HCLSoftware

HCL BigFix
CyberFOCUS Security Analytics

Significantly reduce cyber risk and improve resilience through prioritized vulnerability remediation

Organizations struggle to remediate vulnerabilities fast. The gap in objectives, tools and processes of security and IT operations results in critical vulnerabilities not being remediated quickly enough to protect the enterprise. BigFix CyberFOCUS Security Analytics helps IT Operations collaborate with Security Operations to PRESCRIBE the most effective remediation strategies, PROTECT against exploits and PROVE better cyber security outcomes in real time.

Prescribe

Simulate the best vulnerability remediation strategies against exploits used by APT groups and show remediation status to the CISA Known Exploited Vulnerabilities catalog.

Protect

Immediately patch exploitable vulnerabilities within BigFix that are discovered by scanning tools and correlated with available fixes.

Prove

Use Protection Level Agreement (PLA) Analyzer so you can measure and track actual cyber risk reduction using agree-upon targets defined by business stakeholders and IT Operations.

Advanced Persistent Threat (APT) Mapping and the Vulnerability Remediation Simulator

The Vulnerability Remediation Simulator displays your recorded, unremediated vulnerabilities, grouped by the most critical exploits used by MITRE APTs. Simulation shows you which remediations will reduce the APT exploit attack surface the most.

Assume a BigFix administrator wants to identify one or more vulnerabilities that, when remediated, will reduce the exploitable attack surface the most. In Figure 1, the administrator sees all the attack groups present in the environment are shown as well as the number of exposures in each group. Additionally, the administrator sees all the CVEs that are applicable to the environment, represented by the different colored bars.

By selecting CVE-2017-0199, the administrator simulates the remediation of that vulnerability and sees the number of exposures are reduced in five different attack groups as shown in Figure 2.

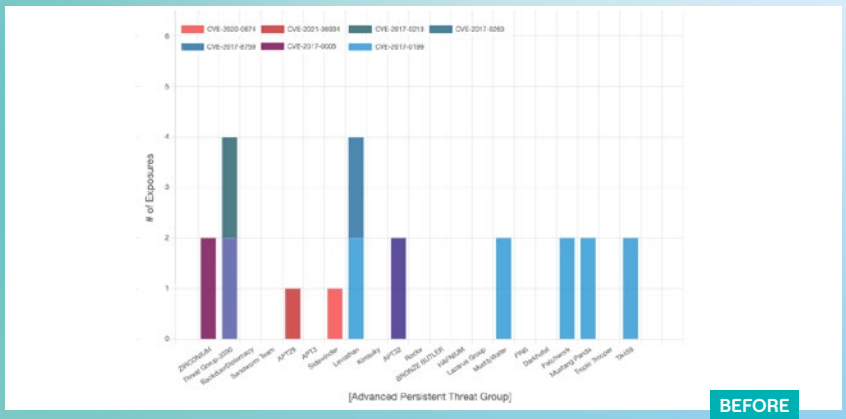

Figure 1 - Current APT Exposure

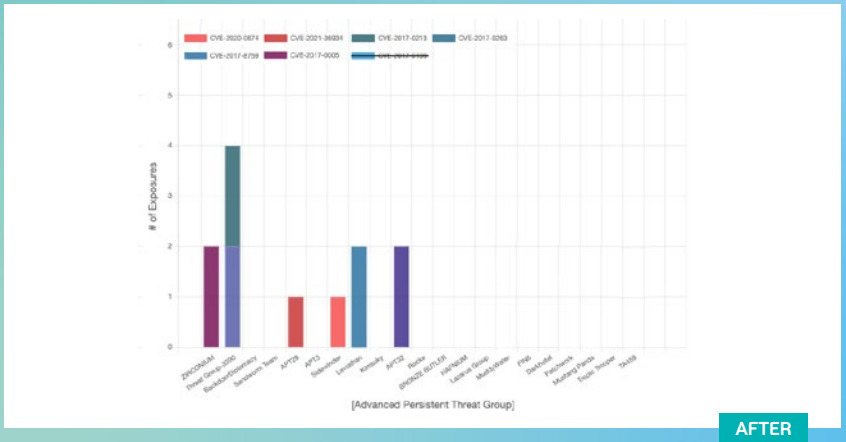

Figure 2 - Simulated APT Exposure **AFTER** remediation

Prescriptive Remediate Guidance

The Vulnerability Remediation Simulator also recommends the most impactful CVE remediations. Figure 3 depicts a pop-up which appears in the upper right corner of the Vulnerability Remediation Simulator.

Figure 3 is an example of prescriptive remediation guidance suggesting that remediating CVE-2020-1472 will remediate eight exposures and result in the greatest overall risk reduction. It also shows the total number of exposures.

Figure 3 - Example of Prescriptive Remediation Guidance

Remediation of Vulnerabilites Discovered by Industry-leading Scanners

BigFix Insights for Vulnerability Remediation integrates BigFix with vulnerability scan data. We can inject data from Tenable, Qualys, and Rapid7 using APIs as well as ingest vulnerabilities exported from another Vulnerability Manager or any vulnerability data provided in a comma-separated values (CSV) file. BigFix Insights for Vulnerability Remediation guides BigFix users on how to apply the best patch and configuration settings to remediate discovered vulnerabilities, and thus reduce risk and improve security.

The report shown in Figure 4 shows the most critical CVE exposures, enabling users to easily prioritize BigFix remediations. It shows critical exposures sorted by the user's choice of filter and sort criteria, overall distribution of exposures by criticality ratings and grouped by priority.

Advanced correlation algorithms aggregate and process the vulnerability data with information from BigFix to drive analytics and reports. At the bottom of Figure 5,

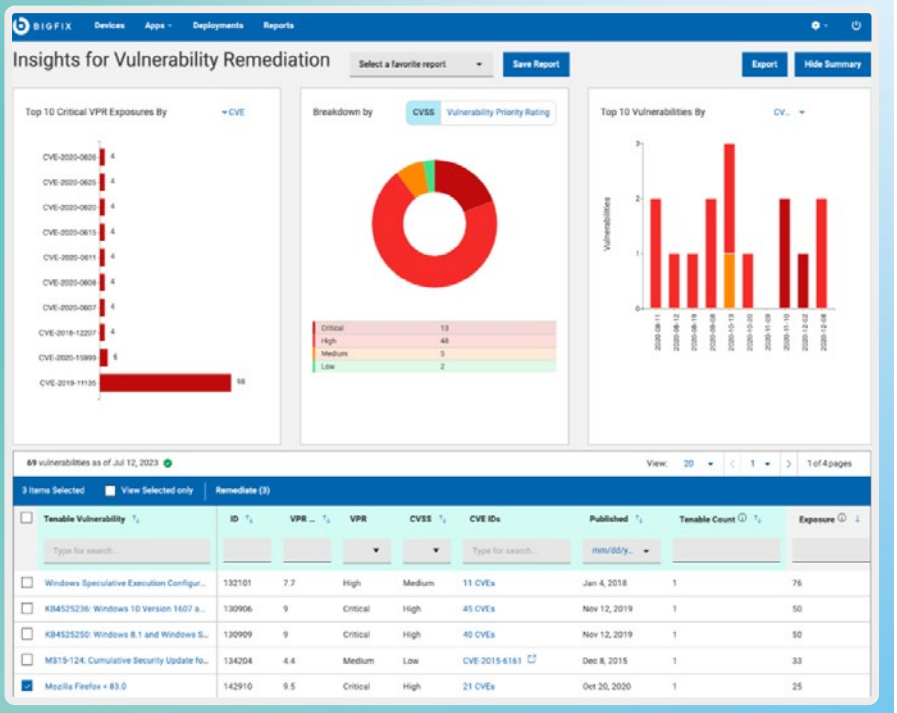

Figure 4 - Example Report of Tenable-discovered vulnerabilities

Tenable-discovered vulnerabilities have been correlated with vulnerabilities with available fixes enabling IT to select which remediations to immediately deploy.

With BigFix Insights for Vulnerability Remediation, organizations can reduce vulnerability risk by substantially reducing the time between discovery and remediation.

"The APT CVE Analyzer is very useful for us to understand what CVEs are available to the attackers. The remediation guidance in particular is really valuable and is really different from anything we have seen before."

- Sec Ops Director, Government Sector

"I love the CISA KEV Analyzer - it's perfect for our executives to understand. All they need to know is if there are a bunch of bubbles, we have a problem."

- Sr. Security Director, Manufacturing Sector

"Protection Level Agreements are now a Key Risk Indicator (KRI) for us. These are outcome driven metrics on how much risk the business is willing to take, and I urge everyone here to adopt this KRI as well. It's helped us a lot.

- BISO/CISO Finance Sector

BigFix CISA Known Exploited Vulnerability Exposure Analyzer

The BigFix CISA Known Exploited Vulnerability Exposure Analyzer maps your remediation history to the constantly updated Known Exploited Vulnerabilities Catalog published by CISA which defines the most critical threats in the world.

Using the Analyzer, IT teams can identify the most urgent and significant security issues. For instance, in Figure 5, the darker the circle, the more severe the vulnerability, and the larger the circle, the more devices are impacted. The dates on the horizontal axis indicate when CISA requires federal agencies to have completed remediation. Access to the detection and remediation content requires the Known Exploited Vulnerabilities Content Pack Add On.

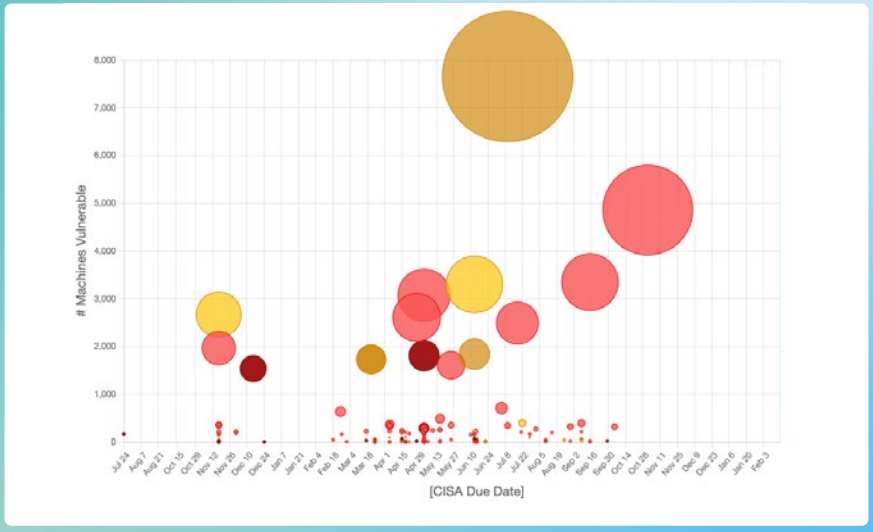

Figure 5 - A CISA Known Exploited Vulnerability Report

Define and Manage your Protection Level Agreements (PLAs)

BigFix CyberFOCUS Security Analytics introduces a new concept we call Protection Level Agreements. These are a set of baselines that combine asset criticality, CVE criticality, desired patch levels, and compliance standards against agreed-upon service levels defined by business stakeholders and IT Operations.

A Protection Level Agreement report shows defined targets and performance against those targets. Figure 6 shows performance against 10 critical areas of vulnerability patching. The blue dots indicate the agreed upon (target) service levels. Gray bars show targets that have been met; purple bars show missed targets.

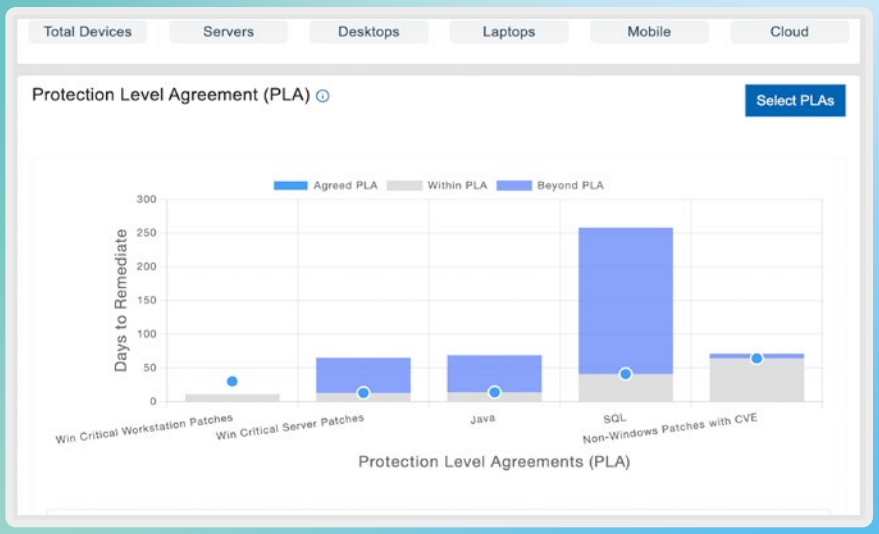

Figure 6 - Example PLA report showing defined targets and patching performance

Summary

With BigFix CyberFOCUS Security Analytics, IT and Security Operations have a set of powerful tools that enables them to align their efforts to remediate vulnerabilities fast. IT Operations can, for the first time, simulate the business impact of remediation actions to focus on the highest exposure threats; Security Operations using leading vulnerability management tools supercharge their effectiveness by more quickly correlating discovered vulnerabilities with available remediations; and IT Operations can also take a more active role in Enterprise Security by defining and measuring their performance to agreed-to business objectives. BigFix CyberFOCUS Security Analytics supercharges vulnerability management and reduces cyber risk.

BigFix CyberFOCUS Security Analytics is included with BigFix Lifecycle, BigFix Compliance and BigFix Remediate. For more information or to request a demonstration, visit www.hclfederal.com or email info@hclfederal.com

About HCLSoftware

HCLSoftware develops, markets, sells, and supports product families in the areas of Digital Transformation, Data, Analytics & Insights, AI & Automation and Enterprise Security platforms. HCLSoftware is the cloud-native solution factory for enterprise software and powers millions of apps at more than 20,000 organizations, including more than half of the Fortune 1000 and Global 2000 companies. HCLSoftware's mission is to drive ultimate customer success with its IT investments through relentless product innovation.