HCLSoftware

HCL BigFix

Reducing cyber risk through prioritized vulnerability remediation – Staying one step ahead of APTs.

Mark Hafner

BigFix Federal – CDM Lead

mark.hafner@hclfederal.com

HCL BigFix
Enterprise Security

Agenda

- Intro
- Presentation
  - Challenges
  - CVE Statistics
  - Advanced Persistent Threats (APTs)
  - Improving Detection, Remediation, & Resilience
    - Automatic Patching
    - Prescriptive Guidance
    - Correlation
- Demo
- Q&A

BigFix

Automate, Orchestrate and Secure

The world's leading Endpoint Management Platform with secure AI, automation capabilities, innovative risk management and continuous compliance enforcement.

100M+
Endpoints managed in 47 countries

100+
OSes supported from mobile to hybrid cloud

350K+
Out of box fixlets for remediation

1M+
Endpoints managed with AIOps

38K+
Out of the box compliance checks

- Full visibility and control for lifecycle management from asset to software application
- Continuous security compliance & policy enforcement
- Meet Zero Trust Objectives
- Generative AI and Digital Experiences for the Workspace
- Collaborative Threat Intelligence Driven Risk & Vulnerability Analysis and Remediation
- Machine Learning & Natural Language Processing based runbook automation
- Prescriptive Guidance for least disruptive, most effective patch strategies
- Exclusive C-Level proof Cyber Risk Reduction with PLA
- The Most Robust Remediation Library on the Market, covering the most OSes and applications

Trusted by 180+ Fortune 500 Companies and Over 100 US Federal Agencies

HCLSoftware

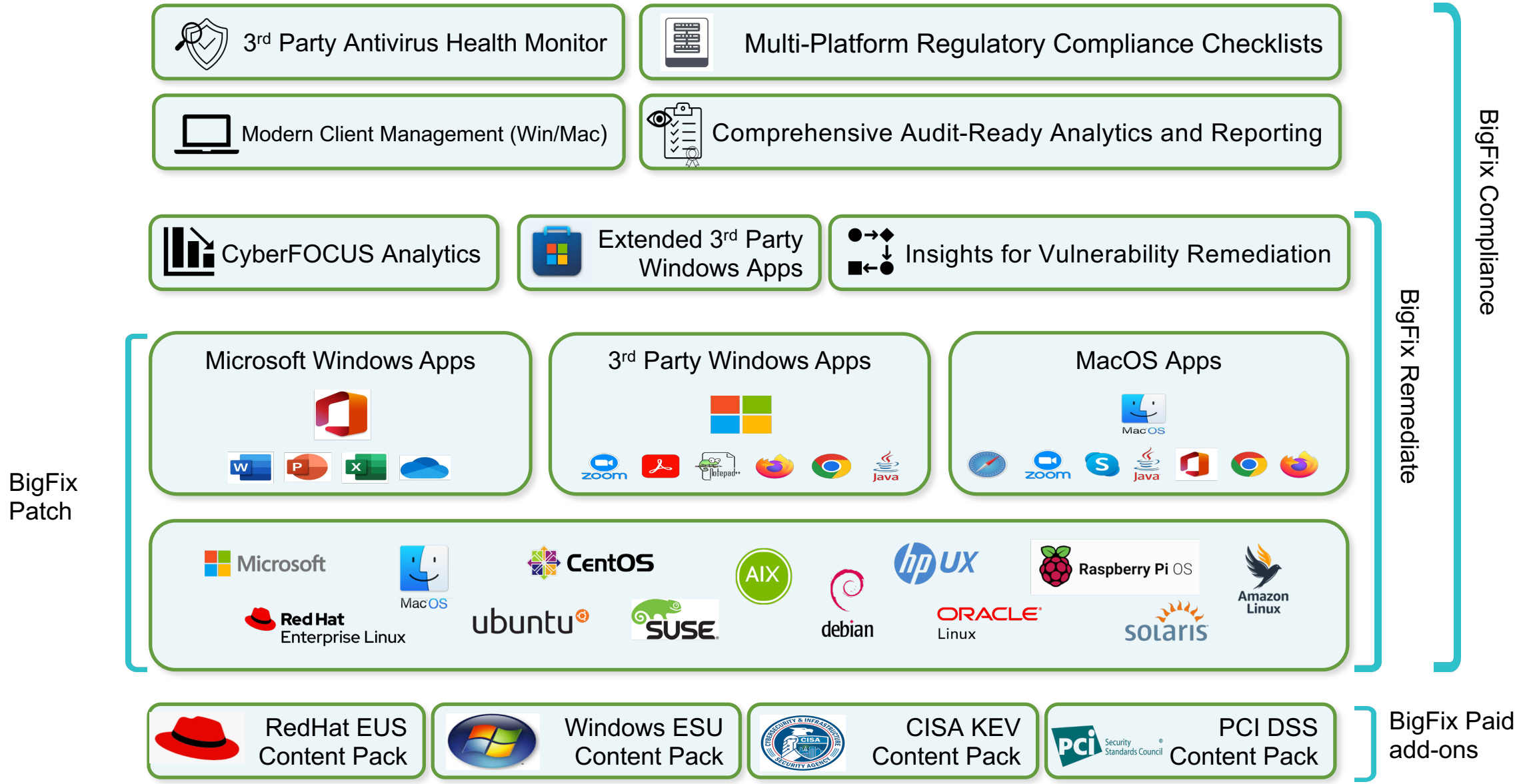
BigFix Platform

- **Scalable** – Up to 300,000 endpoints per management server
- **Secure** – FIPS 140-2 & Message Level Encryption
- **Extensible** – Leverage out-of-box capabilities or build your own
- **Flexible** – Central command and control or autonomous deployments
- **Lightweight –** Full-featured or minimal “light-weight” architecture
- **Works everywhere** – on-network, off-network, in the cloud, air-gapped, over limited bandwidth, via satellite links

BigFix Platform - Real-time visibility, scalability, and ease of use

Single server and console	Cloud-based content delivery	Flexible policy language (Fixlets)	Lightweight infrastructure	Single intelligent agent
• Highly secure and scalable • Aggregates data, analyzes and reports • Pushes out pre-defined / custom policies	• Highly extensible • Automatic, on-demand functionality • 500K+ Published Fixlets. • New content added daily + community (BigFix.me)	• Thousands of out-of-the-box policies • Simple custom policy authoring • Highly extensible/applicable across all platforms	• Use existing systems as relays • Built-in redundancy • Supports roaming endpoints • Bandwidth / CPU throttling • Single Port (52311)	• Performs multiple functions • Continuous self-assessment and enforcement • Minimal impact (< 2% CPU)

BigFix Content and Functionality Offerings – Partial List



BigFix Federal Customer Profiles

65,000 endpoints
CONUS
19+ deployments
Scientific research
On-Prem

300,000 endpoints
Globally distributed
Top Secret enclaves
100+ deployments
Air-gapped

100,000 endpoints
CONUS (mostly)
Non-Class & Class
Centralized
Integrated / Orchestration

110,000 endpoints
CONUS
Non-Class & Class
Centralized
Multi-Tenant

30,000 endpoints
CONUS & Ocean-based assets
(100+ buoys)

650,000 endpoints
Globally distributed
6 deployments
Synced content
Aggregated reporting
Laptops, servers, medical devices

20,000 endpoints
CONUS
Centralized
Patch-only
Expanding

FSI MSP
CONUS
SaaS / Azure
DOD

120,000 endpoints
CONUS
Aerospace
Centralized / Missions
1000 operators
High Availability

Challenges

- Proliferation of new Advanced Persistent Threats (APTs)
  - State sponsored
  - Increased sophistication
  - Tools
- Proliferation of CVEs (242,226 as of 7/10/2024)
- De-centralization of endpoints (On-Prem, Cloud, off-network/at home)
- Siloed organizations – lack of central visibility
- Siloed operations – Windows, *NIX, Mac, Mobile
- Lack of skills/resources
- Risk Management / Change Processes

CVE Statistics for 2023

- 29,000 vulnerabilities published in 2023, amounting to over 3,800 more common vulnerabilities and exposure (CVEs) being issued last year
- Less than 1% of these vulnerabilities posed the highest risk, being actively exploited in the wild by ransomware, threat actors and malware.
- 25% of high-risk CVEs exploited on the day of publication
- 75% of vulnerabilities were exploited within 19 days of publication.
- 97 high-risk vulnerabilities, likely to be exploited, were not part of the CISA Known Exploited Vulnerabilities (KEV) catalog.
- Mean time to exploit vulnerabilities in 2023 stands at 44 days
- Exploitation of remote services, exploitation of public-facing applications, and exploitation for privilege escalation are the top three MITRE ATT&CK tactics.

Advanced Persistent Threat (APT)

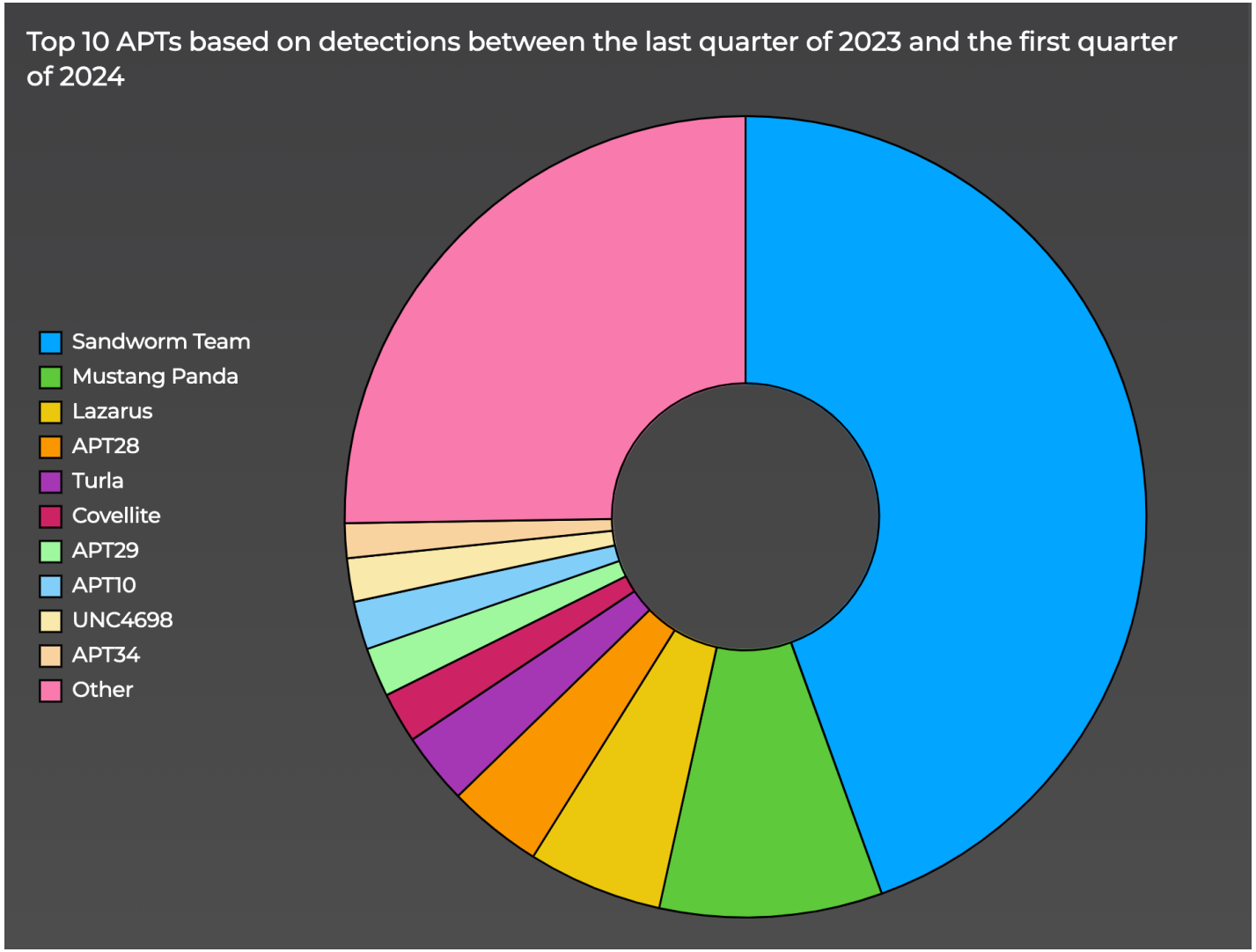
- **Advanced** – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include commercial and open source computer intrusion technologies and techniques, but may also extend to include the intelligence apparatus of a state. While individual components of the attack may not be considered particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from "less advanced" threats.
- **Persistent** – Operators have specific objectives, rather than opportunistically seeking information for financial or other gain. This distinction implies that the attackers are guided by external entities. The targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful. If the operator loses access to their target they usually will reattempt access, and most often, successfully. One of the operator's goals is to maintain long-term access to the target, in contrast to threats who only need access to execute a specific task.
- **Threat** – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well funded. Actors are not limited to state sponsored groups.

Nation-State Cyber Actors

- **Chinese government**—officially known as the People's Republic of China (PRC)—engages in malicious cyber activities to pursue its national interests including infiltrating critical infrastructure networks.
- **Russian government**—officially known as the Russian Federation—engages engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries.
- **North Korean government**—officially known as the Democratic People's Republic of Korea (DPRK)—employs malicious cyber activity to collect intelligence, conduct attacks, and generate revenue.
- **Iranian government**—officially known as the Islamic Republic of Iran—has exercised its increasingly sophisticated cyber capabilities to suppress certain social and political activity, and to harm regional and international adversaries.

Source: CISA
https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors

Top 10 APTs



Sandworm Team Profile

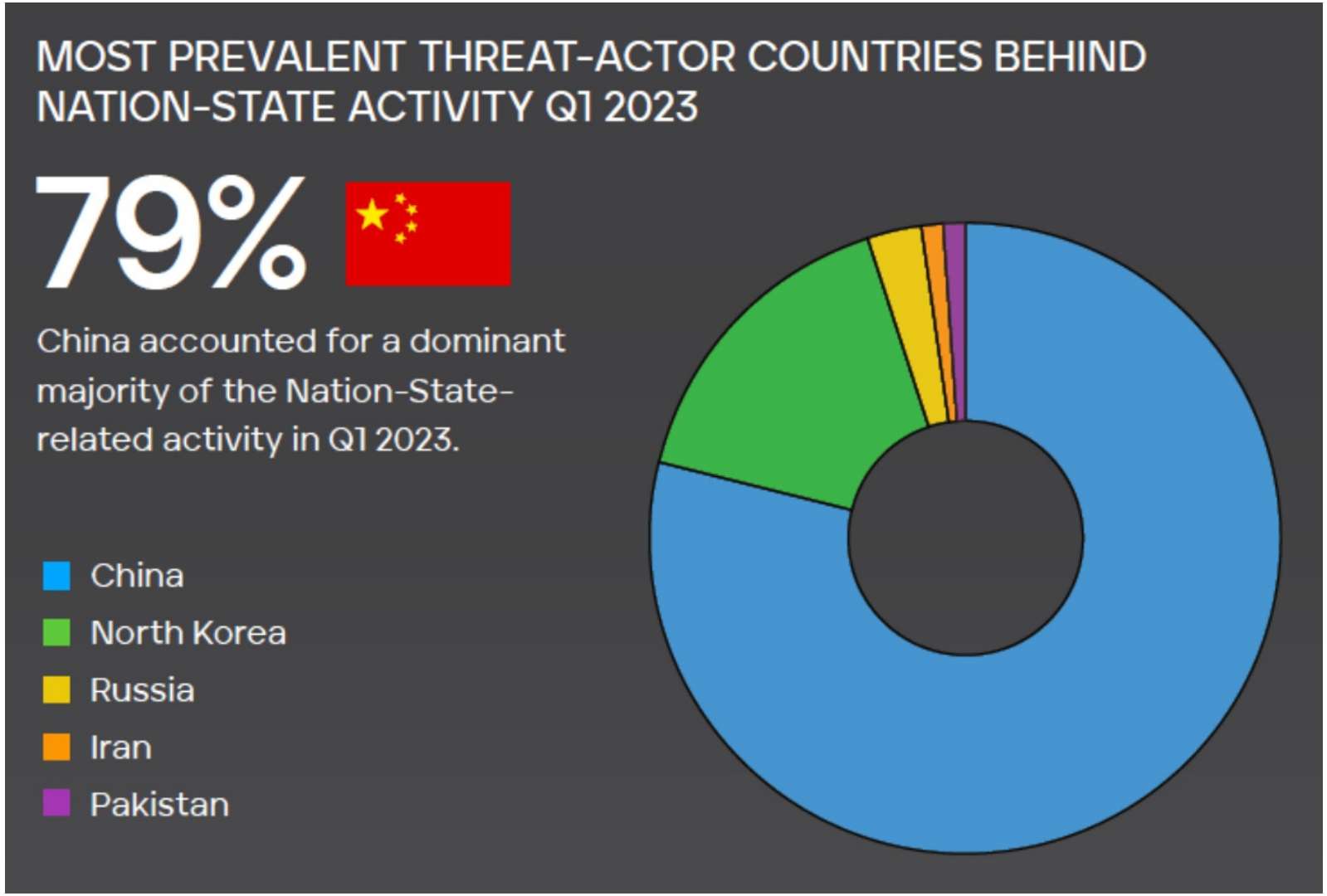
Operated by Military Unit 74455, a cyberwarfare unit of the GRU, Russia's military intelligence service

AKA: Telebots, Voodoo Bear, IRIDIUM, Seashell Blizzard,[4] and Iron Viking

Operations:
2023 SwiftSlicer
2023 Infamous Chisel
2022 Ukrainian power grid attack
2022 Cyclops Blink
2020 Exim Exploitation
2018 Winter Olympics
2017 French presidential election interference
2015/16 Ukraine power grid hack

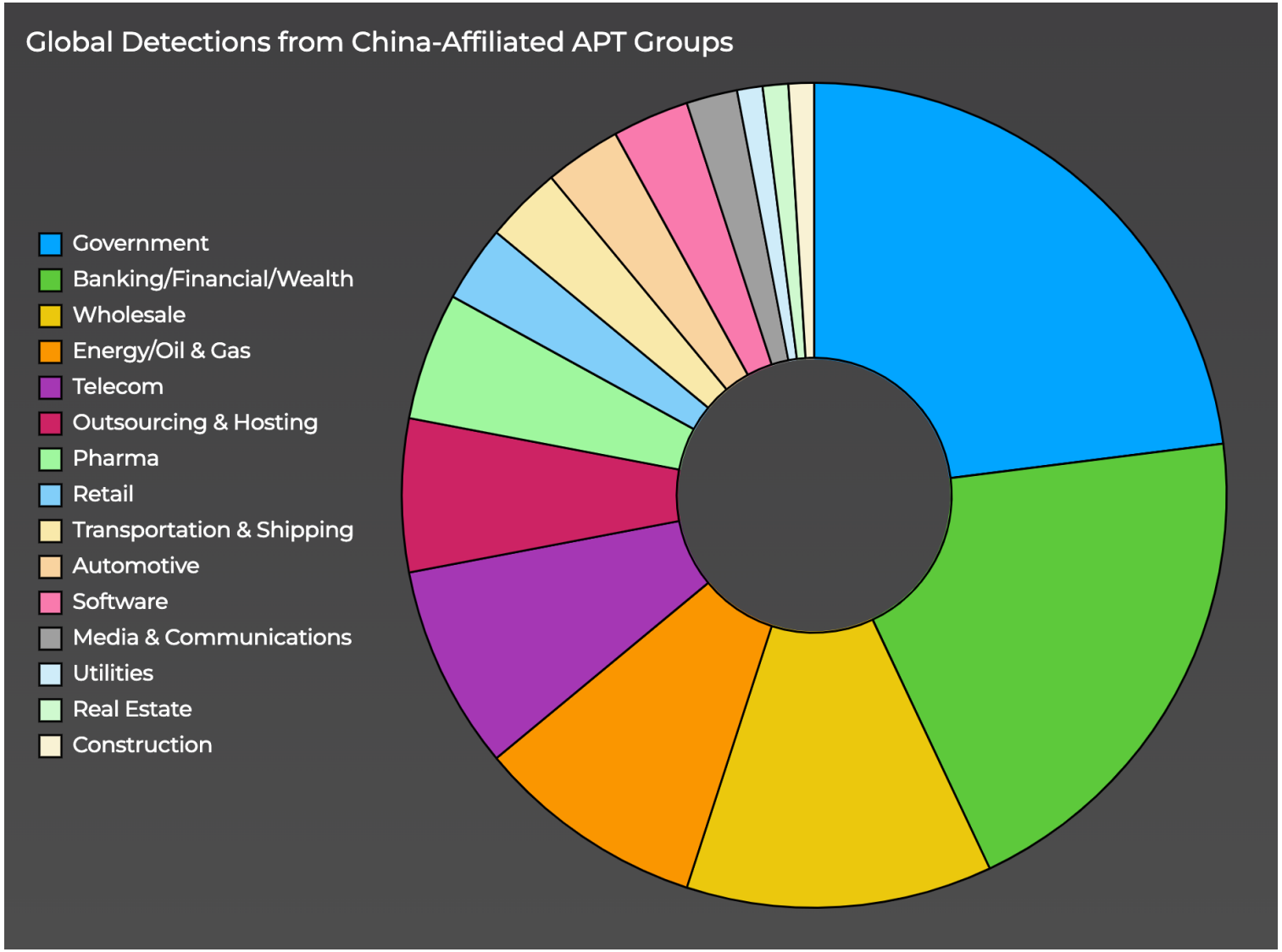
Source: Trellix - Cyberthreat Report, June 2024

Nation-Station Activity



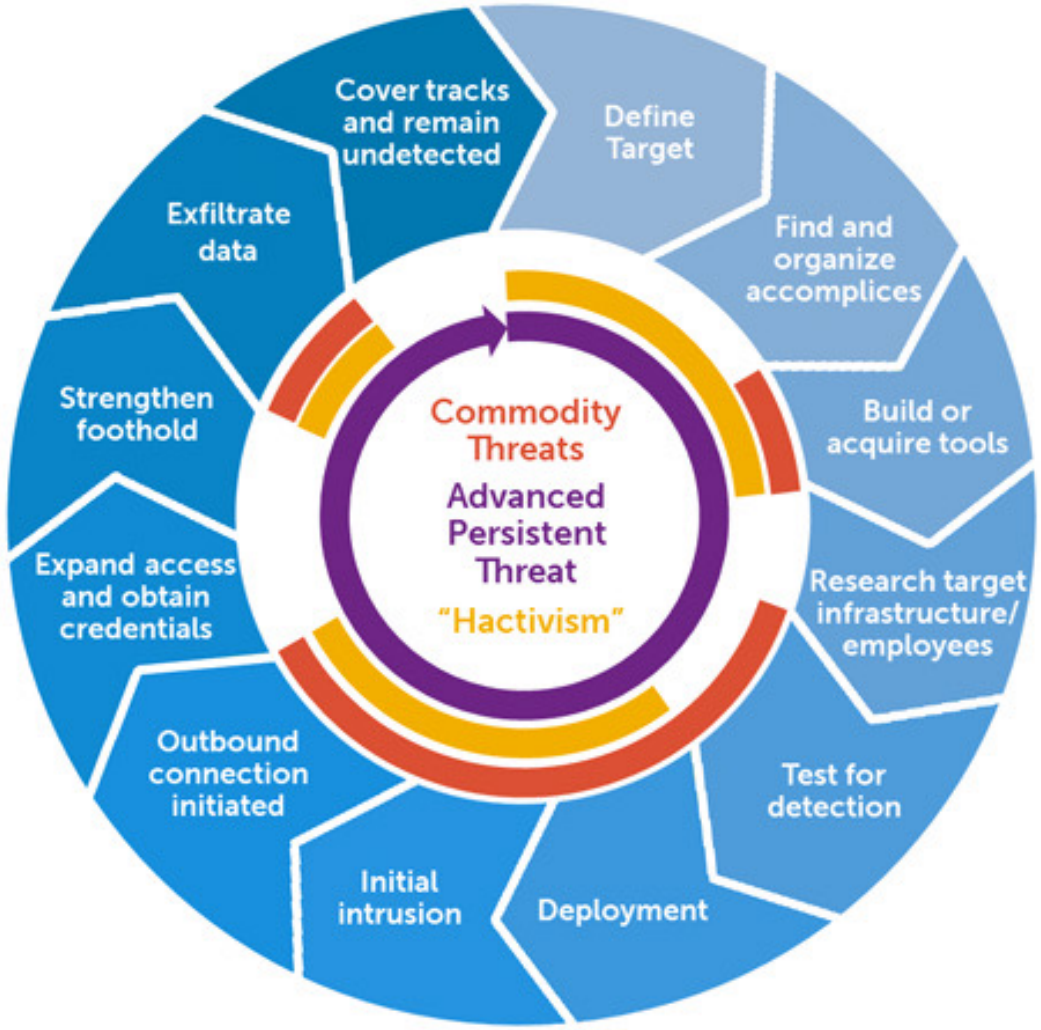
Source: Trellix - Cyberthreat Report, June 2024

By Target Sector (Chinese-Affiliated APTs)



Source: Trellix - Cyberthreat Report, June 2024

Lifecycle of an APT



1. Target specific organizations for a singular objective
2. Attempt to gain a foothold in the environment (common tactics include spear phishing emails)
3. Use the compromised systems as access into the target network
4. Deploy additional tools that help fulfill the attack objective
5. Cover tracks to maintain access for future initiatives

“We have the tools… so why have haven’t we patched those machines?”

Improving Detection, Remediation, & Resilience

Automation	Define patch policies that automatically deploy patches based upon custom criteria to select groups on a schedule.
Prescriptive Guidance	Deploy patches that remediate the most potentially harmful vulnerabilities and reduce the attack surface within my organization. The *most bang for your buck* method using simulations.
Correlation	Find synergy with compliance / vulnerability management / operations by correlating vulnerability scanning findings with your remediation tools.

Process Flows – Patch / Vulnerability Management Improvements

Automate Standard Patching

Offload the bulk of the patching efforts to fully automated content selection and pre-planned rollout schedules

- BigFix Patch Policies OS Patches
- BigFix Patch Policies 3rd Party Patches

Automate Risk/Vulnerability Data Ingestion

Pull in your vulnerability scanner results, MITRE data and CISA Known Exploited Vulnerabilities data and automatically correlate against BigFix data from systems

- Tenable Vulnerability Scan Results
- MITRE Advanced Persistent Threat Groups
- CISA Known Exploited Vulnerabilities

Prioritize the Risk

Leverage the inherent risk visibility presented through BigFix through the various data sources to understand what to focus the remediation activities on

- Leverage Tenable Severity
- Look at APT Groups known to target your specific industry
- Review the CISA list against specific risk in the environment

Roll out Advanced Remediation

Now that know what to focus on first, begin rolling out to test groups and then into full production

- BigFix IVR Remediation Workflow
- Baselines of CISA Kev Remediations
- CVE Search Dashboard to easily build baselines

Remediation Process Flows

BigFix has significantly increased visibility and remediation capabilities as compared to what the organization previously had entitlement to.

Patch Management processes are now leveraging automation in a significant manner, which allows system administrators the ability to focus on the backlog of vulnerabilities – while prioritizing on both generalized risk as well as specific risk in their environment.

Organizational system hardening standards have been established within BigFix and audit-ready reports are always available. The organization is now able to begin stepping towards the desired state in manageable remediation steps, leveraging automated remediation more and more as the organization continues to mature.

As with all patch, risk and vulnerability maturity processes – it takes time to allow for the organization to take steps forward in reasonable and responsible ways as to minimize the impact to the business while achieving better security to better protect the business.

Automation: BigFix Patch Policy (Auto-Patch)

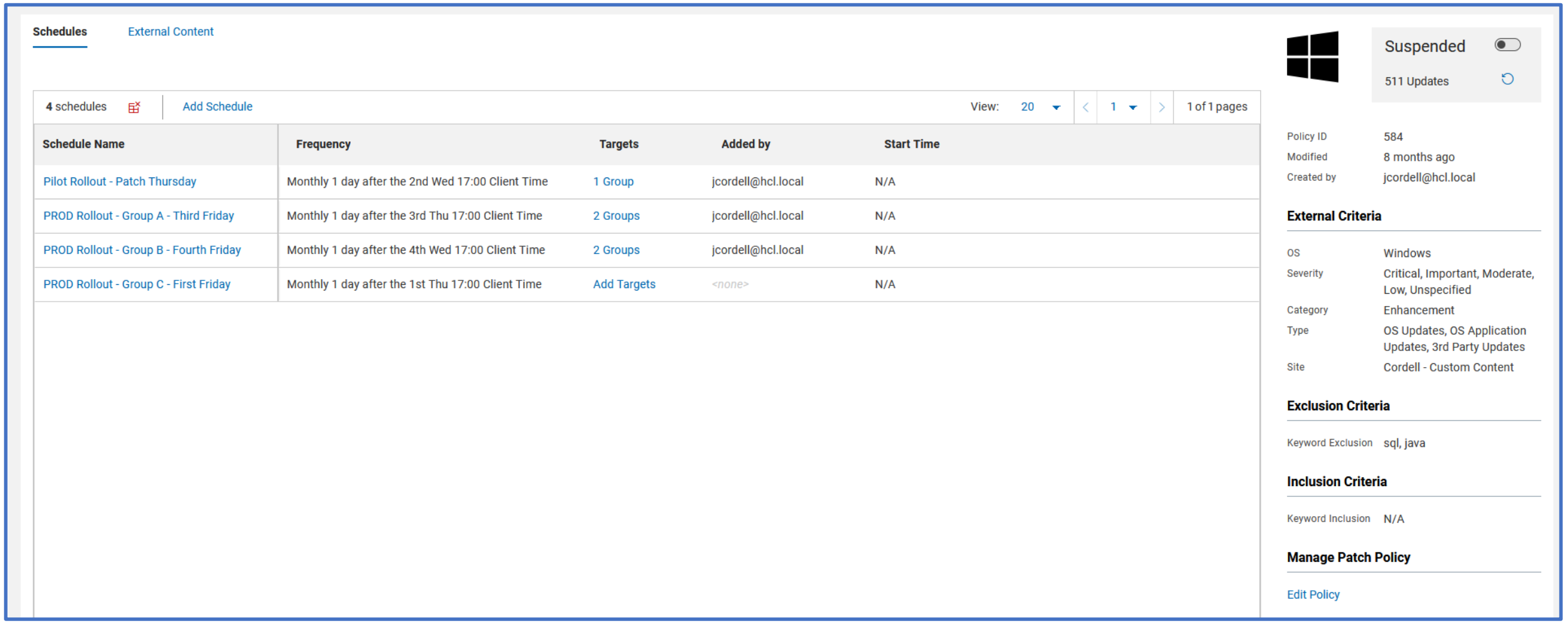
BigFix Auto-Patch

Automated patching reduces the effort required by patch administrators and operators. By defining a patch policy and schedule, operators can automate patching.

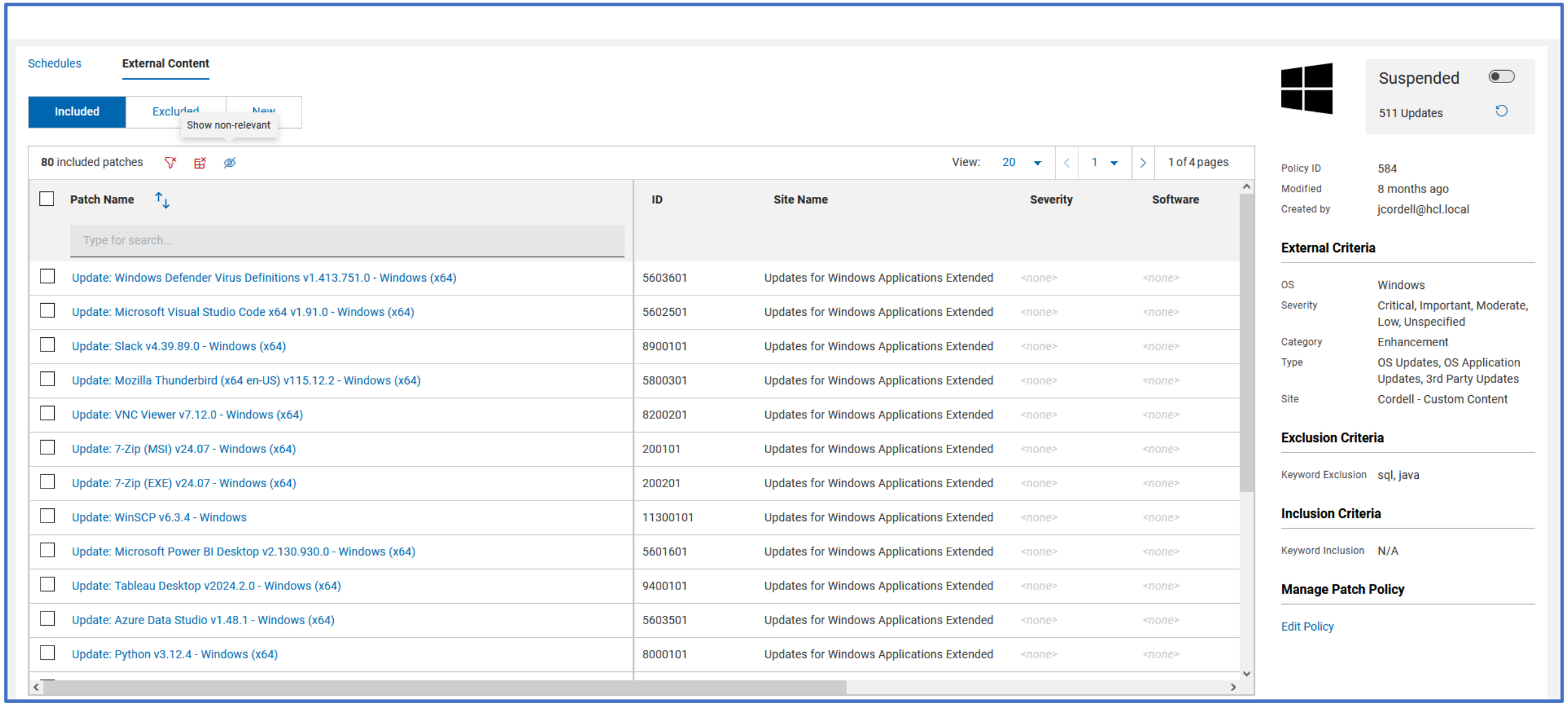
For example, a Windows Server Patch policy can be set up to only deploy critical patches, then overlay with a schedule that targets the Windows servers. Therefore, as soon as your BigFix server downloads the relevant content, patches are automatically deployed.

Refreshing the policy takes a minute or less, every month. Patches are deployed systematically and automatically saving time and effort.

Auto-Patch Schedules

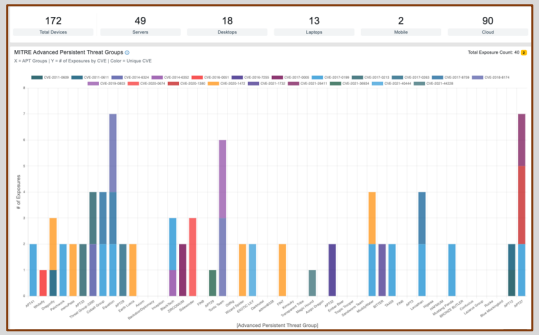


Auto-Patch Criteria & Exclusions

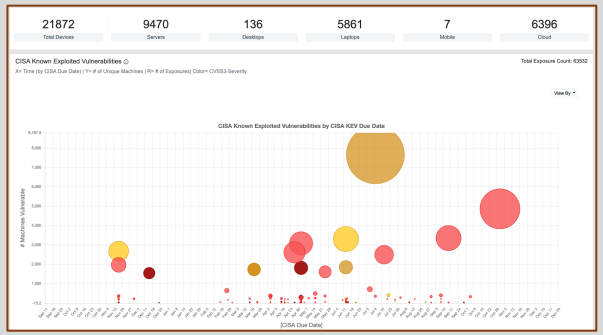


Prescriptive Guidance: BigFix CyberFOCUS

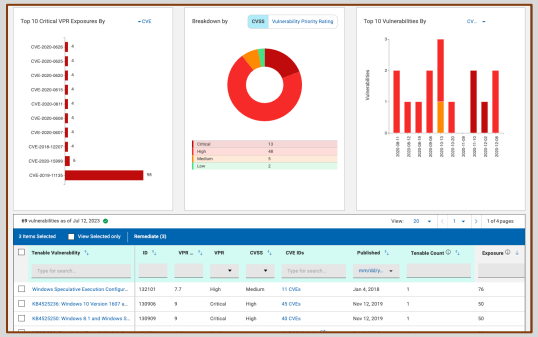
"The first vulnerability remediation solution that helps teams to collaborate to prioritize vulnerabilities, prescribe the most effective remediation strategies, protect through remediation, and prove better cyber security outcomes."



Your Exposure to Known Attackers?



Your Exposure to Known Vulnerabilities?



Your Exposure to Discovered Vulnerabilities?

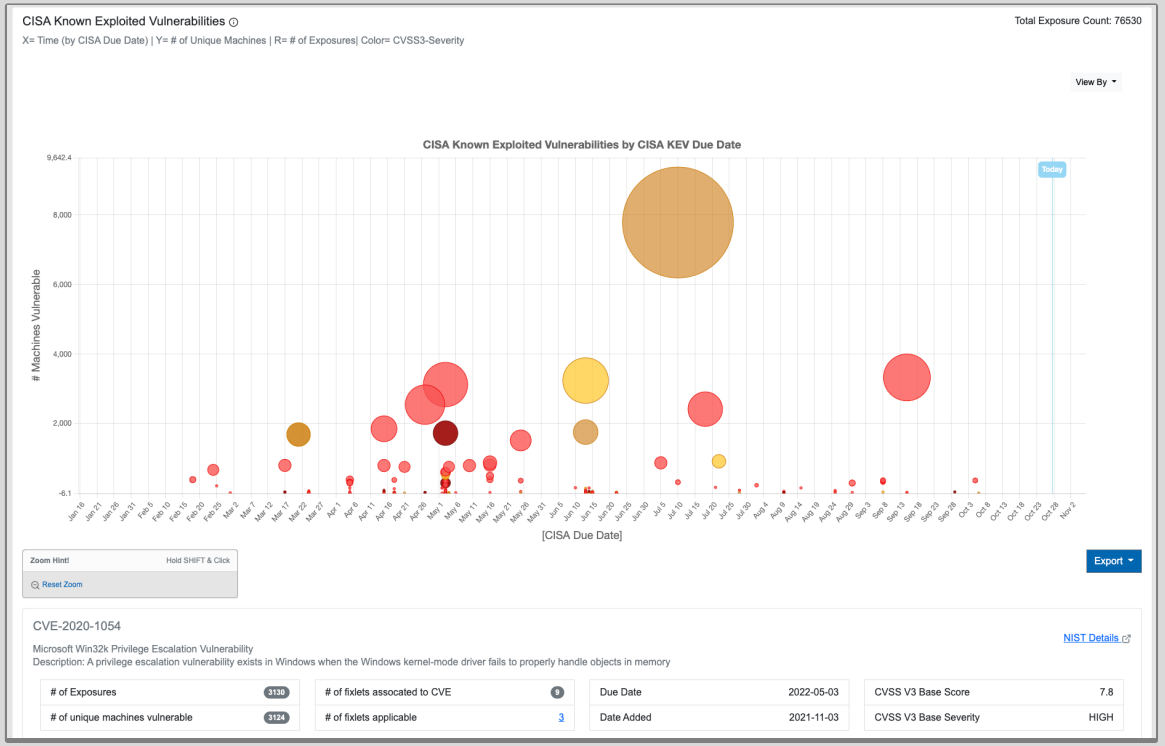
Proven Cyber Risk Reduction to C-Suite?

Advanced Persistent Threat CVE Analyzer

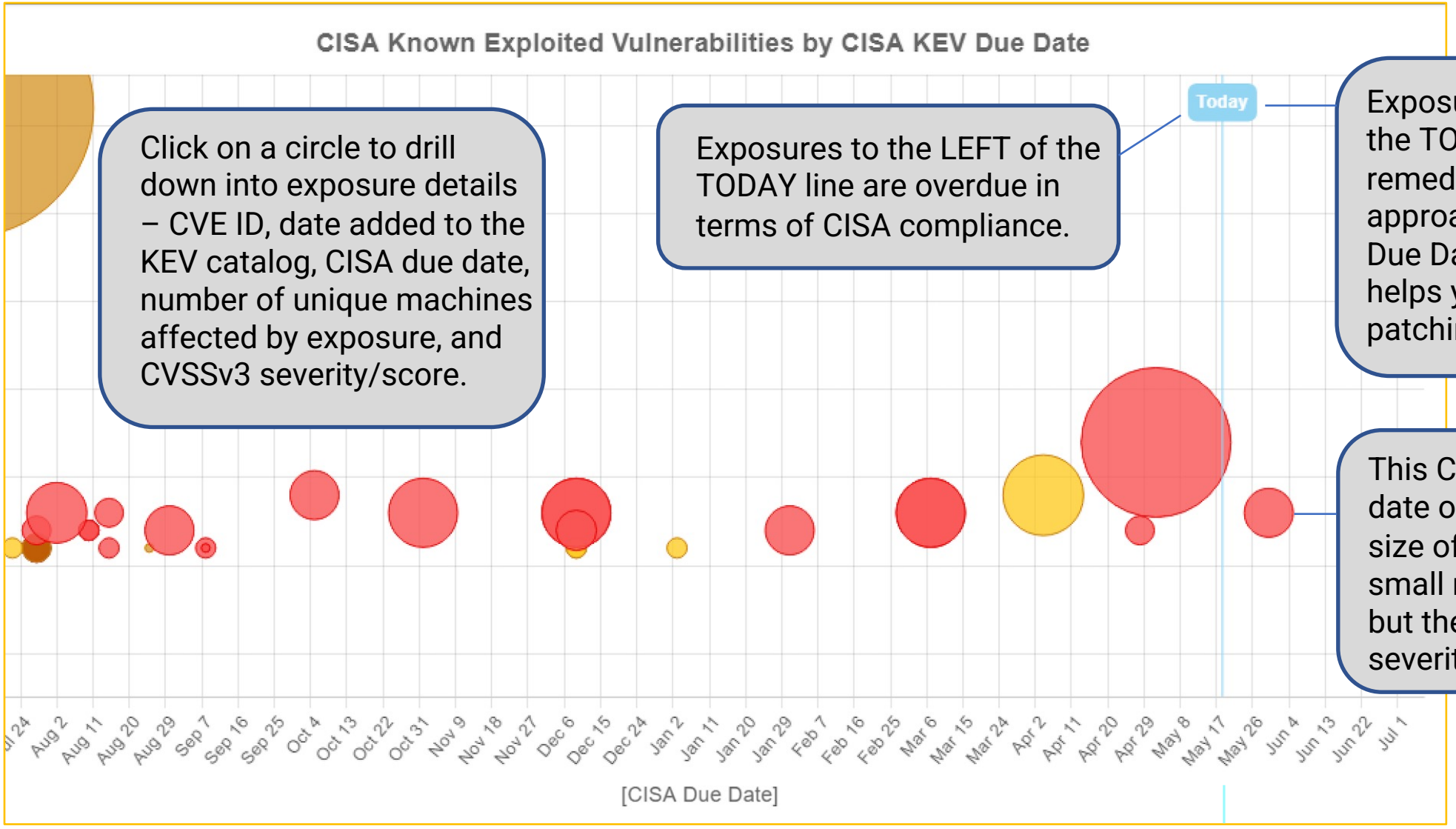
1. **Confirms priority** priority exposures to CVEs known to be used by MITRE ATT&CK Groups based on whether BigFix patched the CVEs.
2. **Includes the CVE Remediation Simulator** to do instant, real-time ‘what if’ analysis of changes in your vulnerability attack surface.
3. **Prescriptive Guidance** provides recommended remediations.
4. **Provides** information on number of devices exposed and device vulnerability density.
5. **Correlates** BigFix patch content needed with the unpatched devices regarding the CVEs in question to provide immediate protection.

CISA KEVs Exposure Analyzer

1. **Identifies priority exposures** to CVEs in CISA's Known Exploited Vulnerabilities Catalog based on whether BigFix patched the CVEs.
2. **Compares** your environment to the CISA-directed due dates for the CVEs, and your performance against those due dates.
3. **Provides** information on number of devices exposed and device vulnerability density. Prescribes the biggest attack surface gaps that need to be patched.
4. **Correlates** the BigFix Patch Content needed and the unpatched devices regarding the CVEs in question to protect the organization.



Forward-Looking Remediation Planning



Click on a circle to drill down into exposure details – CVE ID, date added to the KEV catalog, CISA due date, number of unique machines affected by exposure, and CVSSv3 severity/score.

Exposures to the LEFT of the TODAY line are overdue in terms of CISA compliance.

Exposures to the RIGHT of the TODAY line are not yet remediated and have an approaching pending CISA Due Date. This demarcation helps you prioritize your patching efforts.

This CVE has a pending due date of 05/30/2023. The size of the circle indicates a small number of exposures, but the color indicates HIGH severity.

Past Due Date (Overdue)

Pending Due Date

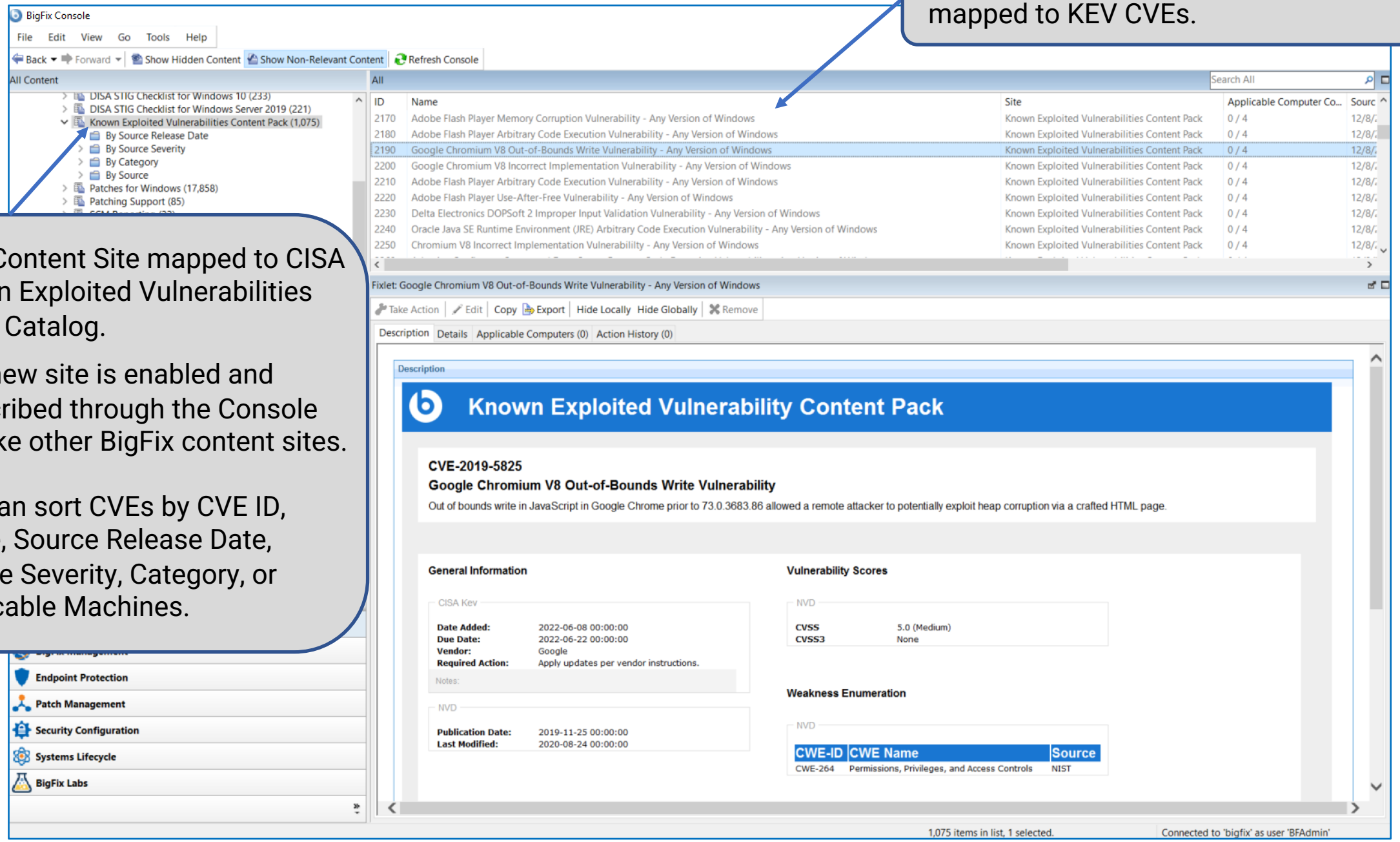
Fixlet Content Mapped to KEV Catalog

Thousands of out-of-box Fixlets per OS mapped to KEV CVEs.

New Content Site mapped to CISA Known Exploited Vulnerabilities (KEV) Catalog.

This new site is enabled and subscribed through the Console just like other BigFix content sites.

You can sort CVEs by CVE ID, Name, Source Release Date, Source Severity, Category, or Applicable Machines.



BigFix KEV Content Pack Summary

- New add-on solution leverages your existing BigFix deployment to detect, analyze, and remediate* time-sensitive vulnerabilities published in the CISA KEV catalog.
- Includes an updated Fixlet content site mapped directly to the CISA KEV catalog. Simply enable it, subscribe your endpoints, and within minutes you have CISA KEV exposure reports and planning guidance.
- Forward-looking analytics (CyberFOCUS Dashboard) keeps you focused on pending due dates, and additional exposure and severity indicators help prioritize your remediation efforts.
- Leverages your existing BigFix infrastructure; no new servers, databases, or agents required. Deployment takes just minutes.
- Operates in both internet-facing and air-gap networks.
- Priced by endpoint count.

* Remediation for given CVEs for in-scope platforms will be made available in the Content Pack where possible

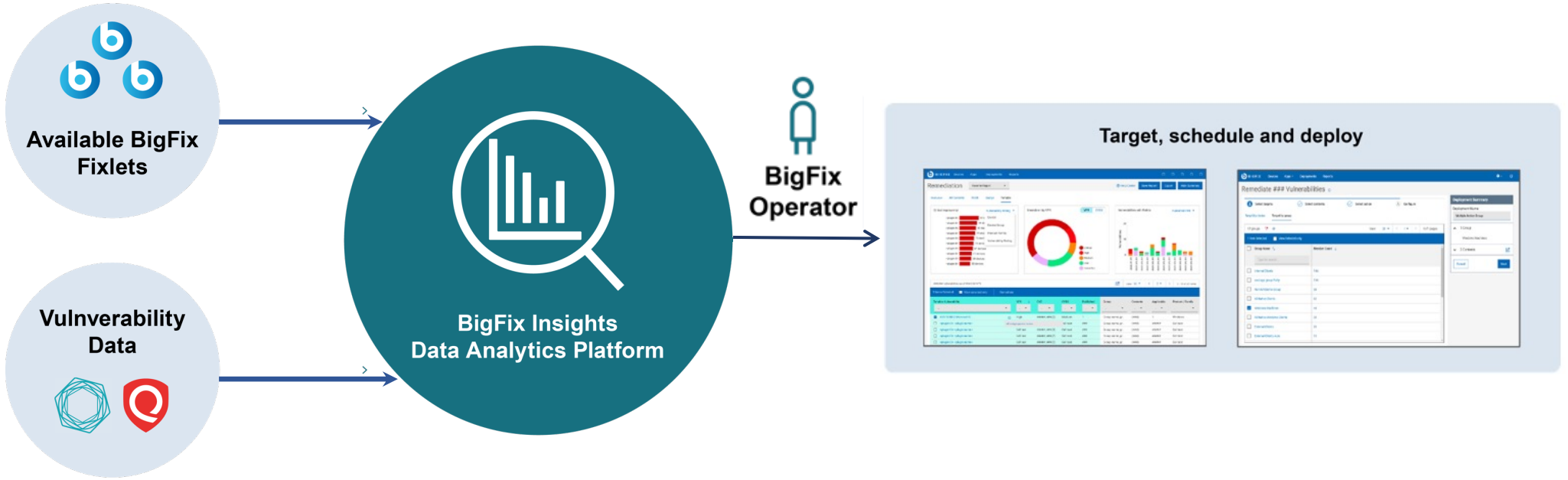
HCL BigFix

Protection Level Agreements

Measure performance of remediation against business-driven targets

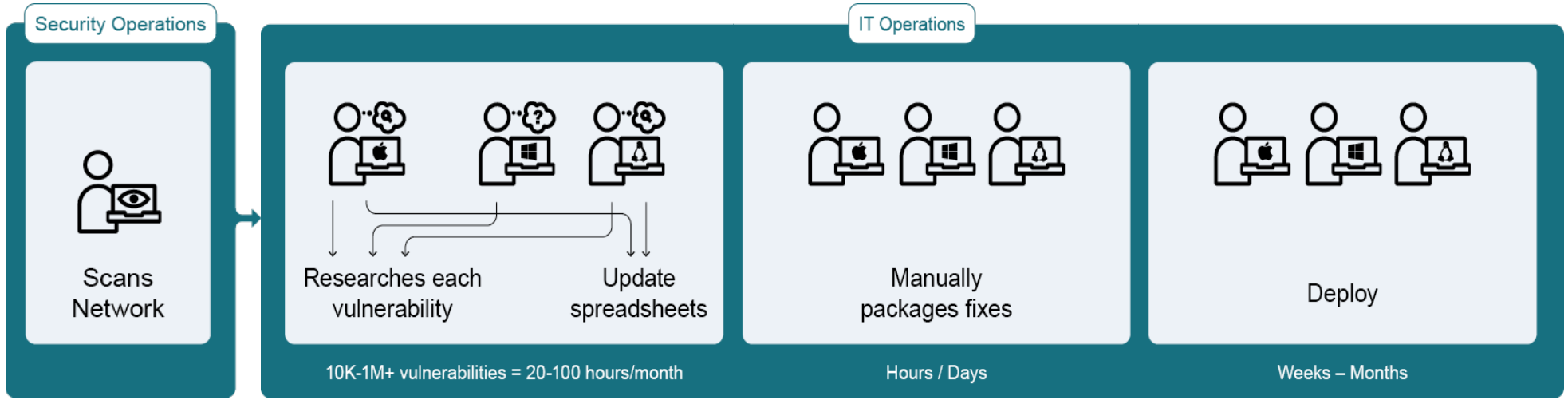
- ✓ **Aligns IT Operations with Business Objectives**, balancing business objectives/goals with cyber risk tolerance.
- ✓ **Leverages baselines** that combine asset criticality, CVE criticality, desired patch levels, and compliance standards against agreed-to organizational service levels/
- ✓ **PLA report** shows remediation performance against specific asset groups.

Correlation: BigFix Insights for Vulnerability Remediation



Integrates with Tenable, Rapid7 and Qualys, and imports CVS files

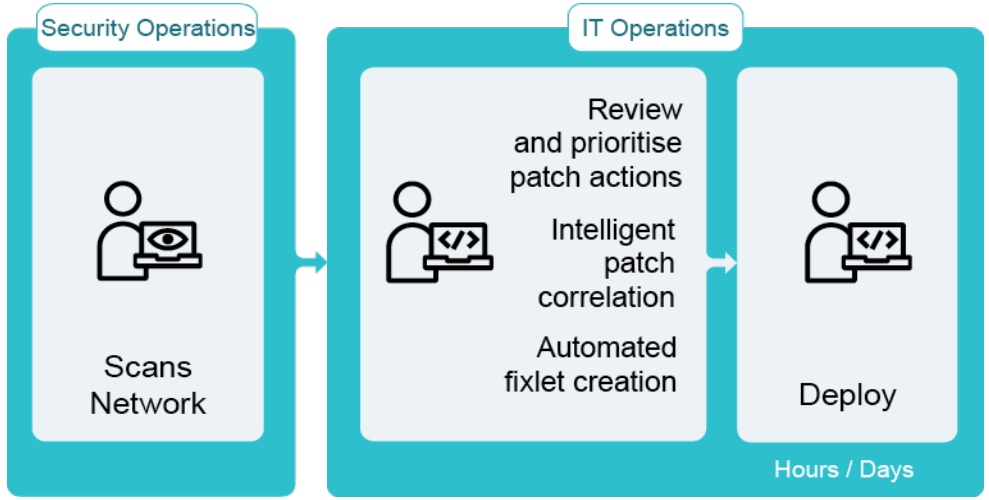
Typical Vulnerability Remediation using current tools



Current

- IT is at the end of the process
- Research and Fixes are manual tasks taking weeks
- Management activities organized by OS
- Remediations are prioritized manually
- WEEKS / MONTHS

Vulnerability Remediation using BigFix



BigFix

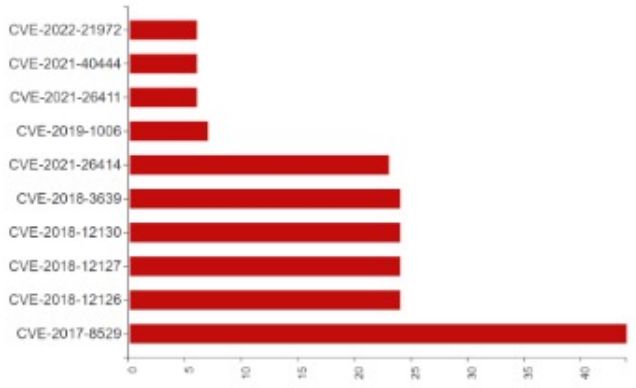
- Automates correlation and research
- Automates Fixlet creation
- Activities are OS-independent
- Speeds patching and vulnerability remediation
- Allows IT Ops to stay ahead of the threat
- HOURS / DAYS

BIGFIX Devices Apps Deployments Reports

Insights for Vulnerability Remediation

Select a favorite report | Save Report | Export | Hide Summary

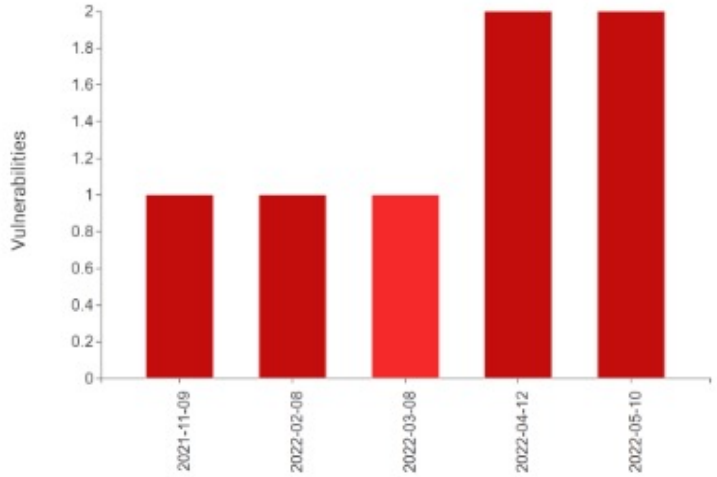
Top 10 Critical Exposures By CVE



Breakdown by CVSS | Vulnerability Priority Rating

Critical	56	Medium	39
High	45	Low	14

Top 10 Vulnerabilities By Vulnerability Priority Rating Published



154 vulnerabilities as of Jun 13, 2022 | Reset all filters | Reset columns | View: 100 | 1 | 1 of 2 pages

Tenable Vulnerability	VPR Score	VPR	CVSS	CVE IDs	Published	Tenable Count	Exposure	Product / Family
Type for search...				Type for search...	mm/dd/yy...		1	
139489: KB4571723: Windows 8.1 and Windows Server 2012...	10	Critical	Critical	49 CVEs	Aug 11, 2020	1	1	Windows
147228: Security Updates for Internet Explorer (March 2021)	9.8	Critical	High	CVE-2021-26411	Mar 9, 2021	1	3	Windows
147229: KB5000853: Windows 8.1 and Windows Server 2012...	9.8	Critical	Critical	27 CVEs	Mar 8, 2021	1	4	Windows
150354: KB5003681: Windows Server 2012 R2 Security Upda...	9.8	Critical	Critical	19 CVEs	Jun 8, 2021	1	23	Windows
151477: KB5004958: Windows Server 2012 R2 OOB Security ...	9.8	Critical	High	CVE-2021-34527	Jul 1, 2021	1	4	Windows
153374: Security Updates for Internet Explorer (September 2...	9.8	Critical	High	CVE-2021-40444	Sep 14, 2021	1	3	Windows
153375: KB5005627: Windows 8.1 and Windows Server 2012...	9.8	Critical	Critical	26 CVEs	Sep 14, 2021	1	4	Windows
121014: KB4480964: Windows 8.1 and Windows Server 2012...	9.8	Critical	High	22 CVEs	Jan 8, 2019	1	29	Windows, Office

HCLSoftware

DEMO

HCL BigFix
Enterprise Security

Useful Links

BigFix Briefing Room: What's New June 2024

https://www.youtube.com/watch?v=O8rgxdwD9J8&list=PLVAvGzDq49UlKLmsLngRqUNJBylbPOpOu&index=7

BigFix Tech Advisors (All Videos)

https://www.youtube.com/@BigFixTechAdvisors

MITRE ATT&CK®

https://attack.mitre.org/

APT Groups

https://attack.mitre.org/groups/

BOD 23-01

https://www.cisa.gov/news-events/directives/bod-23-01-improving-asset-visibility-and-vulnerability-detection-federal-networks

CISA Known Exploited Vulnerabilities (KEV) Catalog

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

HCLSoftware

Questions?
Feedback?
Demo?
Trial / Eval?
Support?

Mark Hafner
BigFix Federal
301-785-5808
mark.hafner@hclfederal.com

HCL BigFix
Enterprise Security