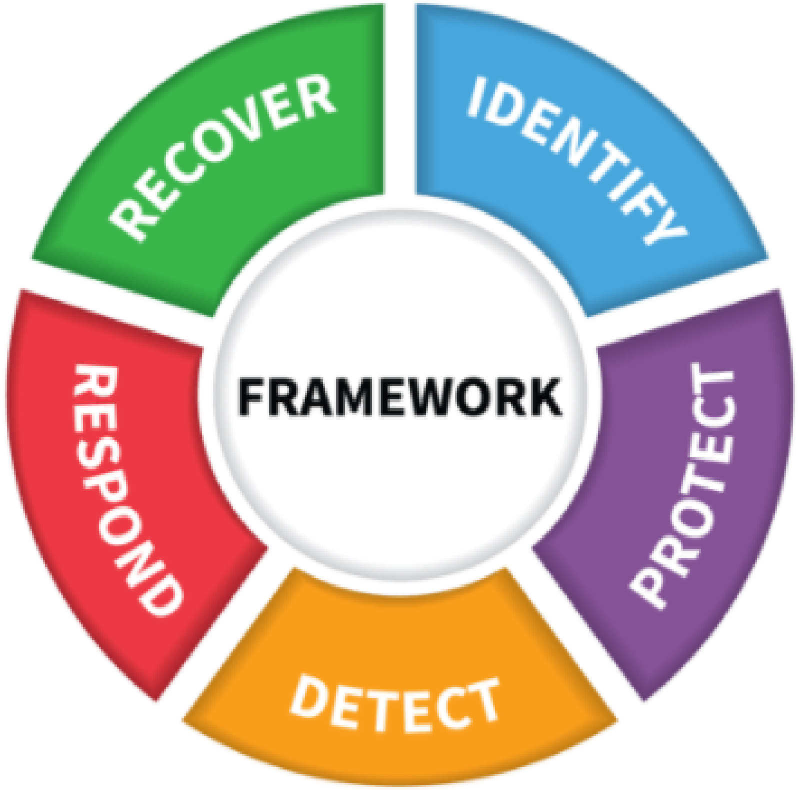
AVEVA™

Industry Best Practice Recommended Actions

AVEVA

NIST Guides

- Customers should follow the NIST Cybersecurity Framework (CSF)
- And the NIST Guide to Industrial Control Systems (ICS) Security – NIST SP 800-82.



Key Concepts and Best Practices

- Architecture and network segmentation
- Security Controls and User Management
- Vulnerability Management
- Patch/Version Management
- System Protections (Antivirus, Firewalls etc)
- Policies, Monitoring and Reporting
- Incident Response
- Business Continuity / Disaster recovery
- Training and User Education

CISA Performance Goals

CPG

Cross-Sector Cybersecurity Performance Goals

March 2023 Update

NIST CSF	Cybersecurity Practices to Address ICS Att&ck Tactics
Identify	Asset Inventory
	Mitigating Known Vulnerabilities
	Supply Chain Risk Management
Protect	Changing Default Passwords
	Account Management
	Network Segmentation
	Phishing-Resistant MFA
	Cybersecurity Training
	Strong and Agile Encryption
	Secure Sensitive Data
	Hardware and Software Approval
	System Backups
	Secure Log Storage
	Prohibit Connection of Unauthorize Devices
	No Exploitable Services on the Internet
	Limit OT Connections to Public Internet
Respond	Vulnerability Disclosure/Reporting
	Deploy Security.txt Files

Conclusions

Our Vision of Success for Internal and External Stakeholders

Customers

- Minimal risk of attack through a vulnerability in AVEVA products
- Security updates are non-disruptive and manageable

AVEVA

- Software development and operation is secure and cost efficient
- Product offers are not economically viable targets (for internal or external attack)

Regulators

- AVEVA is a trusted industry partner and actively engaged in collaboration
- Product offers are certified as fit for purpose (support of critical operations)

Moving Forward

Cybersecurity is a Partnership and Shared Commitment

- AVEVA is committed to keeping our customers secure.
- AVEVA will continue to focus on product Cybersecurity through its SDL, Tools and Practices
- AVEVA will continue to evolve our products with the latest technology to ensure our customers a secure experience with all our product offerings

Stay Safe and Secure!

Questions

Resources

Resources

Page 1

- NIST CSF
  - https://www.nist.gov/cyberframework
- NIST 800-82 r2: Guide to Industrial Control Systems (ICS) Security
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- NIST 800-61 r2, Computer Security Incident Handling Guide
  - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Resources

Page 2

- NIST 800-184, Guide for Cybersecurity Event Recovery
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf
- NIST 800-30 r1, Guide for Conducting Risk Assessments
  - https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- GPO Resources
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines
  - https://www.cisecurity.org/benchmark/microsoft_windows_server/
- Microsoft's Threat Modeling Tool
  - https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Resources

Page 3

- CISCO-AVEVA-SE Oil and Gas Pipeline Security Reference Document
  - https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Oil_and_Gas/Pipeline/SecurityReference/Security-IRD/Security-IRD.html
- National Vulnerability Database (NVD) by NIST
  - https://nvd.nist.gov/
- Common Vulnerabilities and Exposures (CVE)
  - https://cve.mitre.org/

Resources

Page 4

- SANS (Information Security Training and Resources)
    - https://www.sans.org/
- Center for Internet Security (CIS)
    - https://www.cisecurity.org/
- CISA / NCCIC / ICS-CERT
    - https://www.cisa.gov/ics
    - https://www.us-cert.gov/ics
- OWASP (Open Web Application Security Project)
    - https://owasp.org/

Resources

Page 5

- NIS Directive
  - https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
- Standards
  - IEC 62443, ISO 2700x, NERC, NIST
- FAIR (Factor Analysis of Information Risk)
  - Value at Risk (VaR) Framework for cybersecurity and operational risk
  - https://www.fairinstitute.org/

This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.

AVEVA

linkedin.com/company/aveva

@avevagroup

ABOUT AVEVA

AVEVA is a world leader in industrial software, providing engineering and operational solutions across multiple industries, including oil and gas, chemical, pharmaceutical, power and utilities, marine, renewables, and food and beverage. Our agnostic and open architecture helps organizations design, build, operate, maintain and optimize the complete lifecycle of complex industrial assets, from production plants and offshore platforms to manufactured consumer goods.

Over 20,000 enterprises in over 100 countries rely on AVEVA to help them deliver life's essentials: safe and reliable energy, food, medicines, infrastructure and more. By connecting people with trusted information and AI-enriched insights, AVEVA enables teams to engineer efficiently and optimize operations, driving growth and sustainability.

Named as one of the world's most innovative companies, AVEVA supports customers with open solutions and the expertise of more than 6,400 employees, 5,000 partners and 5,700 certified developers. The company is headquartered in Cambridge, UK.

Learn more at www.aveva.com

AVEVA