Powering Prevention
Lessons Learned from Building a Global Security Response Team

Christopher Clark – Director, GSRT
Many Brilliant People, Many Small Silos

Rapid organic growth in products and customers

Effort duplication, inconsistencies, and internal focus
Connect the dots and deliver holistic prevention

Proactively detect and respond to threat evolutions

Develop countermeasures, reporting, and technical solutions
Faster, Better, and Globally Impactful

Define Mission, Build Processes, Hire Team and Internalize Response in <12 months

250m+ Attacks, 31k+ Customers, 10k+ Engagements, 600+ Threats Identified
Agenda
Building a Global Security Response Team

- Stakeholder Empowerment
- Mission over Metrics
- Strategic Hiring
- Communication & Collaboration
Research & Response

Questions?

Automation, Automation, Automation!

FINISH
Stakeholder Empowerment
Proactively Engage Everyone

Seek out, Sit down (in person), and LISTEN

Understand the current reality and pain points

Access stakeholder resources and capabilities

Plan for unknown unknowns (then double it!)
Education is the MOST important job

Skip the details, tell the story

Be a trusted resource and teach up, down, left and right
Know the “NO” Monster

Leverage expertise to prioritize security resource expenditure
Identify fires before they start and protect the team
Strategic Hiring
Strategic Talent Capture

Start at the core and identify key functional areas

Acquire and empower proven leaders
Functional Teams with Matrixed Deliverables

**Vulnerability and Exploit Unit**
- Provide actionable vulnerability and exploit intelligence.
- Coverage for delivery methods and hack/post exploitation tools.

**Threat Analysis Unit**
- First line of triage. Conducting analysis of adversaries, campaigns, and TTPs.

**Malware and Countermeasures Unit**
- Provide actionable malware analysis and deployable countermeasures.

**Tools and Technology**
- Develop and enhance collection, analysis, and detection capabilities, as well as DevOps support for existing tools.
Identify and Ensure Critical Skillsets

- Improved communication and operational efficacy
- Eliminate single points of failure
- Career progression and cross training
# Team Member Critical Skillset Continuum

## Threat Researcher
- Security Operations: 80%
- Malware Analysis: 50%
- Scripting & Development: 40%
- Penetration Testing: 40%

## Malware Researcher
- Security Operations: 40%
- Malware Analysis: 80%
- Scripting & Development: 40%
- Penetration Testing: 20%

## Vulnerability and Exploit Researcher
- Security Operations: 50%
- Malware Analysis: 40%
- Scripting & Development: 40%
- Penetration Testing: 80%

## Automation Engineer
- Security Operations: 30%
- Malware Analysis: 30%
- Scripting & Development: 90%
- Penetration Testing: 30%
Regional Threat Expertise

Cultural and Linguistic Knowledge

Improved Response Speed and Quality
Metrics are an indicator, not the goal

Progress is achieved through failure

Culture is the key
PASSION: believe in the mission and what you can do
CAPACITY: learn. share. ask for help
INNOVATION: rules are a finite construct
AGILITY: change is constant, be multi-disciplinary
HUMILITY: ego-less execution

- Bryson Bort, CEO GRIMM
Great Communication is *required* for Great Security

“Remote by default” ensures expansion, flexibility, and data retention

Trust is formed in person and grows through transparency
Remove (or Connect) Data and Operational Silos

 Normalize processes and remove effort duplication
 Transparent and accessible data and deliverables
Vertical and Horizontal Status Reports

Deliver regular status reports on both research and response goals

Ensure broad delivery to all team members and stakeholders
Research & Response
Encourage Research and Response from All

Diversity of experience drives new approaches

Innovation is born from operations
Response must be efficient, Research must be impactful

Publications (Reports or Code), Presentations, or Products
Security Innovation is Distilled Threat Intelligence

Prevention is driven by heuristics refined through research

Targeted research is made possible by intelligent response
Automation, Automation, Automation!
Automation is critical to efficacy and scale

POC by researchers, maturation and upkeep by automation engineers

“Do it three times? Automate it!”
Enable and Liberate Researchers

Centralize response tool stack and maximize data density

Ensure complete auditable transparency
Develop Integrations and Orchestration

Connecting existing detection, analysis, workflow and collaboration platforms
Stakeholder Enablement
Actively engage with all stakeholders, understand their needs. Educate non-security teams, and protect your resources.

Mission Over Metrics
Culture is the most important part of the team, never compromise on fit and ensure Metrics are a guide not a target.

Communication & Collaboration
Leverage technology to expand coverage, improve efficacy, and reduce effort duplication.

Research & Response
Ensure staff is focused on short and long term research projects as well as operational triage.

Strategic Hiring
Identify required talent and proactively recruit it. Ensure all team members possess key skills.

Automation!
Dedicate resources to automating processes and tools once they have been proven.
Questions?
cclark@paloaltonetworks.com
https://www.linkedin.com/in/cybersec